Úvod do kybernetickej a informačnej bezpečnosti a jeho riadenia

(Vzdelávanie pre zamestnancov verejnej správy v kategórií používateľov „IT manažér“, „informatik“, „zamestnanec v kybernetickej bezpečnosti“ – modul č. 1)

Meno a priezvisko

XX.XX.XXXX

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KC KB UPJŠ (I.)

- UPJŠ – všetky fakulty / CSIRT-UPJS / CCVaPP
- cieľ: zvýšenie bezpečnostného povedomia relevantných subjektov | operatívnej bezpečnosti | výskum v KB

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

KC KB UPJŠ (II.)

A1 - Zariadenie a vybavenie KC

A4 - Výskumná činnosť

A7 – Zvyšovanie odbornosti

A2 - Tvorba materiálov, predmetov

A5 - Expertná činnosť

A8 - Spolupráca

A3 - Tvorba metodík, vzdelávacích materiálov

A6 - Celoživotné vzdelávanie

A9 - Odborné poradenstvo

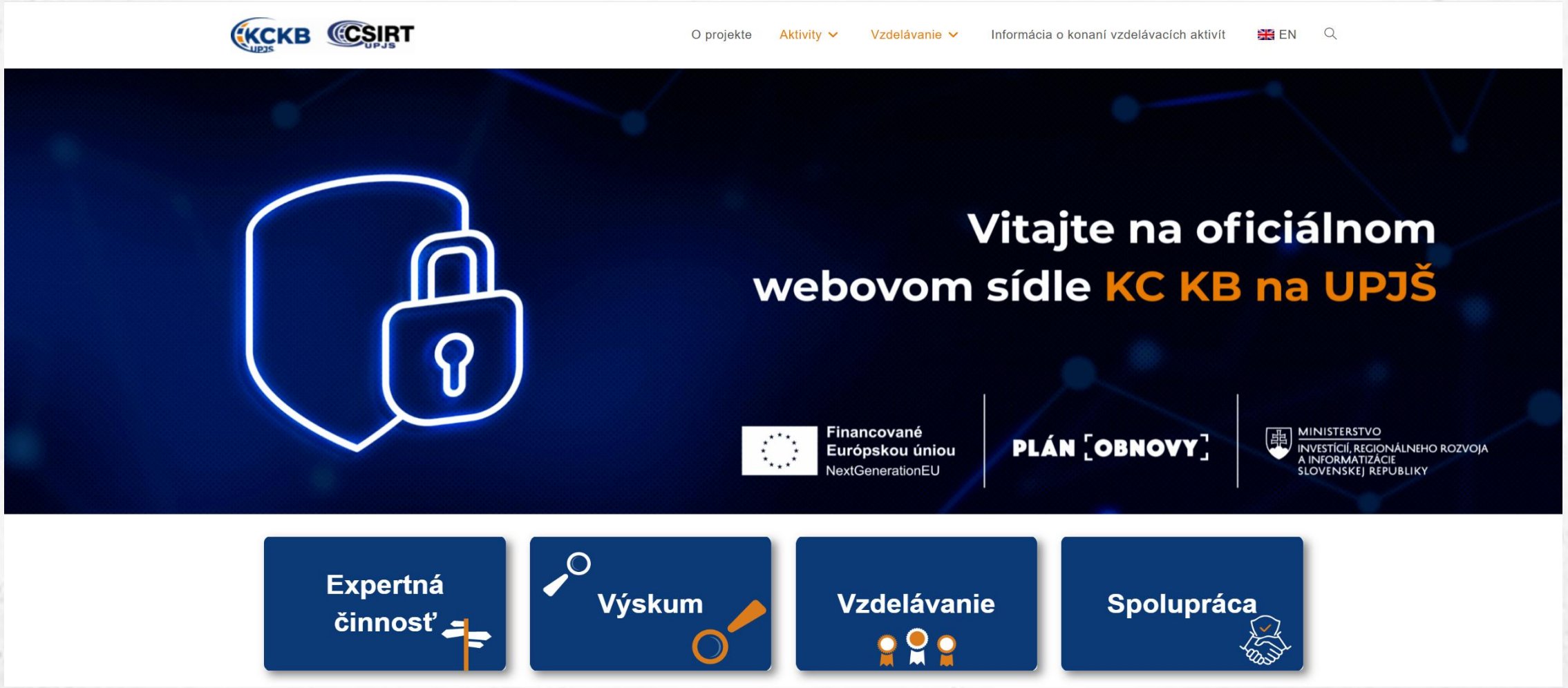
Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KC KB UPJŠ (III.)

https://**cyberawareness.sk/**



Vzdelávacia aktivita (I.)

- Vyhláška č. 492/2022 Z. z. ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti – príloha č. 3 a 4
  - kategória používateľov **„IT manažér“, „informatik“, „zamestnanec v kybernetickej bezpečnosti"**
  - kategória používateľov **„laik“, „odborný zamestnanec“ a „manažér“**

Špecialista kybernetickej bezpečnosti

Rola:	**Špecialista kybernetickej bezpečnosti**	
Vedomosti:	**Riadenie bezpečnosti**	
	1) procesy, systémy a zásady riadenia informačnej a kybernetickej bezpečnosti vrátane zásad riadenia fyzickej a objektovej bezpečnosti	BL4
	2) zásady organizácie informačnej a kybernetickej bezpečnosti	BL4
	3) terminológia a skratky v oblasti informačnej a kybernetickej bezpečnosti	BL5
	4) princípy riadenia IT služieb, správy systémov a správy počítačových sietí	BL4
	5) hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (kľúčové ukazovatele výkonnosti – KPI, kľúčové ukazovatele rizík – KRI, metodiky merania vyspelosti atď.)	BL4
	6) zdroje, charakteristiky a použitie informačných aktív organizácie	BL5
	7) organizačné politiky, organizačné štruktúry a koncepty plánovania vzťahov s internými a/alebo externými organizáciami	BL3
	8) koncepcie zlepšovania organizačných procesov a modely hodnotenia vyspelosti procesov (napr. CMMI)	BL5
	9) procesy riadenia kontinuity činností a plánovania havarijnej obnovy prevádzky	BL5
	10) princípy podnikovej architektúry, koncepcie bezpečnostnej architektúry a referenčné modely podnikovej architektúry (napr. TOGAF, Zachman, FEA atď.)	BL5
	11) koncepty, terminológia a princípy prevádzky elektronických komunikačných systémov (počítačové a telefónne siete, satelitné, optické, bezdrôtové atď.)	BL5
	12) model OSI, mapovanie siete, topológia sietí, hlavné sieťové protokoly a sieťové služby	BL4
	13) princípy sieťových zariadení (rozbočovače, prepínače, smerovače, brány, firewall atď.)	BL5
	14) charakteristiky fyzických a virtuálnych nosičov údajov	BL5
	15) elektronické zariadenia (napr. počítačové systémy/komponenty, zariadenia na kontrolu prístupu, digitálne fotoaparáty, digitálne skenery, pevné disky, pamäťové karty, modemy, sieťové komponenty, sieťové zariadenia, sieťové domáce ovládacie zariadenia,	BL5

Vzdelávacia aktivita (II.)

- Registrácia – portál CCVaPP – https://portal.ccvapp.upjs.sk/

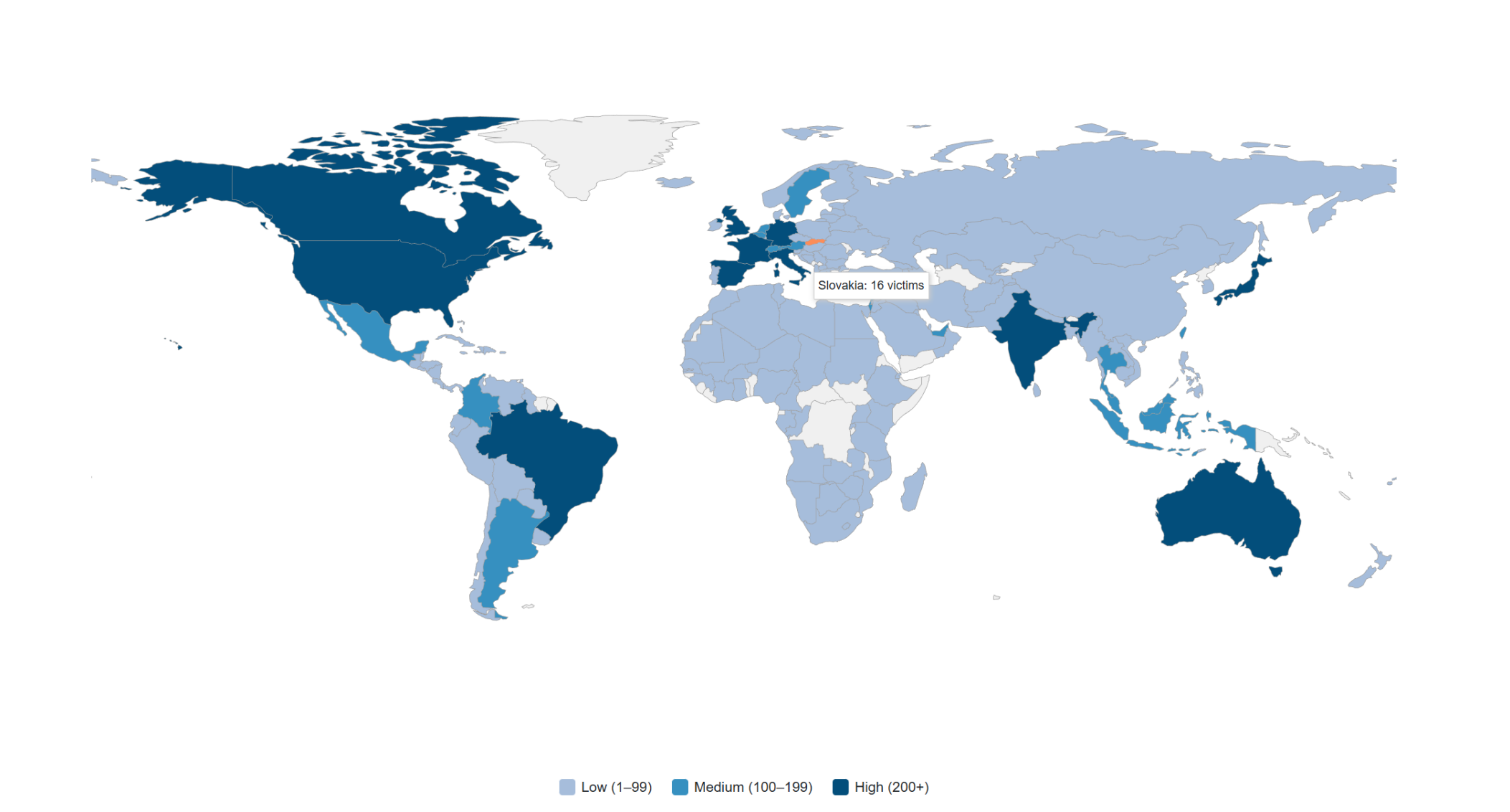
- Vzdelávanie prebieha online / prezenčne
  - Online – MS Teams platforma
  - pred každým stretnutím – odkaz
  - Prezenčne – počítačová učebňa - SJ2C06 (Prírodovedecká fakulta, Jesenná 5)

- 7 modulov
- po ukončení všetkých – osvedčenie o absolvovaní
- Diskusia – priebežne aj na záver
- Spätná väzba

Vzdelávacia aktivita (III.)

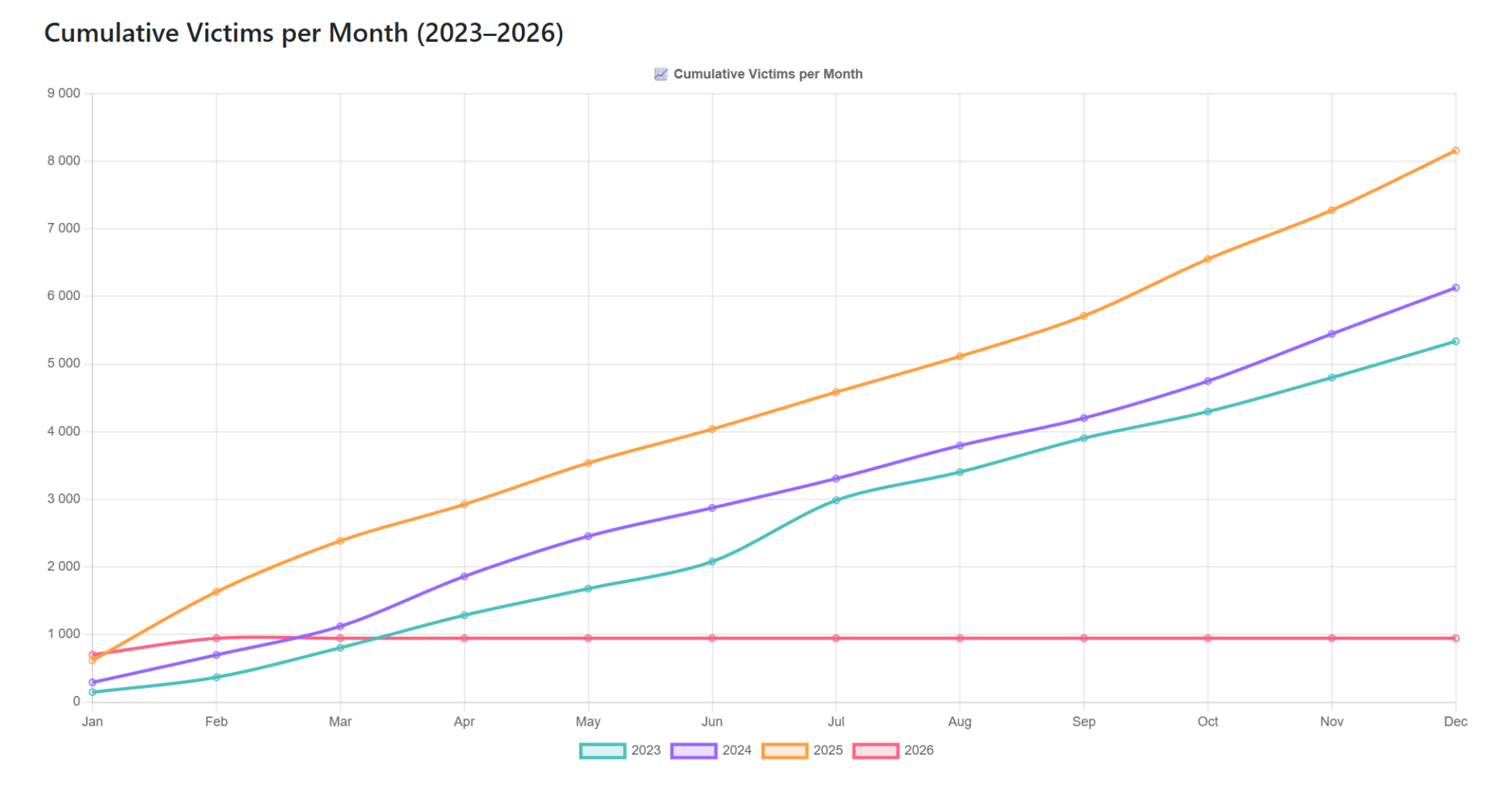
Číslo modulu	Názov modulu	Časová dotácia (45 min.)	Forma stretnutia
Modul č. 1	**Úvod do KIB a riadenie KIB**	8	Online / Prezenčne
Modul č. 2	**Vybrané kapitoly z kryptografie**	8	Prezenčne
Modul č. 3	**Vybrané kapitoly zo sieťovej bezpečnosti**	16	Prezenčne
Modul č. 4	**Reaktívne a proaktívne činnosti**	8	Prezenčne
Modul č. 5	**Reaktívne činnosti – komunikácia**	6	Prezenčne
Modul č. 6	**Vybrané kapitoly z práva informačných a komunikačných technológií I.**	8	Online / Prezenčne
Modul č. 7	**Vybrané kapitoly z práva informačných a komunikačných technológií II.**	8	Online / Prezenčne

Svet okolo nás (I.)



Zdroj: https://www.ransomware.live/map?year=full

Svet okolo nás (II.)



Zdroj: https://www.ransomware.live/stats

Svet okolo nás (III.)

2020

Nemocnicu v Česku ochromil ransomvér, naplánované operácie sa rušia

Redakcia CyberSec.sk / 12.12.2019

Ransomware attack: Maastricht University pays out $220,000 to cybercrooks

Adam Bannister 07 February 2020 at 16:05 UTC
Updated: 11 May 2020 at 08:17 UTC

Ransomware | Netherlands | Cybercrime

Dutch institution regrets striking 'devil's bargain' but said it had to put staff and students first

Zdroje: https://mobil.sk/clanok/3517-hackeri-sa-naburali-do-kamier-android-smartfonov-keby-sa-nepriznali-nikto-by-to-ani-nevedel, https://portswigger.net/daily-swig/ransomware-attack-maastricht-university-pays-out-220-000-to-cybercrooks

Svet okolo nás (IV.)

2021

Hackers Breached Colonial Pipeline Using Compromised Password

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

LIVE ON BLOOMBERG
Watch Live TV >
Listen to Live Radio >

Photographer: Samuel Corum/Bloomberg

By William Turton and Kartikay Mehrotra
June 4, 2021, 3:58 PM EDT

Internal emails published by Bleeping Computer reveal that leading furniture retailer IKEA is battling an ongoing campaign of phishing attacks, fueled by internal and vendor accounts that have already been compromised.

Zdroje: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password,
https://www.cpomagazine.com/cyber-security/ikea-suffers-ongoing-phishing-attacks-from-compromised-internal-and-vendor-accounts/

Svet okolo nás (V.)

2022

6. septembra 2022 17:37 Firmy Lesy SR

Štátne lesy zostali po hekerskom útoku bez systémov. Nemôžu predávať palivové drevo a padol im aj portál na kontrolu ťažby

IVAN HALUZA + Zapnúť články e-mailom

Ťažba dreva v lesoch. Ilustračné foto – TASR

28.6.2022 06:55 | Telekom

AKTUALIZOVANÉ Telekom zasiahol ransomvérový útok. Funguje aktivácia balíčkov aj e-shop

Zdroj: iStock a úprava Živé.sk

Zdroj: https://zive.aktuality.sk/clanok/j42eNLl/telekom-zasiahol-ransomverovy-utok-funguje-aktivacia-balickov-aj-e-shop/, https://e.dennikn.sk/2999023/statne-lesy-zostali-po-hekerskom-utoku-bez-systemov-nevedia-predavat-drevo-a-padol-im-aj-portal-na-kontrolu-tazby/

Svet okolo nás (VI.)

2023

11.7.2023 15:14 | Bezpečnosť

TOP Hackeri zverejnili dáta ukradnuté Univerzite Mateja Bela, začínajú sa šíriť internetom

Zdroj: Ján Koliba

8.9.2023 13:59 | Bezpečnosť

Košická župa čelila kybernetickému útoku, elektronické služby úradu sú dočasne nefunkčné

Zdroj: Pixabay

Podobne ako v minulosti, aj tentoraz malo ísť o ransomvér.

Zdroj: https://zive.aktuality.sk/clanok/8rvLPeR/kosicka-zupa-celila-kybernetickemu-utoku-elektronicke-sluzby-uradu-su-docasne-nefunkcne/
https://zive.aktuality.sk/clanok/cfRr3Xq/hackeri-zverejnili-data-ukradnute-univerzite-mateja-bela-zacinaju-sa-sirit-internetom/

Svet okolo nás (VII.)

2024

22.3.2024 15:46 | Bezpečnosť

Hackeri udreli na Slovenskú národnú knižnicu. Nejdú prístupy k zdrojom ani kontakty

Zdroj: reprofoto Snk.sk, iStock a úprava redakcia

Rumunské nemocnice napadnuté ransomvérom

Vypublikované 13. 02. 2024

ransomware-nemocnice-860x360

Najmenej 25 rumunských nemocníc bolo odrezaných od online služieb po tom, čo útok ransomvéru znefunkčnil ich systém na správu zdravotnej starostlivosti. Cieľom útoku bol HIS, ktorý sa používa v nemocniciach na správu lekárskej činnosti a údajov o pacientoch. Útok, ktorý sa odohral počas noci z 11. na 12. februára 2024, zasiahol produkčné servery HIS a v dôsledku toho s**ystém prestal fungovať**, súbory a databázy boli zašifrované. **Rumunské ministerstvo zdravotníctva** uviedlo, že incident je predmetom vyšetrovania IT špecialistami, vrátane odborníkov na kybernetickú bezpečnosť z Národného riaditeľstva pre kybernetickú bezpečnosť (DNSC), a posudzujú sa možnosti obnovy. Zoznam zasiahnutých nemocníc bol aktualizovaný po zverejnení aktualizácie DNSC a zahŕňa nemocnice v rôznych regiónoch Rumunska vrátane centier pre regionálnu a onkologickú liečbu.

Zdroj: https://www.nbu.gov.sk/rumunske-nemocnice-napadnute-ransomverom/, https://zive.aktuality.sk/clanok/1CGRx85/hackeri-udreli-na-slovensku-narodnu-kniznicu-nejdu-pristupy-k-zdrojom-ani-kontakty/

Svet okolo nás (VIII.)

2025

TREND Predplatiť

Hekeri po útoku na kataster žiadajú vysoké výkupné, štát nemusí disponovať zálohami dát

Daniel Ivančák
online editor

9.1. 7:35 | **Ak sa hekerský útok v takomto rozsahu potvrdí, na Slovensku môže nastať chaos**

ŽIVE Predplatné

TOP Kataster po mesiaci: Štát prelomil mlčanie. Čo radí a sľubuje ľuďom

Zdroj: iStock, reprofoto Zbgis.skgeodesy.sk, úprava redakcia

Lukáš Kosno

Filip Hanker

Zhrnuli sme novinky okolo katastra presne mesiac po útoku. Máme oficiálne vyjadrenia úradu.

Zdroj: https://www.trend.sk/spravy/hekeri-utoku-kataster-ziadaju-vysoke-vykupne-stat-nemusi-disponovat-zalohami-dat
https://zive.aktuality.sk/clanok/MkBBFdI/kataster-po-mesiaci-stat-prelomil-mlcanie-co-radi-a-slubuje-ludom/

Zdroj: https://www.timeout.com/chicago/tv/under-the-dome-tv-review

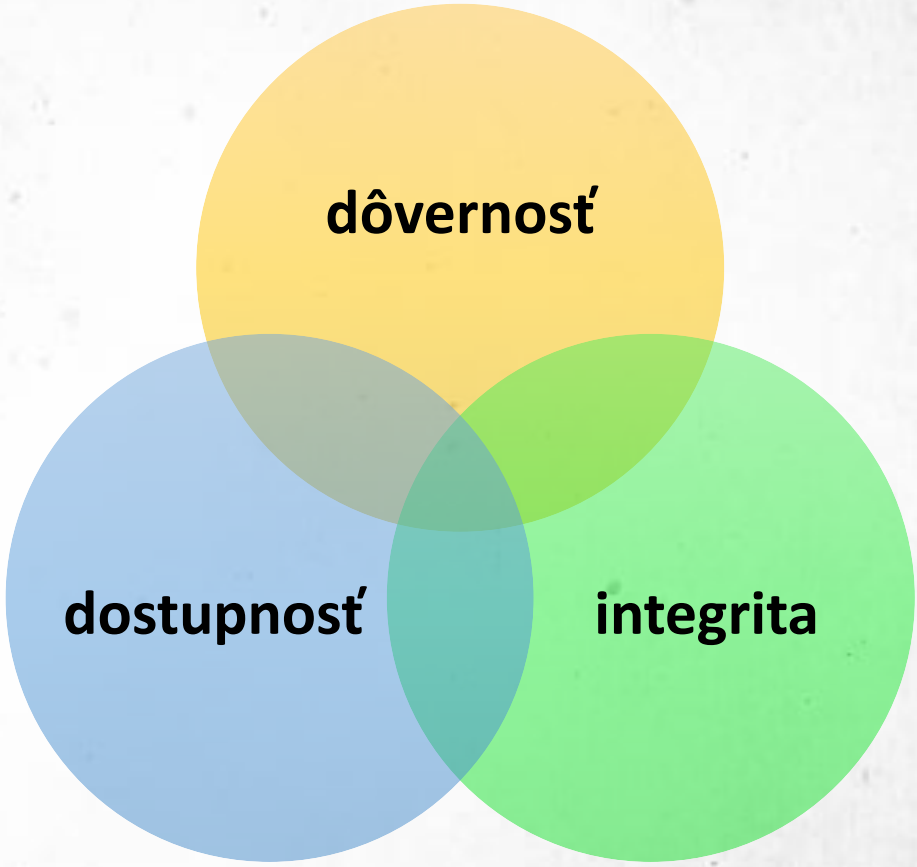
Čo je kybernetická bezpečnosť?

stav, v ktorom sú siete a informačné systémy ***schopné odolávať na určitom stupni*** *spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje* ***dostupnosť, pravosť, integritu alebo dôvernosť*** *uchovávaných, prenášaných alebo spracúvaných* ***údajov*** *alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov*

(§ 3 ods. 1 písm. h) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti)

Triáda CAI

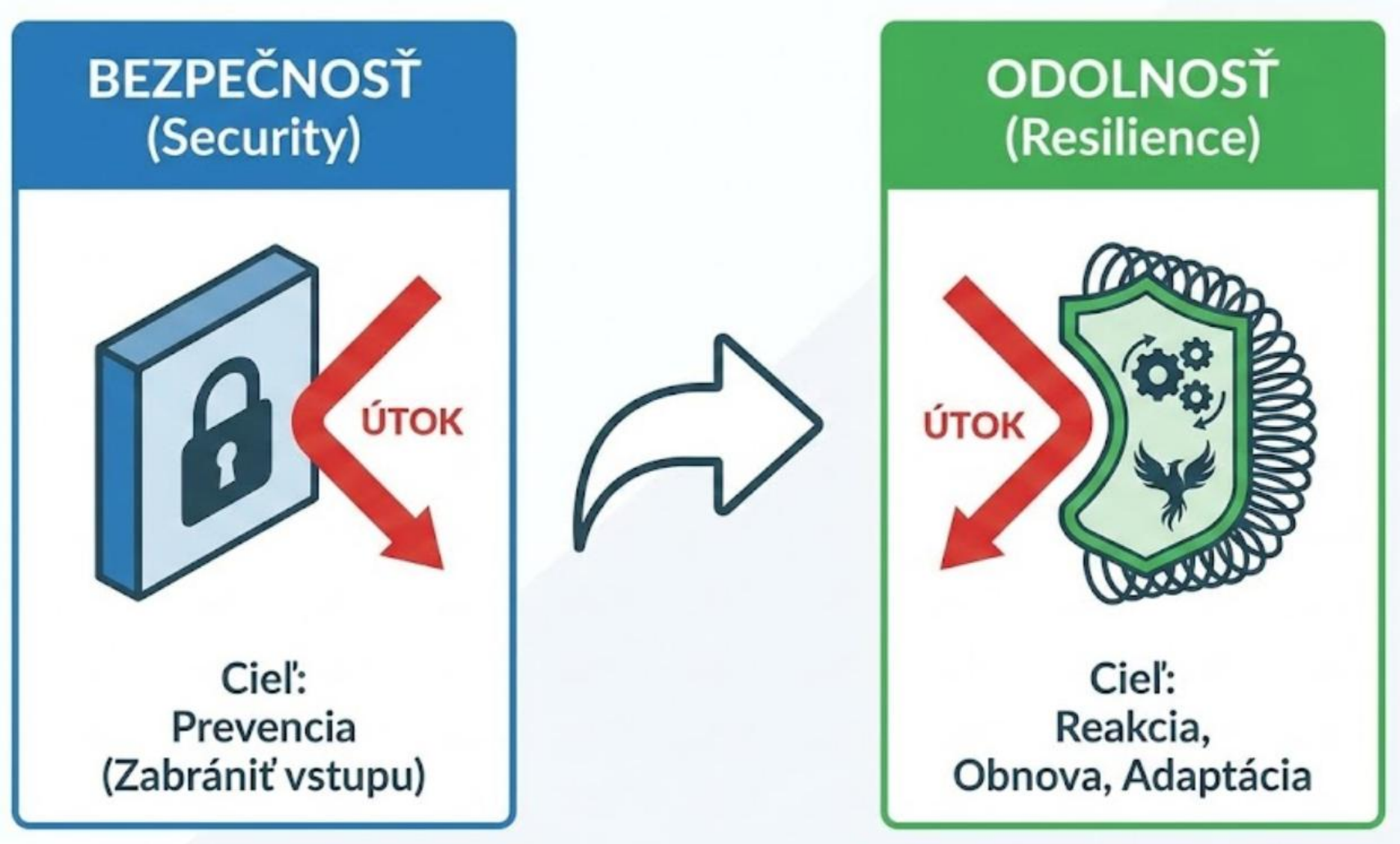
- **dôvernosť**
  - informácie prístupné len osobám, ktoré určíme
- **integrita**
  - informácie sú úplné a neboli nevedomky upravované
- **dostupnosť**
  - informácie prístupné na požiadanie týchto osôb v tom čase



ODOLNOSŤ VOČI KYBERNETICKÝM HROZBÁM

„Skutočná odolnosť nespočíva v tom, že zabránime každému útoku, ale v tom, ako rýchlo a efektívne sa dokážeme zotaviť.“

Odolnosť voči kybernetickým hrozbám (I.)



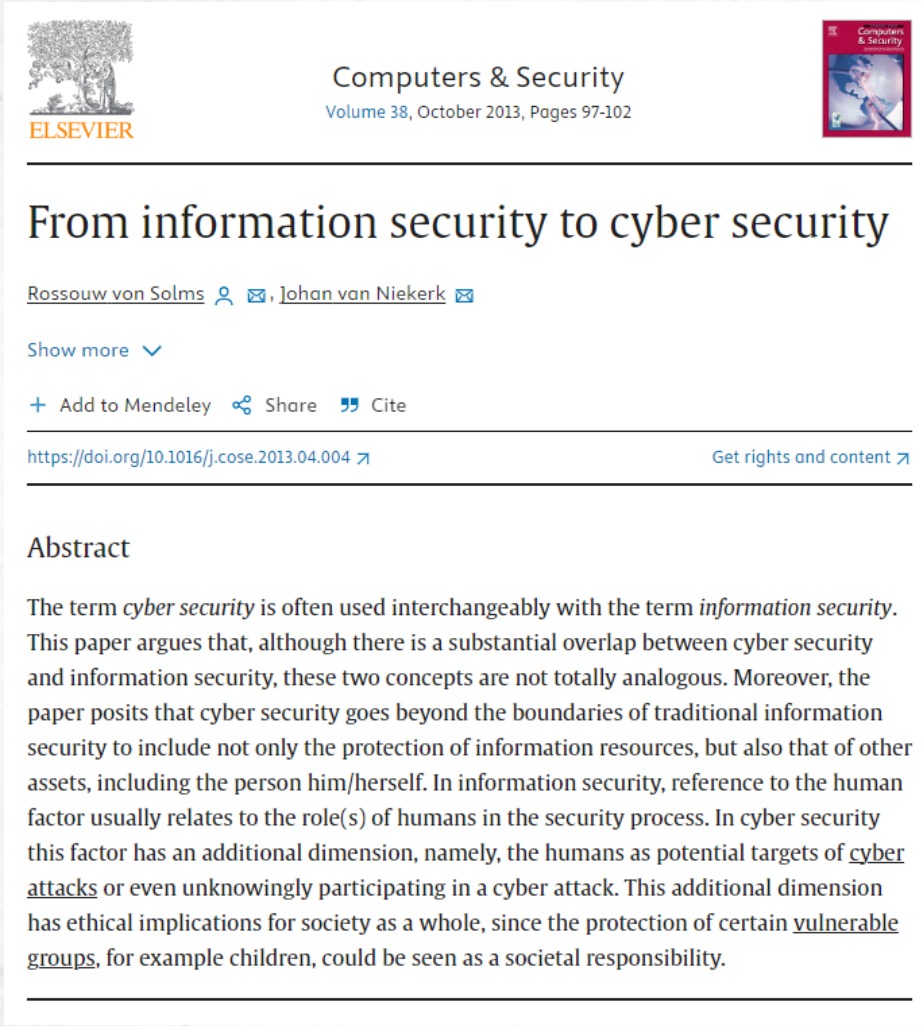
Zdroj: Vygenerované pomocou AI Google Gemini

Odolnosť voči kybernetickým hrozbám (II.)

- antivírusové programy (antimalvérová ochrana) mnohokrát rieši len známe kybernetické hrozby
- útočníci využívajú viacero spôsobov útoku (sociálne inžinierstvo, zneužitie zraniteľností, ...)
- spoliehať sa len na antimalvérové riešenie je ako zamknúť vchodové dvere, ale nechať otvorené okná.

Zdroj: Vygenerované pomocou AI Google Gemini

Informačná a kybernetická bezpečnosť (I.)



Computers & Security

Volume 38, October 2013, Pages 97-102

From information security to cyber security

Rossouw von Solms, Johan van Niekerk

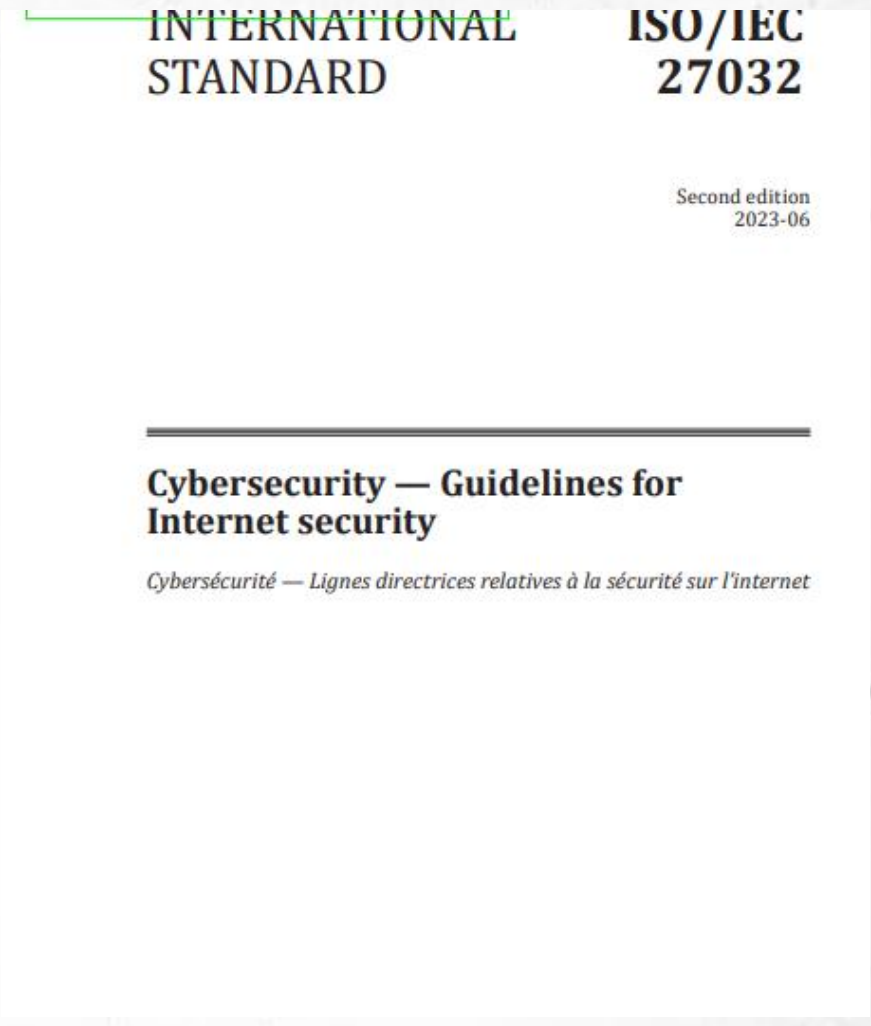
Show more

+ Add to Mendeley Share Cite

https://doi.org/10.1016/j.cose.2013.04.004 Get rights and content

Abstract

The term *cyber security* is often used interchangeably with the term *information security*. This paper argues that, although there is a substantial overlap between cyber security and information security, these two concepts are not totally analogous. Moreover, the paper posits that cyber security goes beyond the boundaries of traditional information security to include not only the protection of information resources, but also that of other assets, including the person him/herself. In information security, reference to the human factor usually relates to the role(s) of humans in the security process. In cyber security this factor has an additional dimension, namely, the humans as potential targets of cyber attacks or even unknowingly participating in a cyber attack. This additional dimension has ethical implications for society as a whole, since the protection of certain vulnerable groups, for example children, could be seen as a societal responsibility.



INTERNATIONAL STANDARD

ISO/IEC 27032

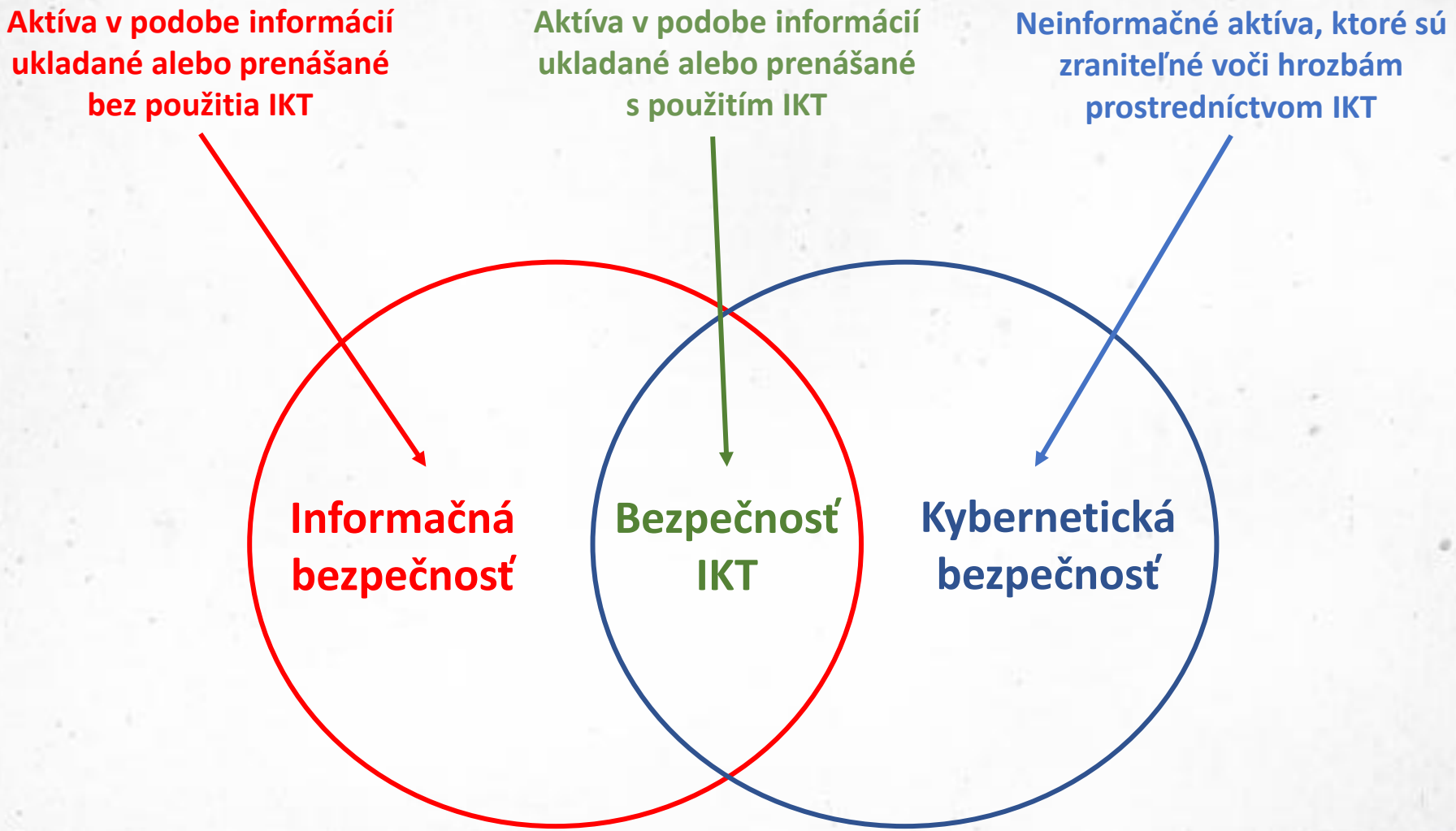
Second edition
2023-06

Cybersecurity — Guidelines for Internet security

Cybersécurité — Lignes directrices relatives à la sécurité sur l'internet

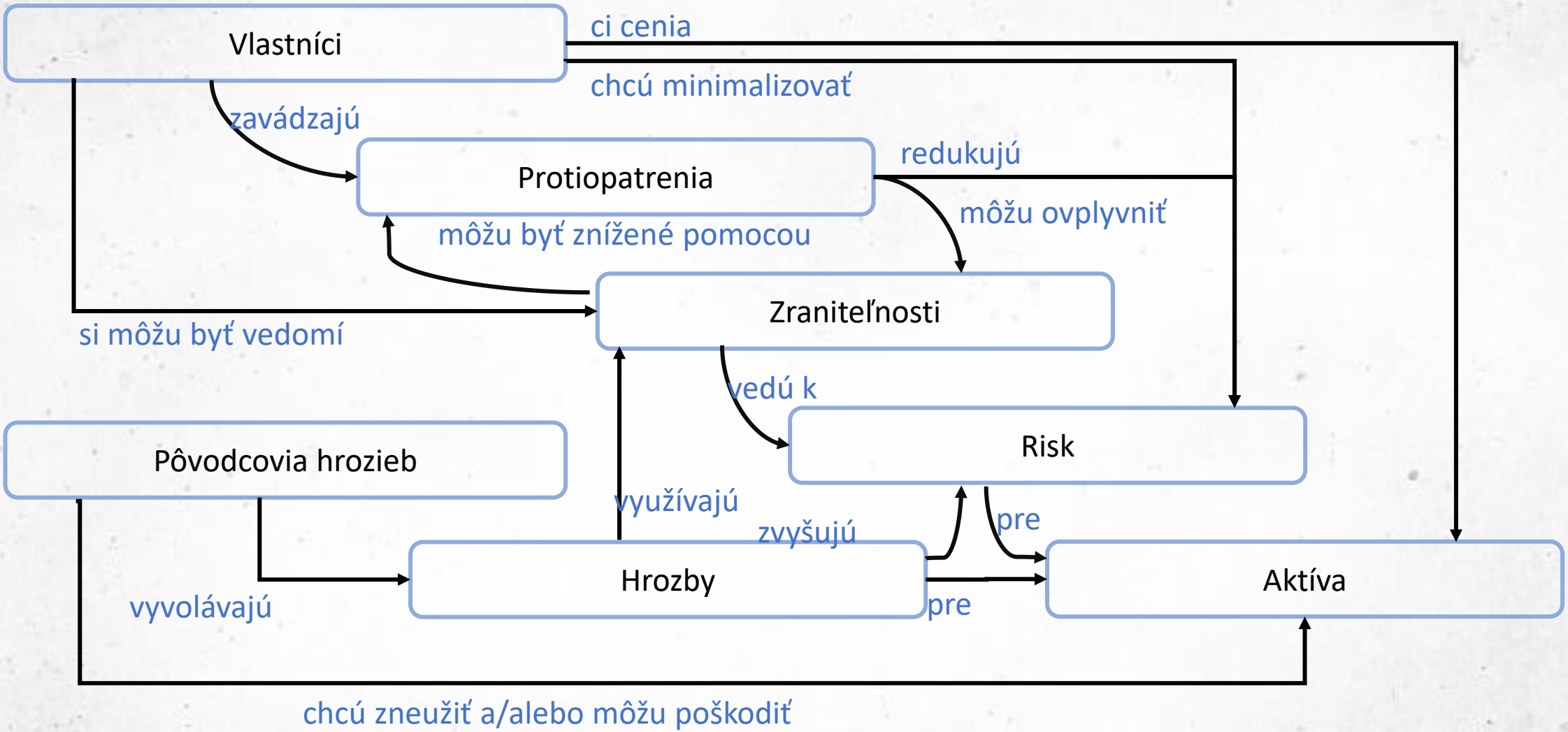
Zdroj: Von Solms, Rossouw, and Johan Van Niekerk. "From information security to cyber security." computers & security 38 (2013): 97-102.

Informačná a kybernetická bezpečnosť (II.)



Zdroj: Von Solms, Rossouw, and Johan Van Niekerk. "From information security to cyber security." computers & security 38 (2013): 97-102.

Model IB a KB


Vlastníci
ci cenia
chcú minimalizovať
zavádzajú
Protiopatrenia
redukujú
môžu ovplyvniť
môžu byť znížené pomocou
Zraniteľnosti
si môžu byť vedomí
vedú k
Risk
Pôvodcovia hrozieb
využívajú
zvyšujú
pre
Hrozby
Aktíva
vyvolávajú
pre
chcú zneužiť a/alebo môžu poškodiť

Aktívum

- **Aktívum (asset)** - všetky hmotné, ale aj nehmotné statky, všetko, čo má pre majiteľa systému určitú hodnotu.

  - **hardvér** – procesor, pamäť, terminály a pod.,
  - **softvér** – operačný systém, aplikačné programy a pod.,
  - **dáta** – dáta uložené v databázach, vstupné dáta, výstupné dáta a pod.
  - **ľudia** – užívatelia systému, administrátori, operátori a pod.

- **cena (hodnota)** aktíva
- najcennejšie aktíva - dáta a informácie, ktorých zneužitie, strata alebo modifikácia by organizácii alebo určitej osobe spôsobilo určitú škodu.

Hrozba (I.)

- čokoľvek (napríklad objekt, materiál, človek) čo je schopné pôsobiť proti aktívu takým spôsobom, že ich môže poškodiť.
- potenciálna príčina nežiaduceho incidentu (ISO/IEC 13335).

- Zdroje:
  - **A (accidental)** - náhodný zdroj - činnosti, ktoré môžu náhodne poškodiť informačné aktíva
  - **D (deliberate)** - úmyselný zdroj - úmyselné akcie zamerané na aktíva
  - **E (environmental)** - environmentálny zdroj

Hrozba (II.)

Zdroj: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats

Hrozba (III.)

Zdroj: ENISA Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Hrozba (IV.)

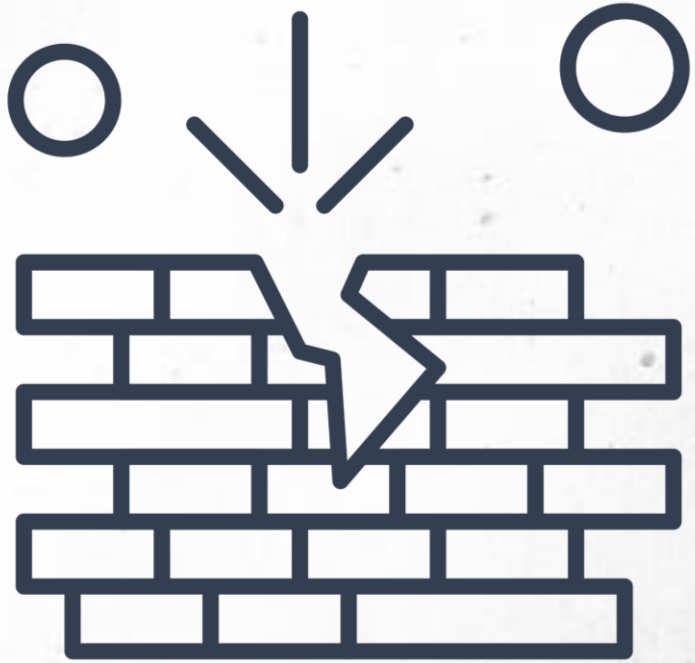
Zdroj: https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

Zraniteľnosť (I.)

- slabé miesto v oblasti vývoja, implementácie, prevádzky alebo vnútorného riadenia procesu, ktorá vplyvom udalostí hrozieb spôsobí stratu CIA alebo niektorého z aktív

- niečo, čo umožňuje hrozbe prejaviť sa

- priesečník 3 prvkov:
  - slabosť alebo chyba systému,
  - útočníkov prístup k chybe a
  - útočníkova schopnosť zneužiť chybu



Zraniteľnosť (II.)

CVE-2019-0708 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may resu
the information provided.

Current Description

A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when
attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services
Vulnerability'.

Source: MITRE

View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 9.8 CRITICAL
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3.0 legend)
Impact Score: 5.9
Exploitability Score: 3.9

CVSS v2.0 Severity and Metrics:

Base Score: 10.0 HIGH
Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C) (V2 legend)
Impact Subscore: 10.0
Exploitability Subscore: 10.0

Zdroj: https://nvd.nist.gov/vuln/detail/CVE-2019-0708

Útok (I.)

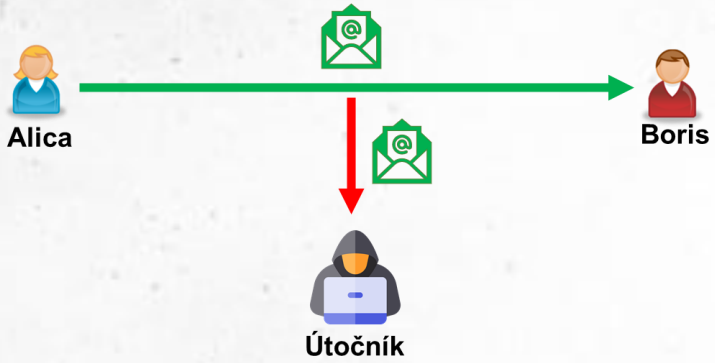
- pokus o zničenie, vystavenie hrozbe, zmenu, vyradenie z činnosti, odcudzeniu aktíva alebo získanie neoprávneného prístupu k aktívu alebo uskutočnenie neoprávneného použitia aktíva (ISO/IEC 27000: 2018)

- činnosti:
  - odpočúvanie (interception),
  - prerušenie (interruption),
  - modifikácia/úprava (modification)
  - výroba (fabrication)

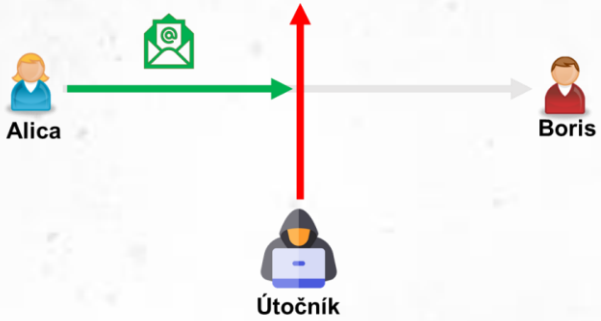
C	**Odpočúvanie**
I	**Prerušenie** **Modifikácia** **Výroba**
A	**Prerušenie** **Modifikácia** **Výroba**

Útok (II.)

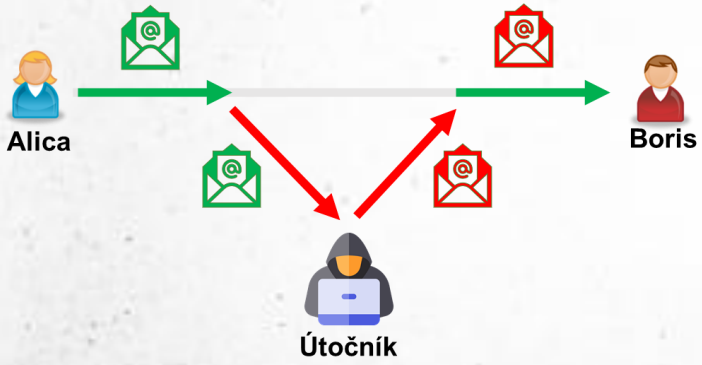
- odpočúvanie (interception)



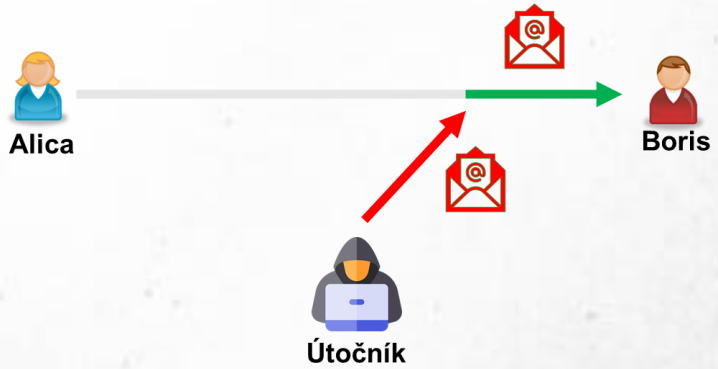
- prerušenie (interruption)



- úprava (modification):

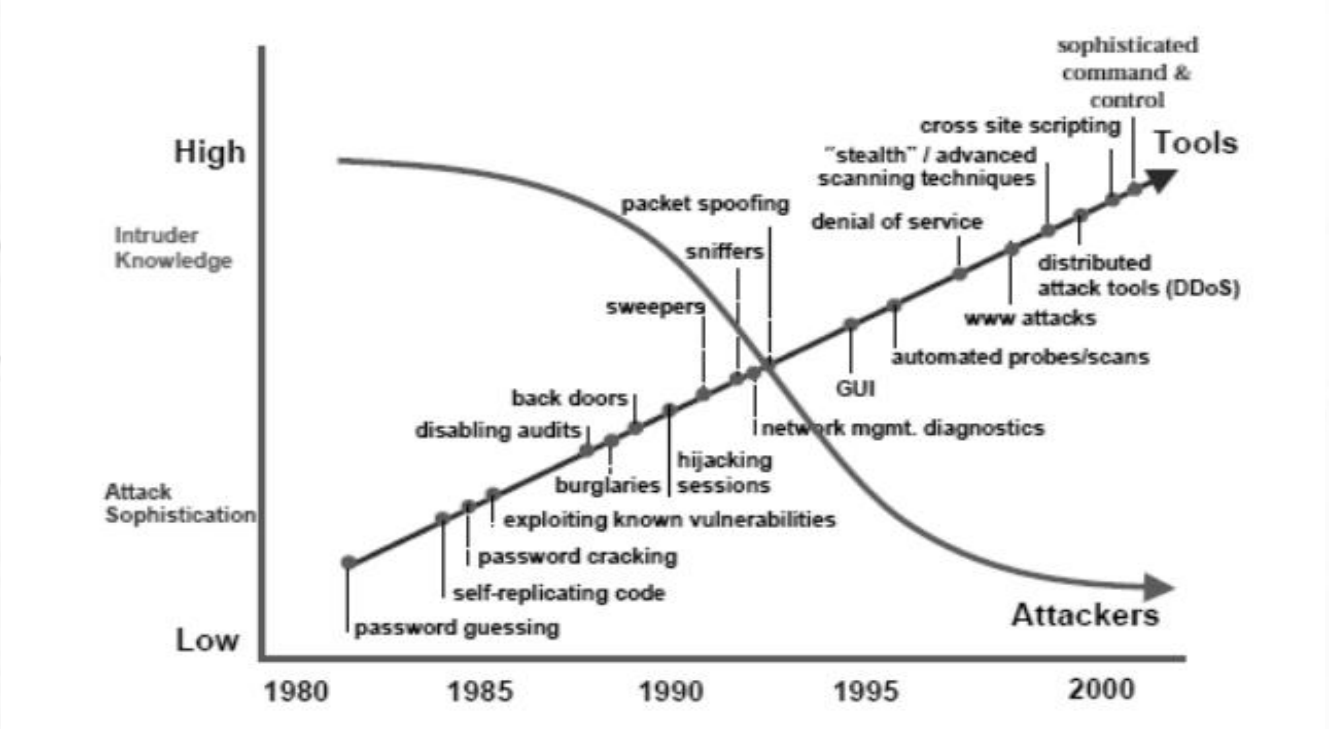


- výroba (fabrication)



Útočník (I.)

- jednotlivec, skupina, organizácia alebo vláda, ktorá vedie alebo má v úmysle vykonávať škodlivé činnosti (SP 800-30).



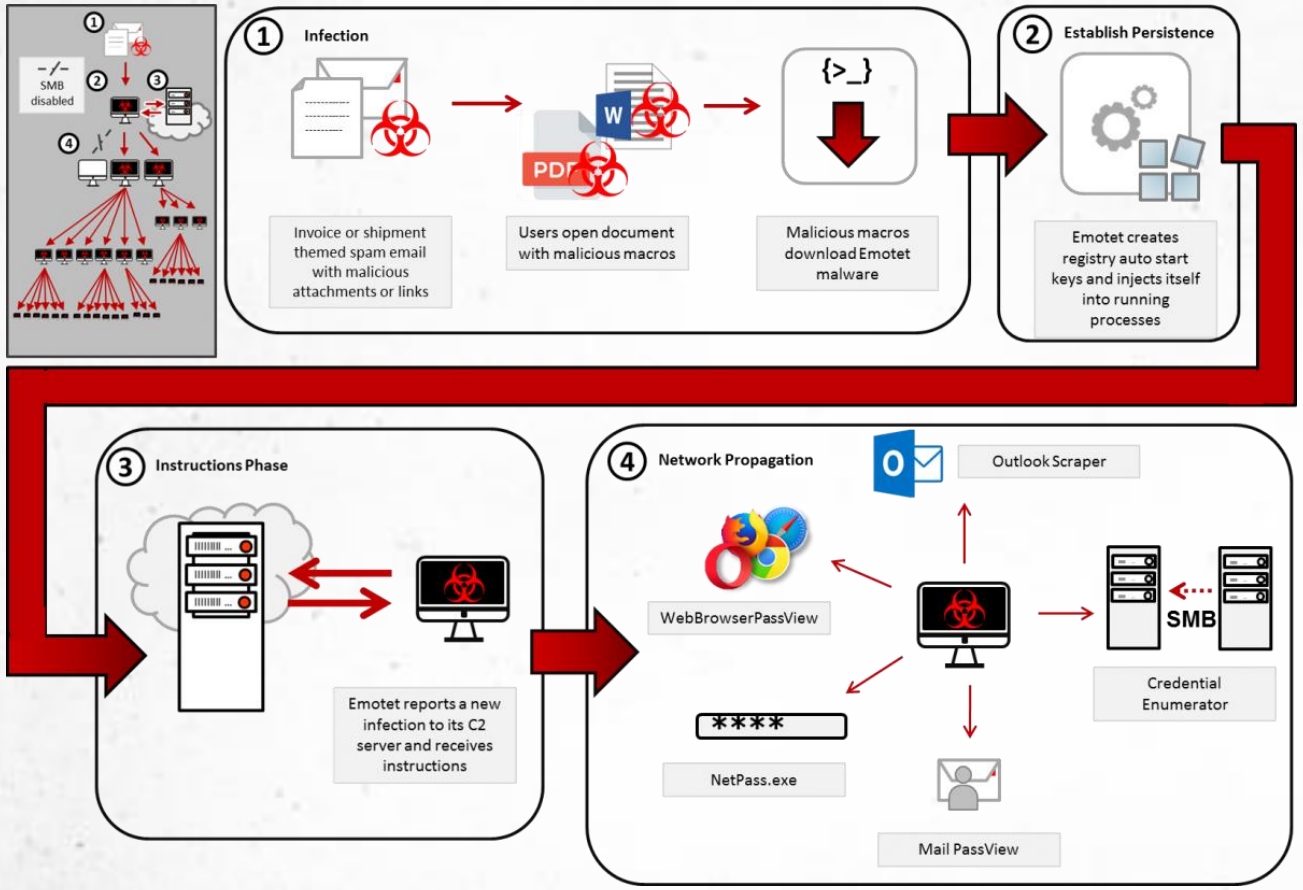
Zdroj: MEYERS, Carol; POWERS, Sarah; FAISSOL, Daniel. Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches. Lawrence Livermore National Laboratory (April 2009), 2009, 7: 1-22,

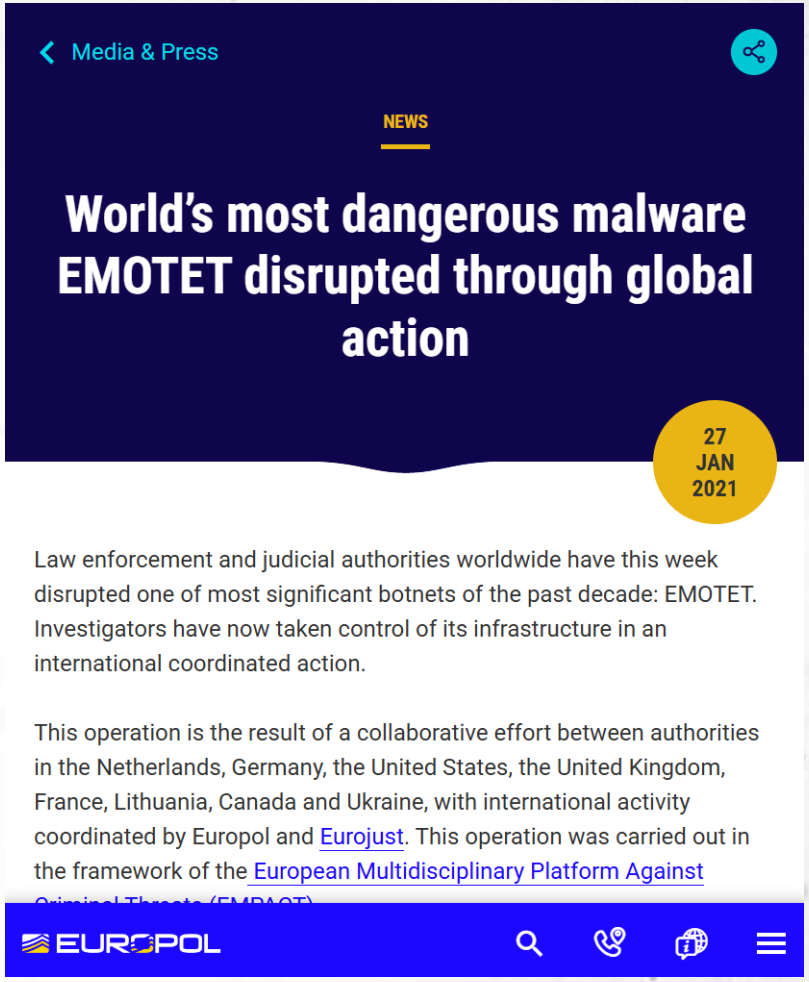
Útočník (II.)

- **Script Kiddies** - nekvalifikovaný heker, ktorý kompromituje systém spustením skriptov, nástrojov a softvéru vyvinutého skutočnými hackermi
- **Organizovaní hackeri** - profesionálni hackeri, ktorí sa snažia zaútočiť na systém so ziskom
- **Hacktivisti** - jednotlivci, ktorí hackovaním propagujú politickú agendu, najmä poškodzovaním alebo deaktivovaním webových stránok
- **Útočníci sponzorovaní štátom** - jednotlivci zamestnaní vládou, aby prenikli a získali prísne tajné informácie alebo poškodili informačné systémy iných vlád
- **Insider Threat** - hrozba pochádzajúca od ľudí v organizácii, môžu to byť nespokojní zamestnanci, prepustení zamestnanci a nedostatočne školení zamestnanci

Útočník (III.)

- **Emotet** - modus operandi





Zdroj: https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action, https://www.cisecurity.org/

Riziko (I.)

- úroveň vplyvu na organizačné operácie (vrátane cieľov, funkcie, alebo povesti), organizačné aktíva alebo jednotlivcov vyplývajúce z prevádzkovania informačného systému so zreteľom na potenciálny dopad hrozby a pravdepodobnosť, že sa táto hrozba vyskytne (FIPS 200).

- KB a IB založená na analýze rizík

- denno-denná analýza rizík

Zdroj: http://www.securityinfowatch.com/blog/11288612/vidsys-2013-national-security-survey-shows-risk-becoming-a-bigger-priority-for-c-level-executives

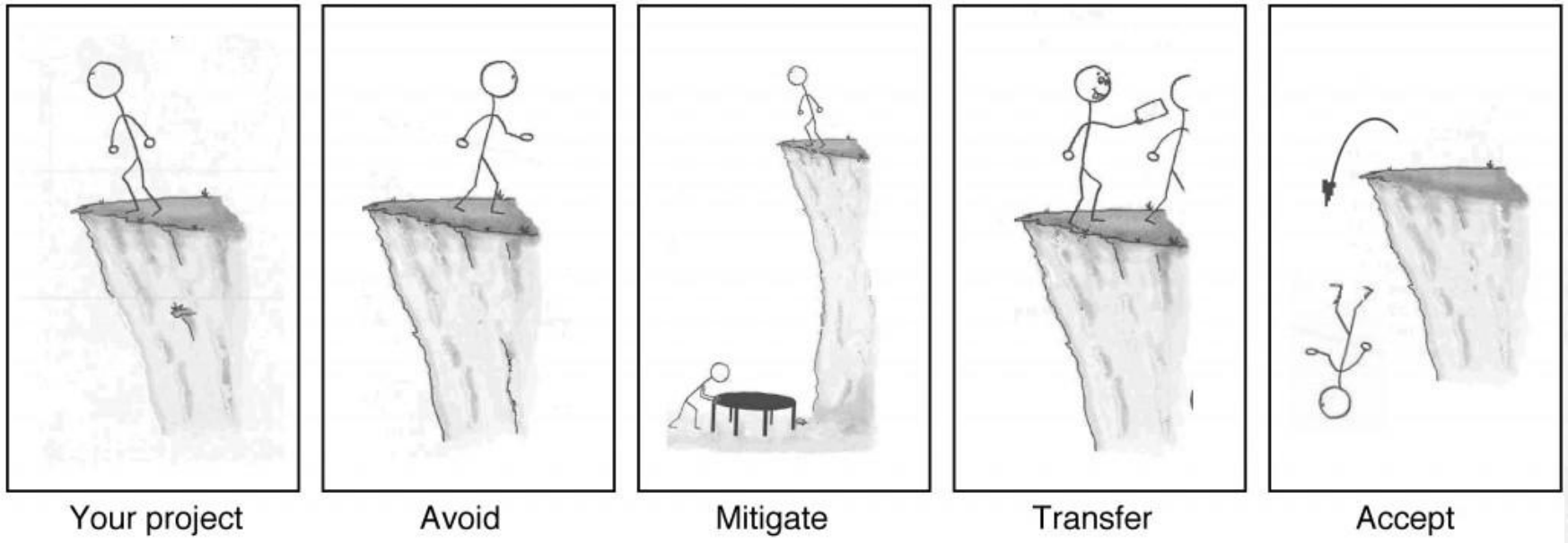
Riziko (II.)

Vyjadrenie rizika (kvalitatívny prístup)

Dopad → Pravdepodobnosť ↓	nízky	stredný	Vysoký
Nulová	Nulové	Nulové	Nulové
Nízka	Nízke	Nízke	Stredné
Stredná	Nízke	Stredné	Vysoké
Vysoká	Stredné	Vysoké	Vysoké

Riziko (III.)

- Akceptovanie/Zachovanie rizika (Accept)
- Vyhnutie sa riziku (Avoid)
- Limitácia/Zníženie rizika (Mitigate / Limit)
- Presun rizika (Transfer)

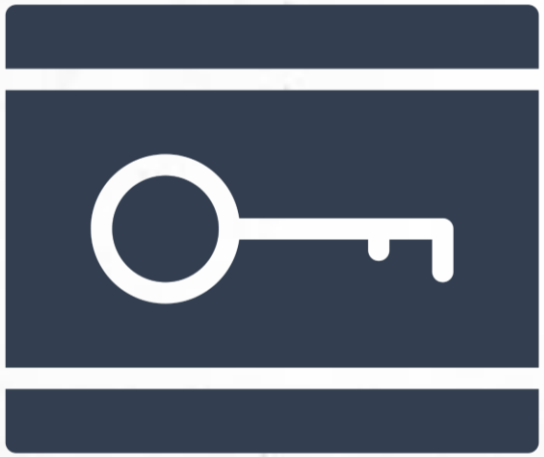


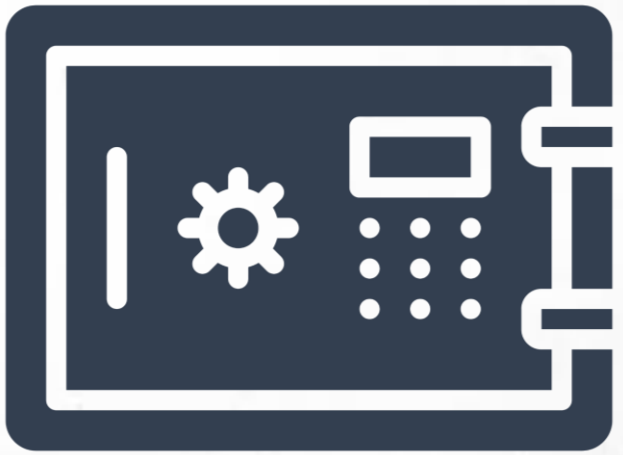
Zdroj: http://cnx.org/content/col11120/1.4/

Bezpečnostné opatrenia (I.)

- akákoľvek činnosť, technické zariadenie, proces, mechanizmus, alebo čokoľvek, čo chráni informačný systém a jeho časti (aktíva) pred pôsobením konkrétnych hrozieb alebo hrozby.

- **Administratívne** – napr. politiky, odporúčania, štandardy
- **Fyzické** – napr. uzamykateľné dvere, náhradný zdroj napájania
- **Logické** – napr. heslá, firewally, prístupové zoznamy





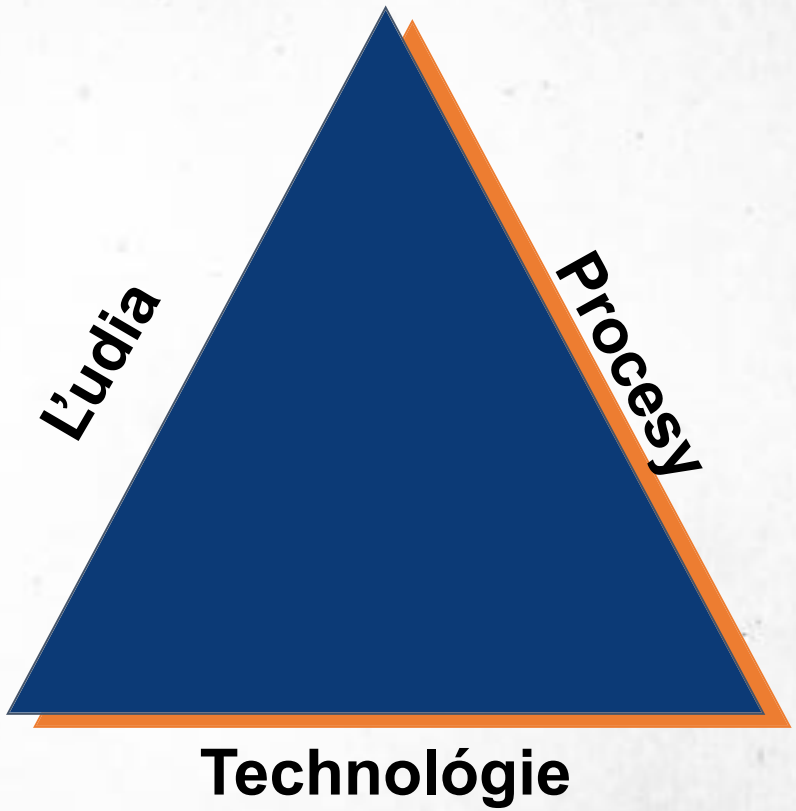
Bezpečnostné opatrenia (II.)

§ 20 ods. 2 Zákona o KB: Bezpečnostné opatrenia sa prijímajú a realizujú najmä pre oblasť

a) organizáciu a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti,
b) správu zraniteľností a kybernetických hrozieb,
c) správu aktív a riadenie kybernetických hrozieb a rizík,
d) riadenie udalostí a kybernetických bezpečnostných incidentov,
e) riadenie kontinuity činností, zálohovanie, obnovu systémov po havárii a krízové riadenie,
f) bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií,
g) postupy posudzovania účinnosti opatrení, riadenie súladu a kontrolné činnosti,
h) kryptografické opatrenia a zásady používania kryptografie,
i) bezpečnosť a spôsobilosti ľudských zdrojov,
j) správu identít a prístupov,
k) bezpečnosť pri prevádzke sietí a informačných systémov,
l) ochranu proti škodlivému kódu a nežiaducemu obsahu,
m) systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť,
n) monitorovanie, zaznamenávanie a hlásenie udalostí,
o) fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení,
p) ochranu záznamov, súkromia a označovanie informácií,
q) dodávateľský reťazec,
r) obstarávanie a využívanie certifikovaných produktov IKT, služieb IKT a procesov IKT.

Mýtus – KIB je jednorazový projekt

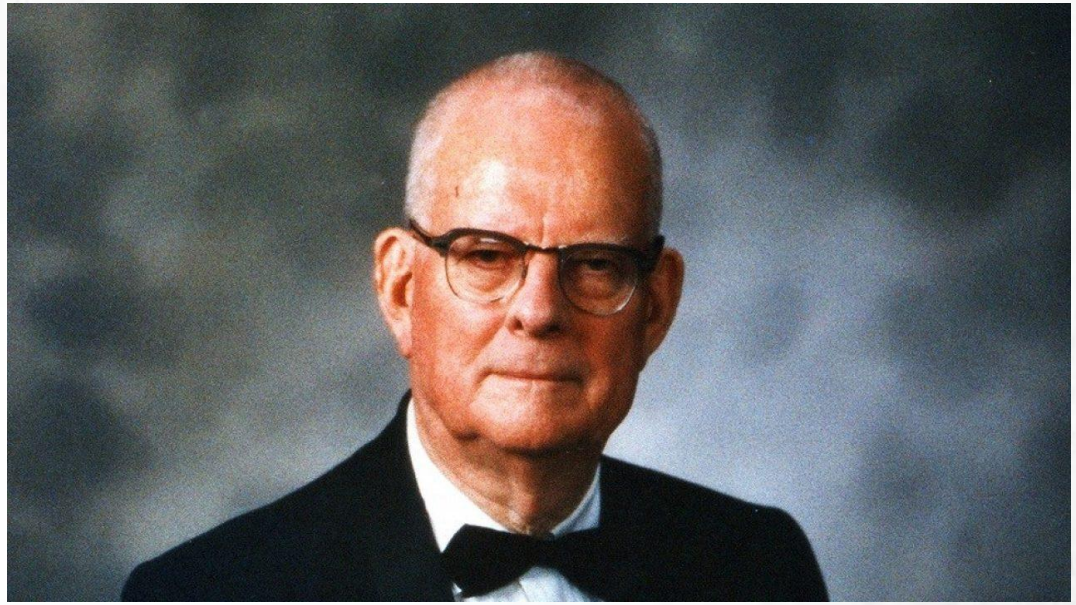
- Kybernetická a informačná bezpečnosť je neustály **proces**, nie stav
- ide o prepojenie procesov, ľudí a technológií
- **Proces** – súbor vzájomne súvisiacich alebo vzájomne pôsobiacich činností
- **Organizácia** – musí efektívne riadiť veľké množstvo previazaných procesov



Riadenie procesov (I.)

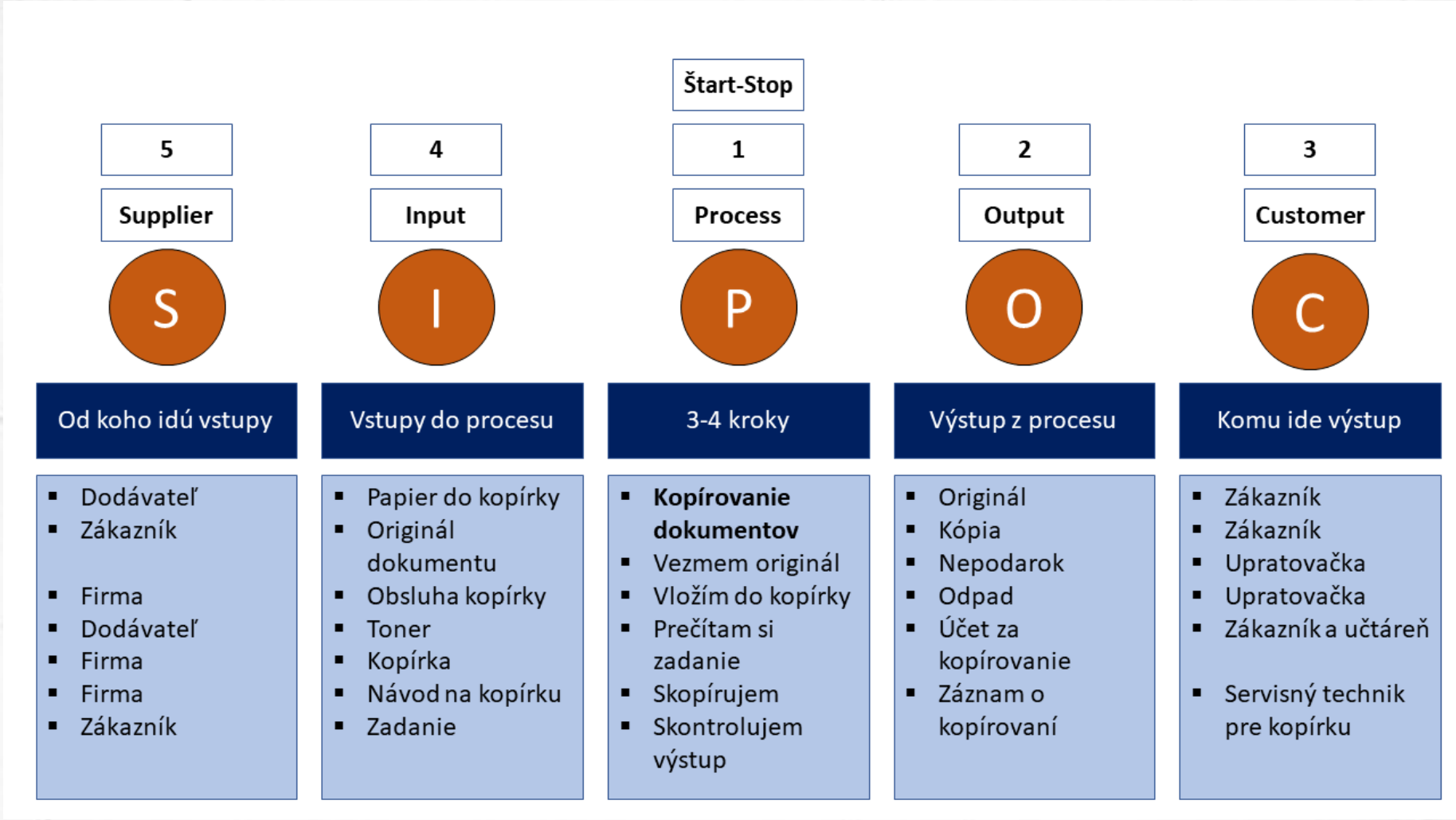
Ak **nedokážeš opísať to, čo robíš, ako proces, potom nevieš, čo vlastne robíš.**

— *W. Edwards Deming*



Zdroj: https://history-biography.com/william-deming/

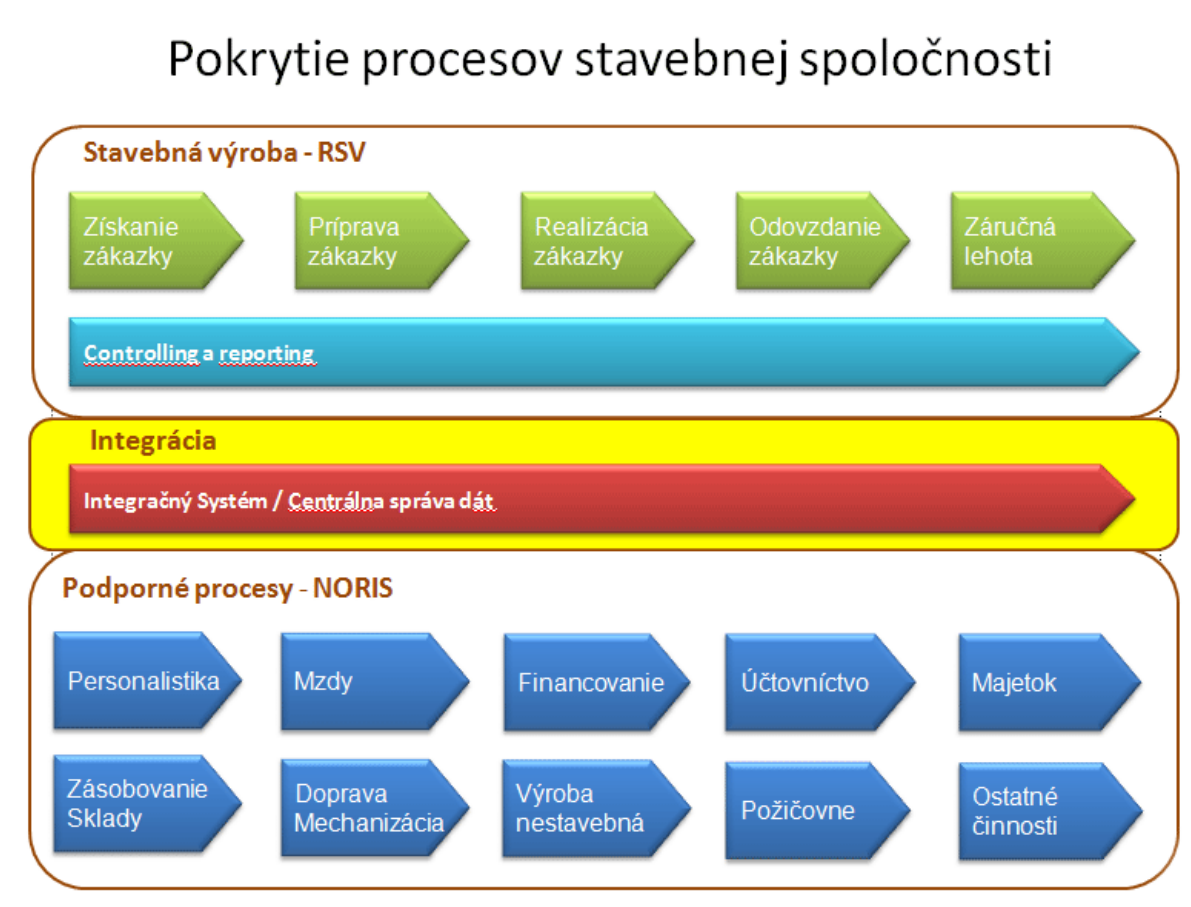
Riadenie procesov (II.)



Zdroj: https://www.cems.sk/clanok/211-sipoc-analyza

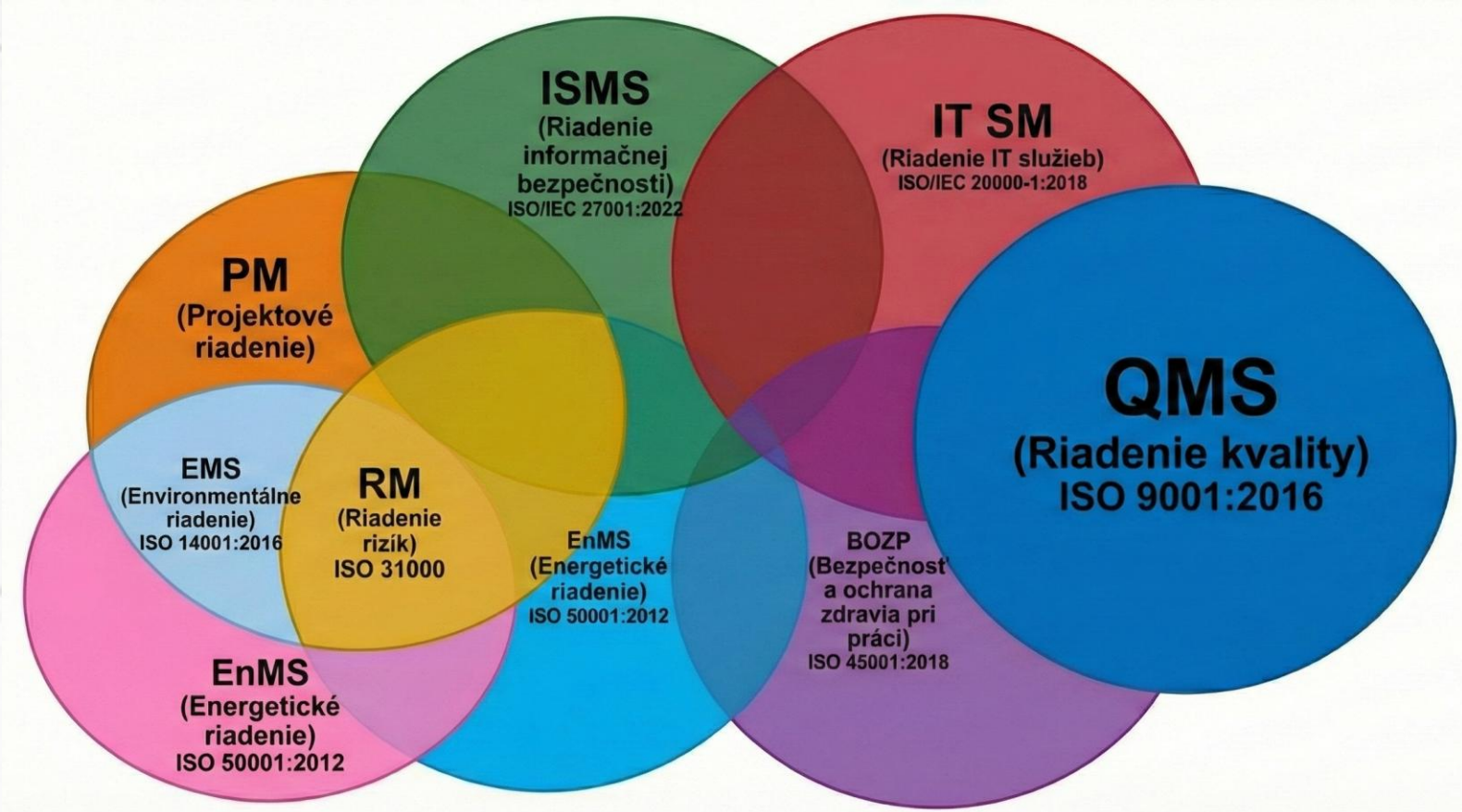
Riadenie procesov (III.)

- hlavné procesy / podporné procesy
- príklad procesov



Zdroj: https://www.noris.sk/stavebnictvo/

Riadenie procesov (IV.)



Zdroj: Vygenerované pomocou AI Google Gemini

Riadenie procesov (V.)

ISMS (Information Security Management System) - systém riadenia informačnej bezpečnosti

- systematický a riadený súbor politík, procesov, postupov, rolí a technických i organizačných opatrení, ktorého cieľom je zabezpečiť ochranu informácií v organizácii so zameraním najmä na triádu CAI.

ISMS umožňuje organizácii:

- identifikovať a hodnotiť riziká informačnej bezpečnosti,
- navrhovať a uplatňovať primerané bezpečnostné opatrenia,
- priebežne monitorovať, preskúmavať a zlepšovať úroveň informačnej bezpečnosti,
- zabezpečiť súlad s legislatívnymi a zmluvnými požiadavkami

Technické normy / štandardy (I.)

- Mýtus: bezpečnostné hrozby a bezpečnostné opatrenia sú záležitosťou posledných rokov
- povinnosť venovať sa informačnej a kybernetickej bezpečnosti bola už predtým
- rok 2000 - ISO/IEC 17799:2000
- rok 2022 - ISO/IEC 27002:2022

Zdroj: https://advisera.com/27001academy/explanation-of-11-new-iso-27001-2022-controls/

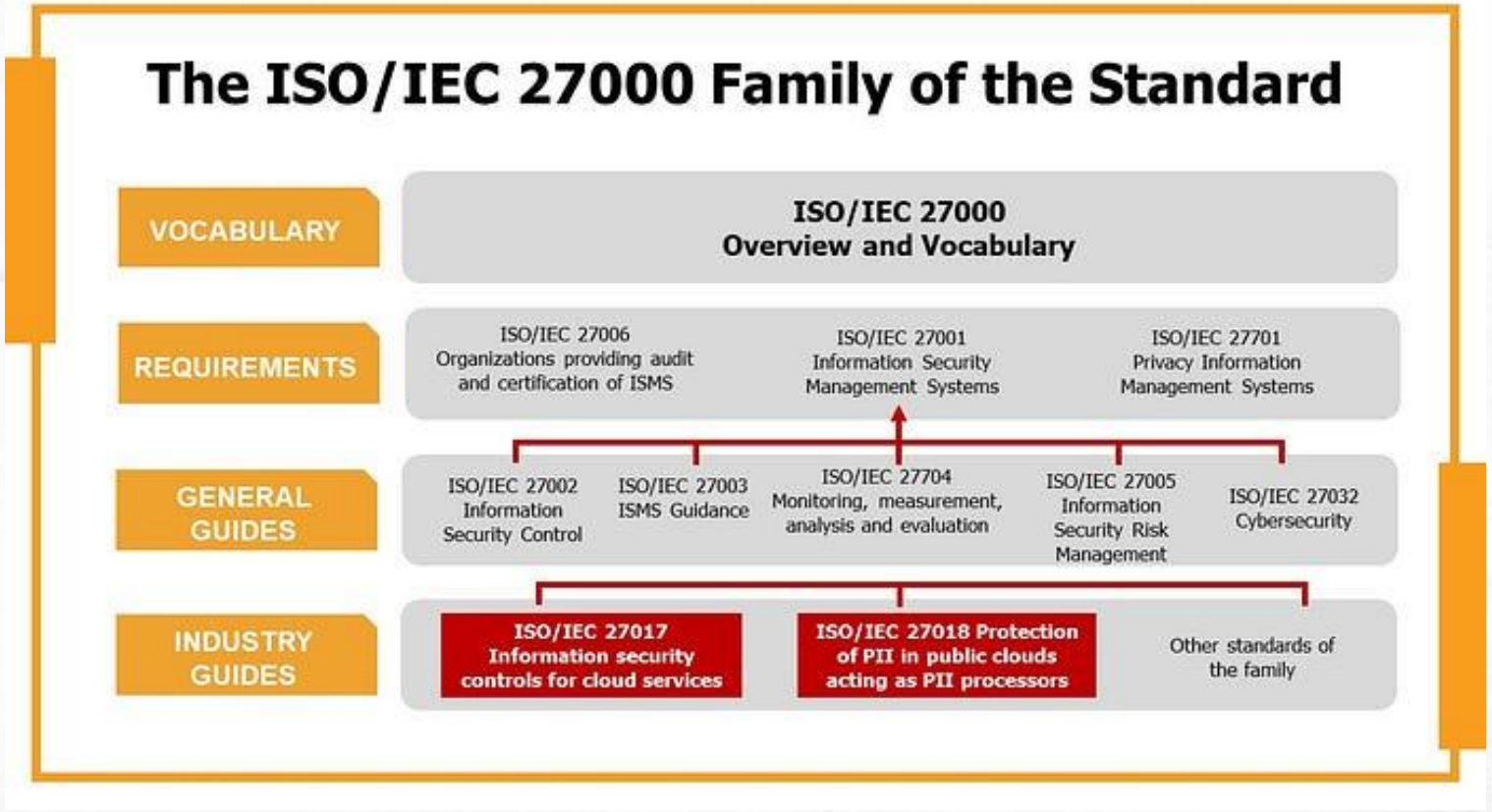
Technické normy / štandardy (II.)

- Technická norma je dokumentom s odporúčaniami, ktorý je možné využiť niekoľkými spôsobmi:
  - súhrn záväzných pravidiel, podľa ktorého sa dá nastaviť kvalita alebo bezpečnosť systému.
  - súhrn pravidiel, ktoré dodržiavajú výrobcovia systémov, pričom norma sa dá použiť na porovnanie kvality systémov.

Technické normy / štandardy (III.)

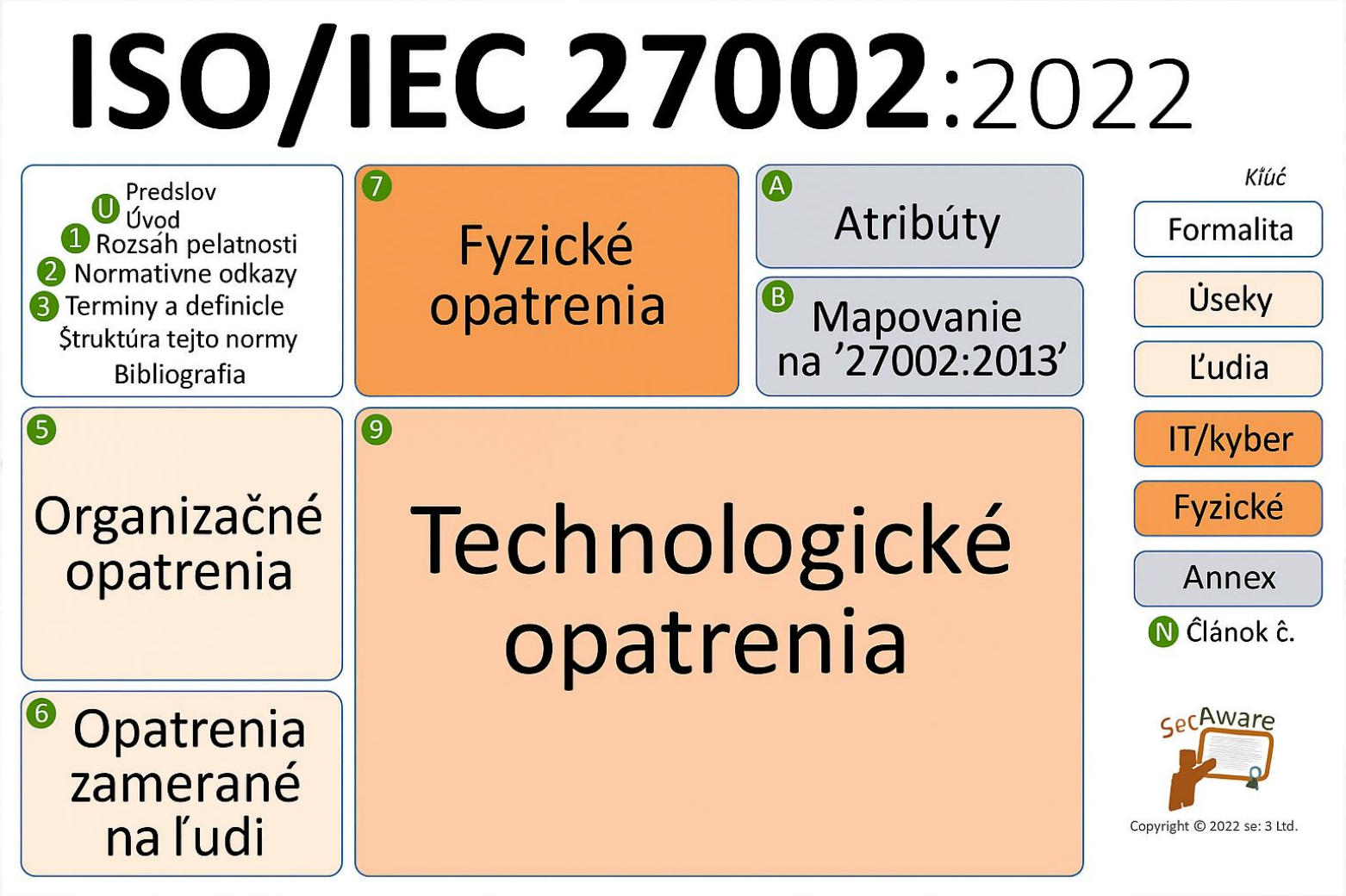
ISO/IEC 27000

- medzinárodné štandardy v oblasti riadenia informačnej bezpečnosti
- založené na britských štandardoch rady BS 7799



Zdroj: https://cfecertification.medium.com/the-iso-iec-27000-family-of-standards-2f04697f2e82

Technické normy / štandardy (IV.)



Zdroj: https://www.iso27001security.com/html/27002.html

Technické normy / štandardy (V.)

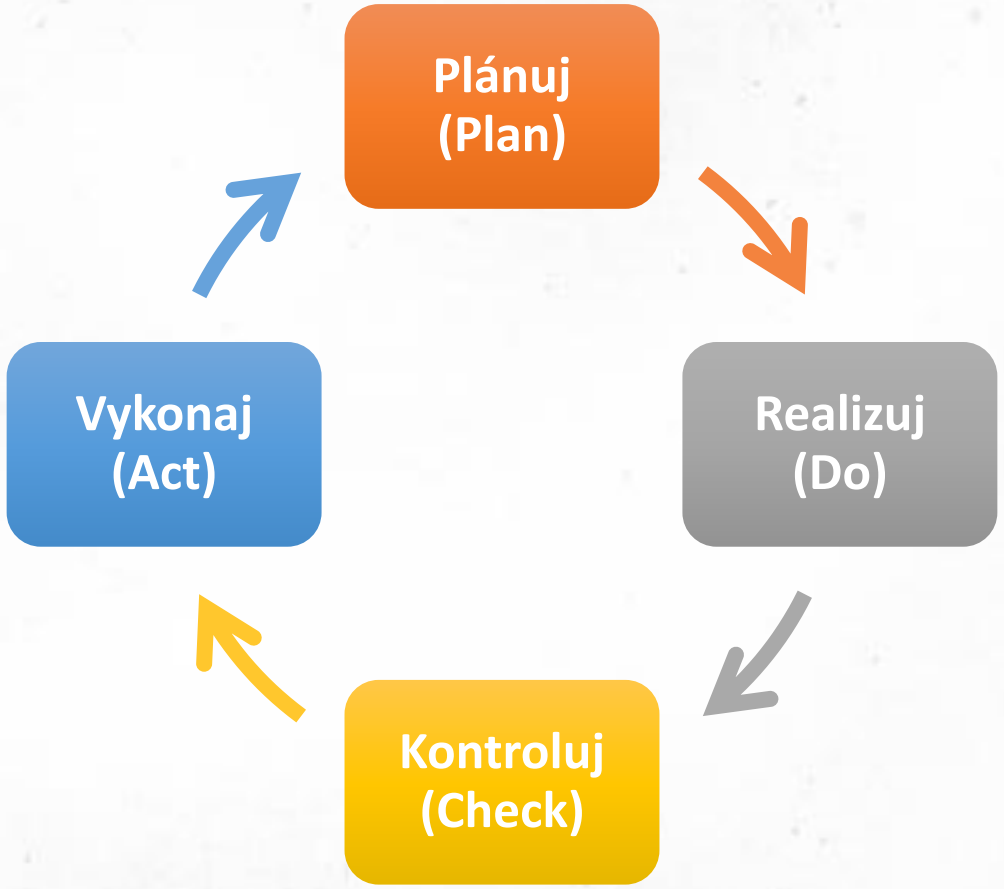
- ISO/IEC 27000 – Information security, cybersecurity and privacy protection — Information security management systems — Overview and vocabulary
- ISO/IEC 27001 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27002 – Information security, cybersecurity and privacy protection — Information security controls
- ISO/IEC 27005 – Information security, cybersecurity and privacy protection — Guidance on managing information security risks
- ISO/IEC 27007 – Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

Technické normy / štandardy (VI.)

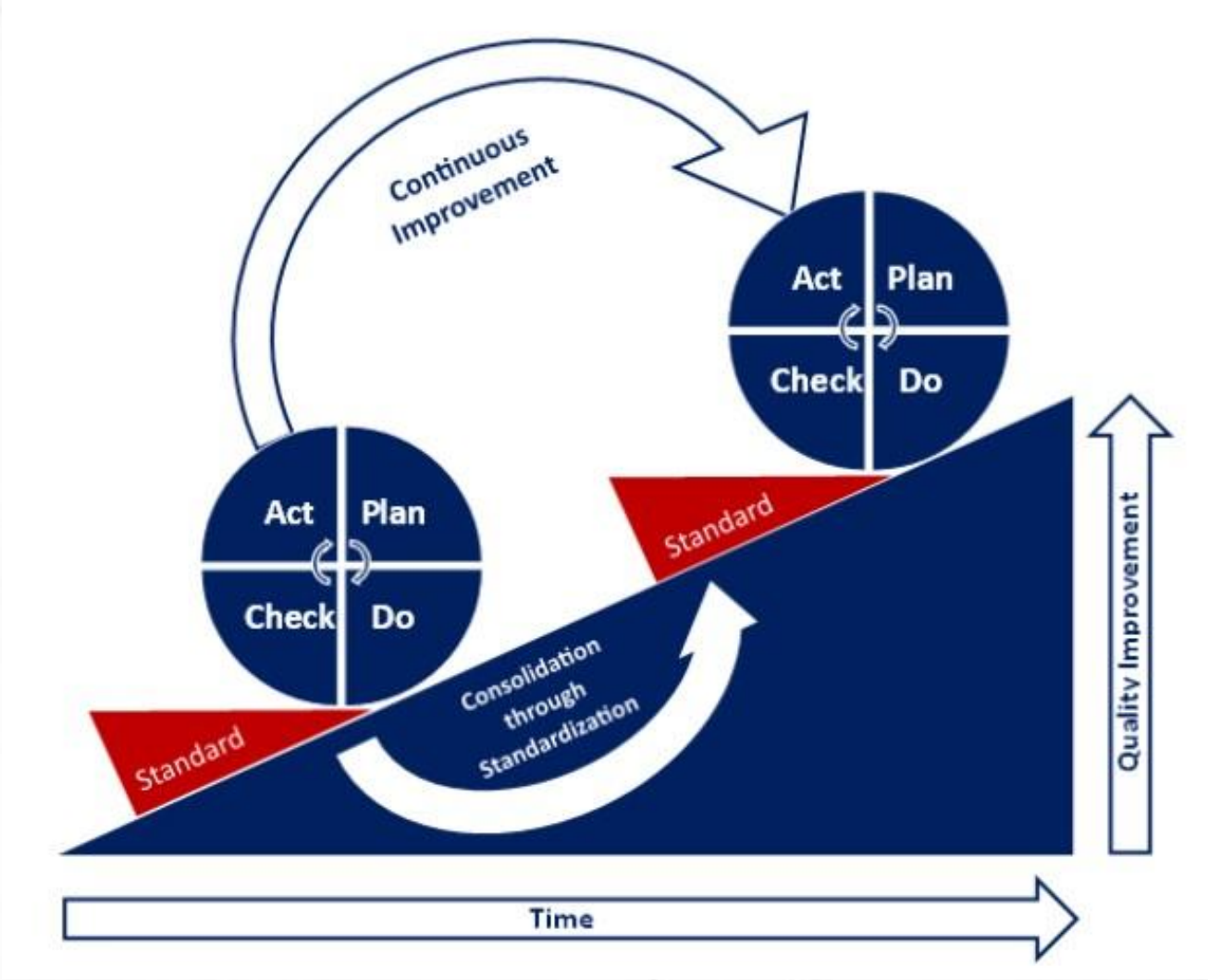
- ISO/IEC 27035 – Information security, cybersecurity and privacy protection — Information security incident management
- ISO/IEC 27031 – Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 27017 – Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27019 – Information security, cybersecurity and privacy protection — Information security controls for the energy utility industry
- ISO/IEC 42001 – Information technology — Artificial intelligence — Management system

PDCA model (I.)

- možný spôsob zavedenia ISMS do organizácie - **Model PDCA** (plan–do–check–act)
- **W. Edwards Deming**



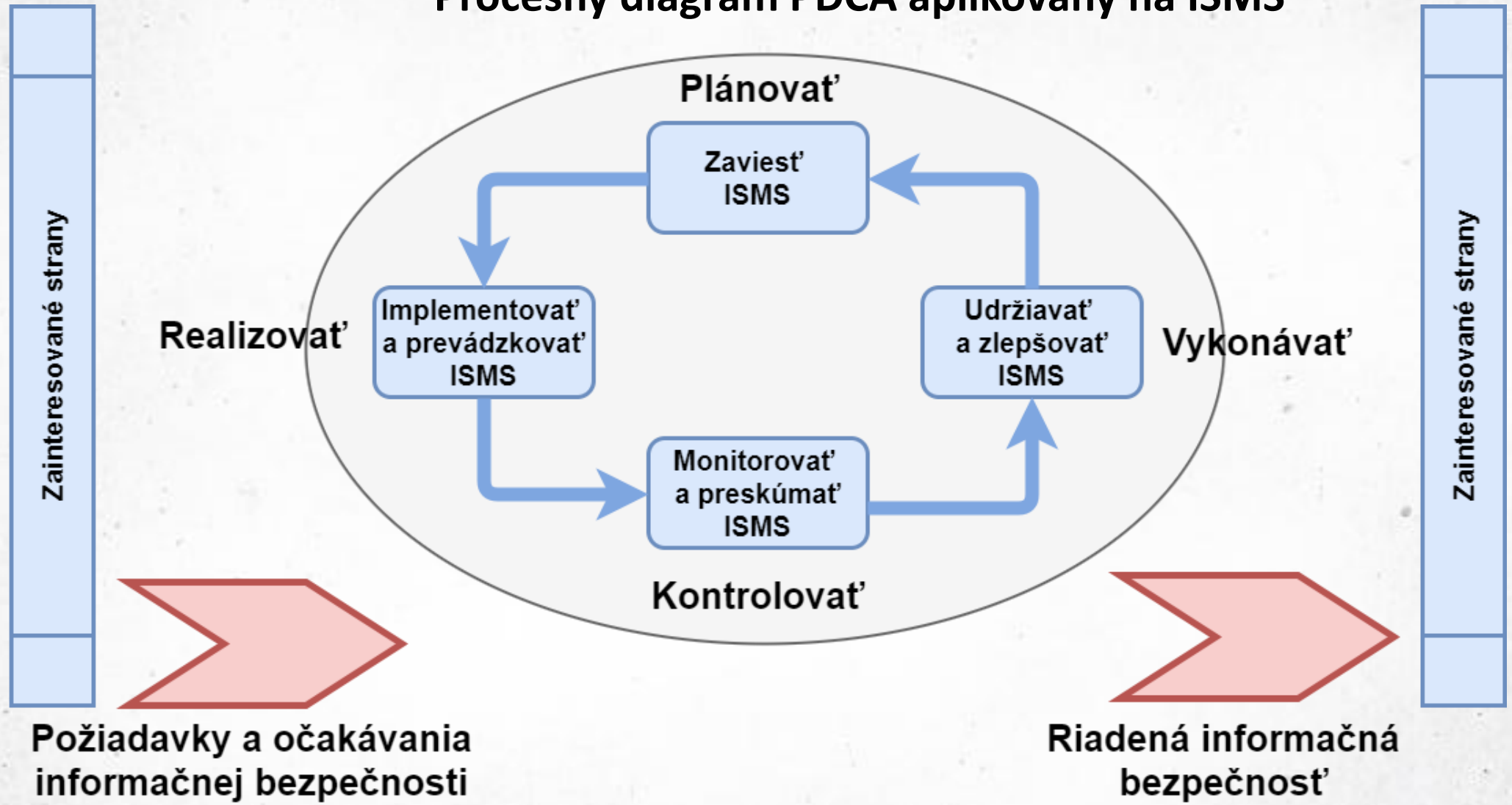
PDCA model (II.)



Zdroj: https://www.leanairline.com/blog/standardized-work

PDCA model (III.)

Procesný diagram PDCA aplikovaný na ISMS



Zavedenie ISMS (I.)

- **Činnosti:**
  1) Definícia rozsahu, hraníc a väzieb ISMS
  2) Definícia a odsúhlasenie Prehlásenia o politike ISMS
  3) Analýza a zvládanie rizík
  4) Súhlas vedenia organizácie s navrhovanými opatreniami pre zvládanie rizík
  5) Príprava Prehlásenia o aplikovateľnosti

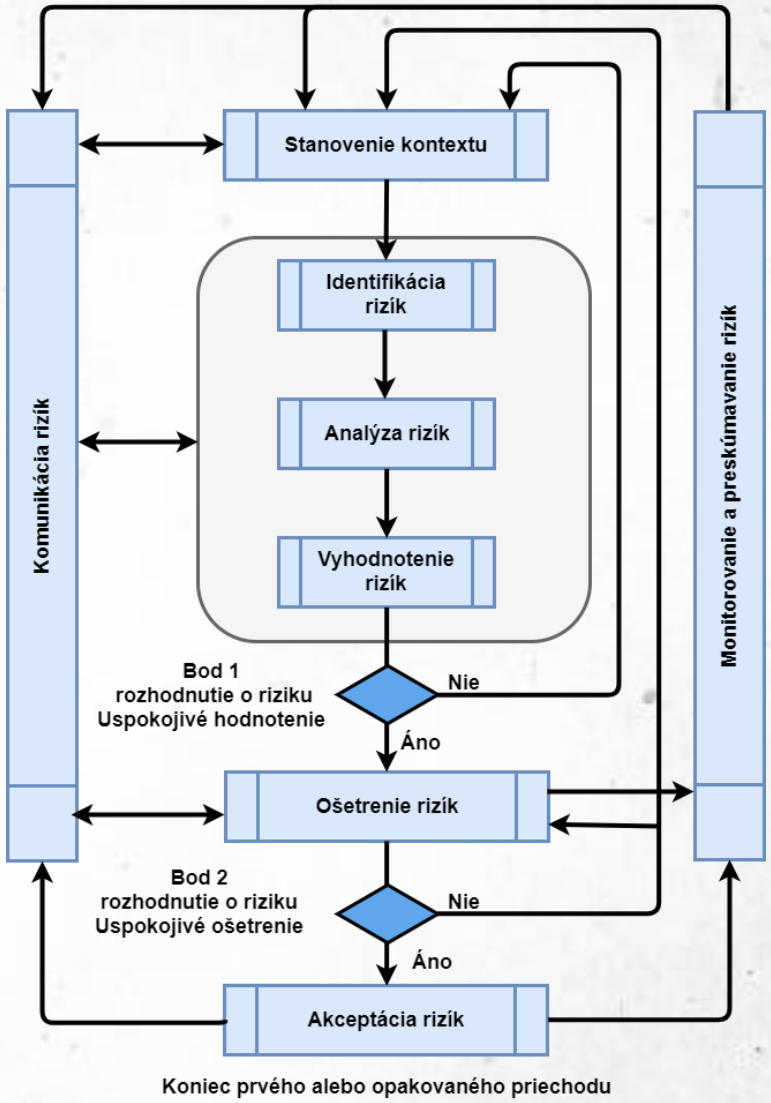
- ISO/IEC 27001:2022 a ISO/IEC 27002:2022

Zavedenie ISMS (II.)

Analýza rizík

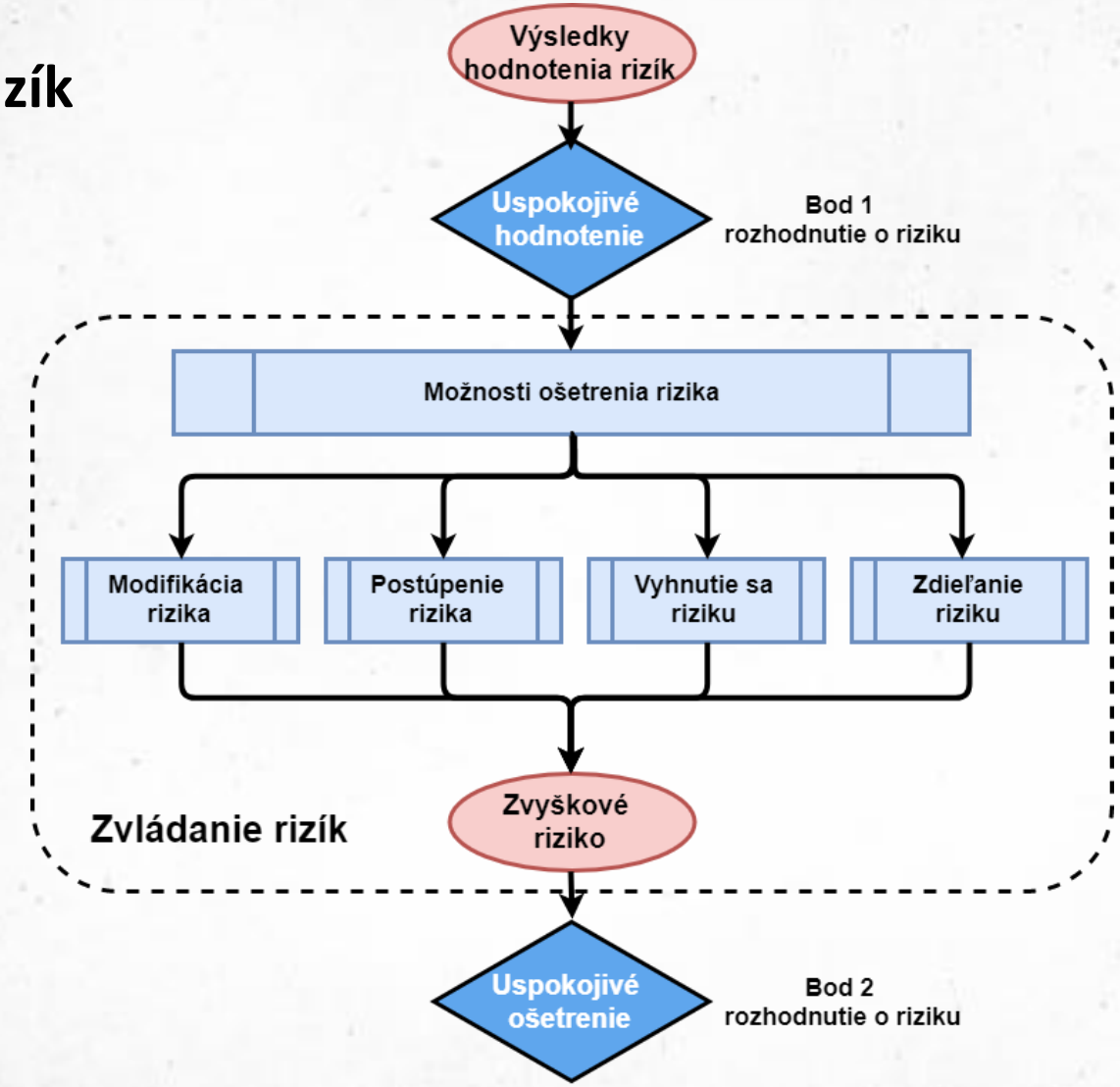
- Metodika analýzy rizík kybernetickej bezpečnosti pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z.´z. o kybernetickej bezpečnosti

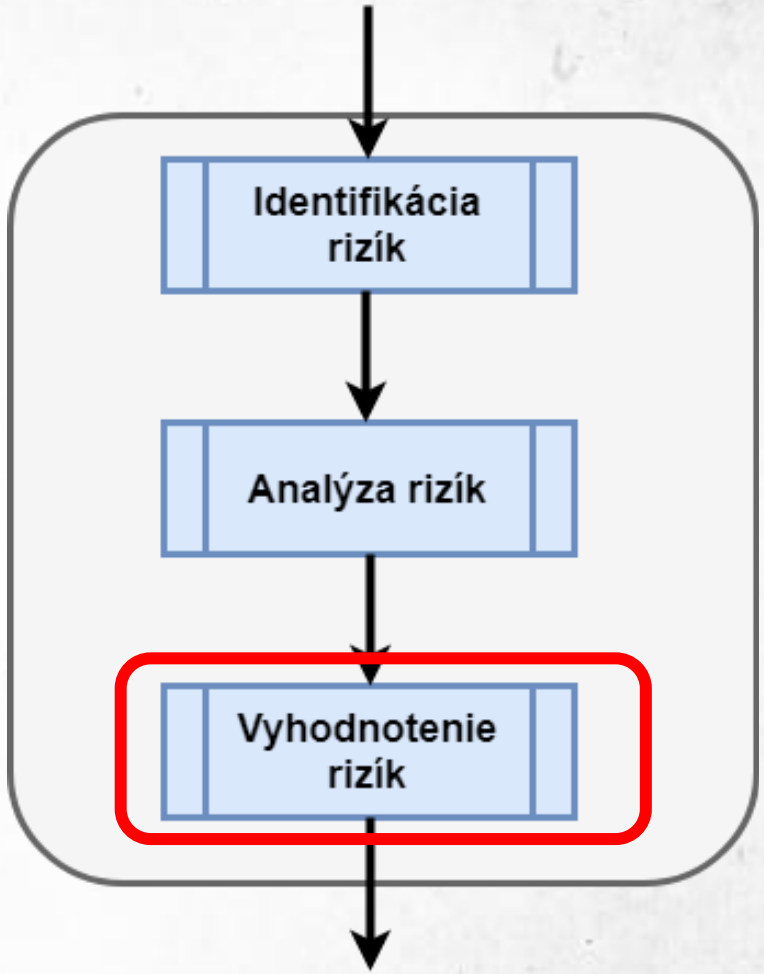
- ISO/IEC 27005:2022 Informačné technológie – Bezpečnostné metódy – Riadenie rizík informačnej bezpečnosti



Zavedenie ISMS (III.)

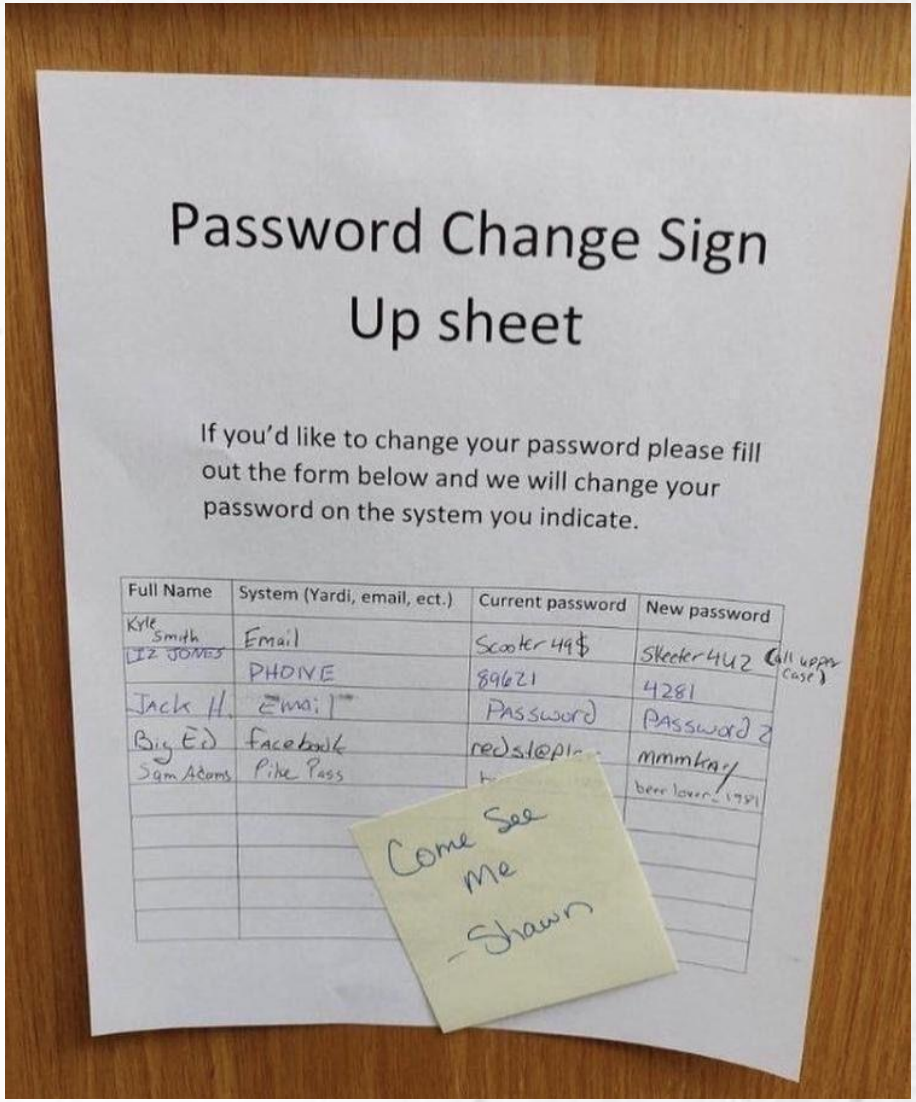
- **Zvládanie rizík**





Implementácia a prevádzka ISMS (I.)

- formulovať plán ošetrovania rizík
- implementovať plán ošetrovania rizík
- implementovať opatrenia na splnenie cieľov riadenia;
- definovať spôsob, akým sa musí merať efektívnosť zvolených opatrení
- implementovať programy školení a budovania povedomia;
- riadiť prevádzku ISMS;
- riadiť zdroje ISMS;
- implementovať postupy a iné opatrenia
- ISO/IEC 27001:2022



Implementácia a prevádzka ISMS (II.)

- definovanie **bezpečnostných rolí a zodpovedností**
  - manažment, zamestnanci, zamestnanec IT ...
- manažér kybernetickej bezpečnosti a zamestnanci IT nedokážu zabezpečiť všetko sami
- právna úprava vyžaduje integráciu kybernetickej bezpečnosti do riadenia organizácie
- zodpovednosť – štatutárny orgán

Hackers Breached Colonial Pipeline Using Compromised VPN Password

Jun 07, 2021 Ravie Lakshmanan

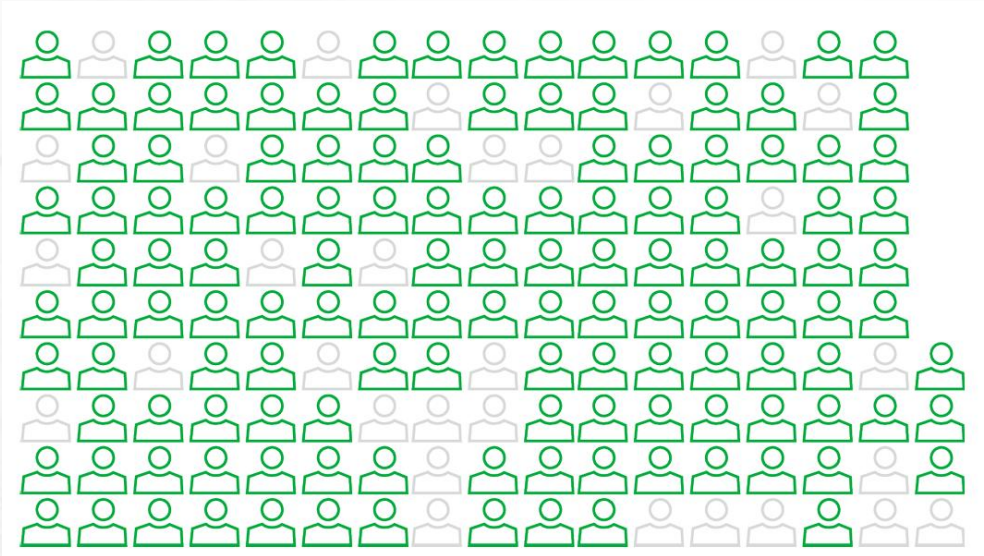
The ransomware cartel that masterminded the Colonial Pipeline attack early last month crippled the pipeline operator's network using a compromised virtual private network (VPN) account password, the latest investigation into the incident has revealed.

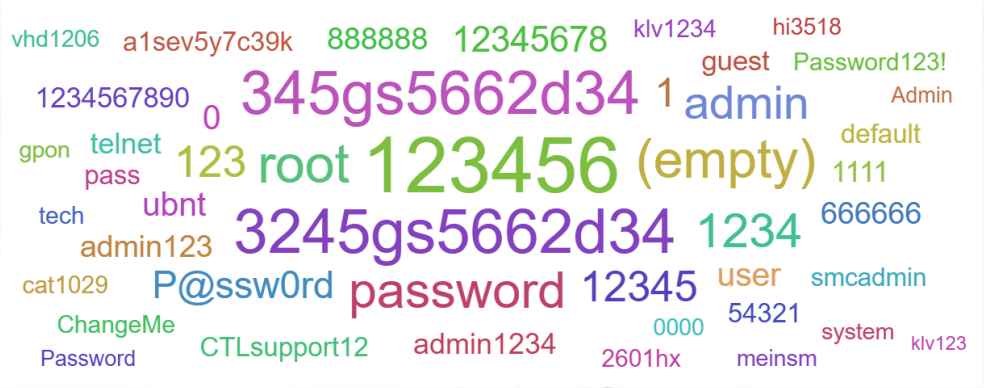
Zdroj: https://thehackernews.com/2021/06/hackers-breached-colonial-pipeline.html

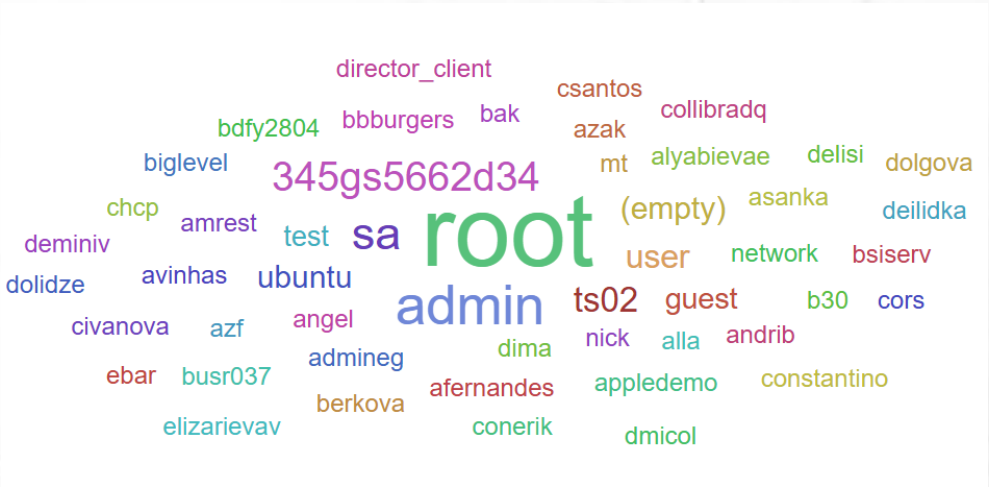
Implementácia a prevádzka ISMS (III.)

- každý zamestnanec nesie svoju mieru zodpovednosti.
- prevencia cez pravidelné školenia a budovanie bezpečnostnej kultúry.

82 %

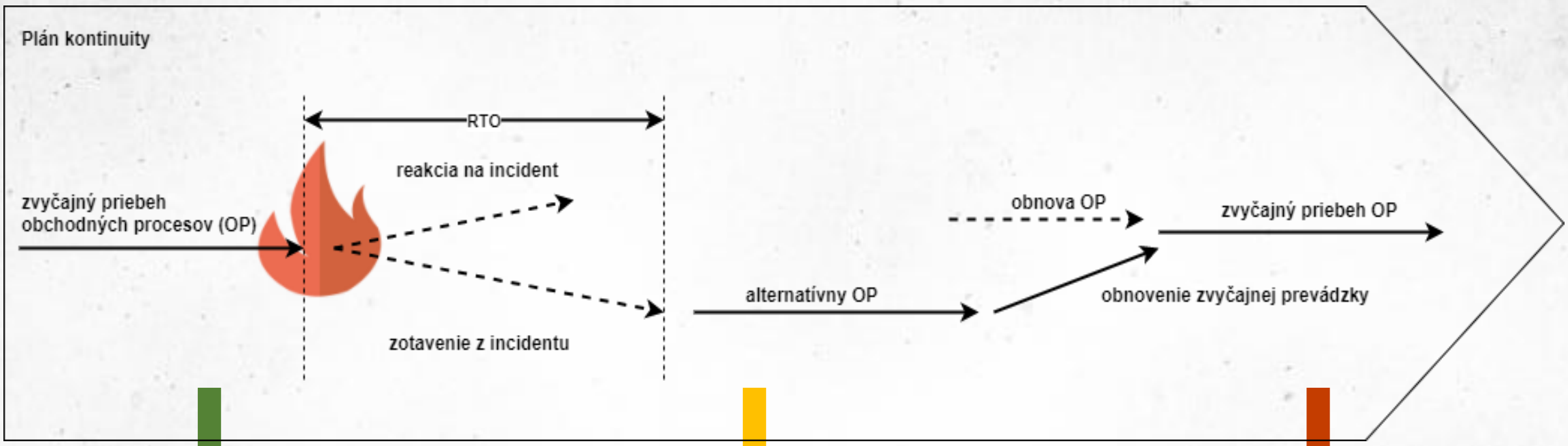






Zdroj: Verizon: DBIR Data Breach Investigations Report, 2022.

Implementácia a prevádzka ISMS (IV.)



Reakcia na incident

(IR)

Kontinuita činností

(BC)

Obnova činností

(BR)

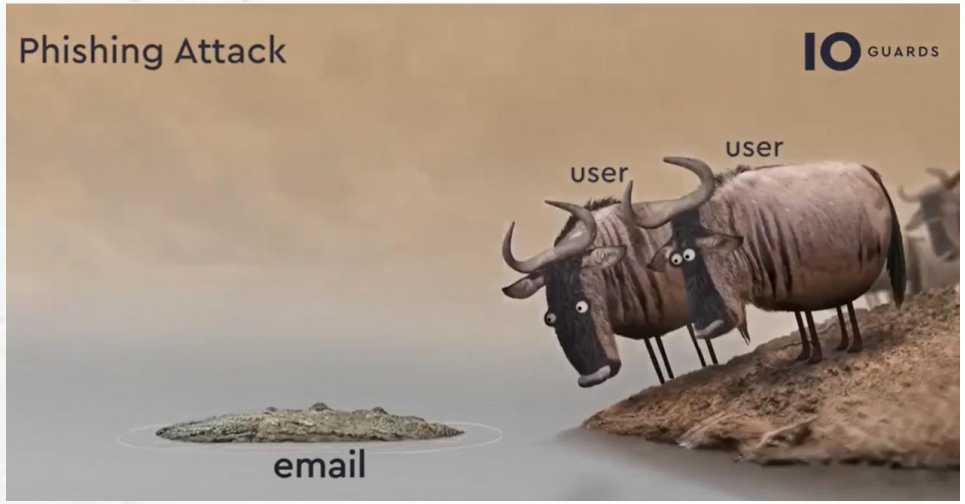
Zdroj: ISO/IEC 270035:2011

Monitorovanie a preskúmanie ISMS (I.)

- Monitorovať a overiť presadzovanie bezpečnostných opatrení
- Previesť interné audity ISMS
- Pripraviť správu o stave ISMS => prehodnotiť ISMS na úrovni vedenia organizácie

Údržba a zlepšovanie ISMS (I.)

- Zavádzať identifikované možnosti zlepšenia ISMS
- Previesť zodpovedajúce opatrenia k náprave a preventívne opatrenia pre odstránenia nedostatku
- Organizácia musí neustále zlepšovať vhodnosť, primeranosť a efektívnosť ISMS.



https://www.youtube.com/watch?v=gSQgbCo6PAg

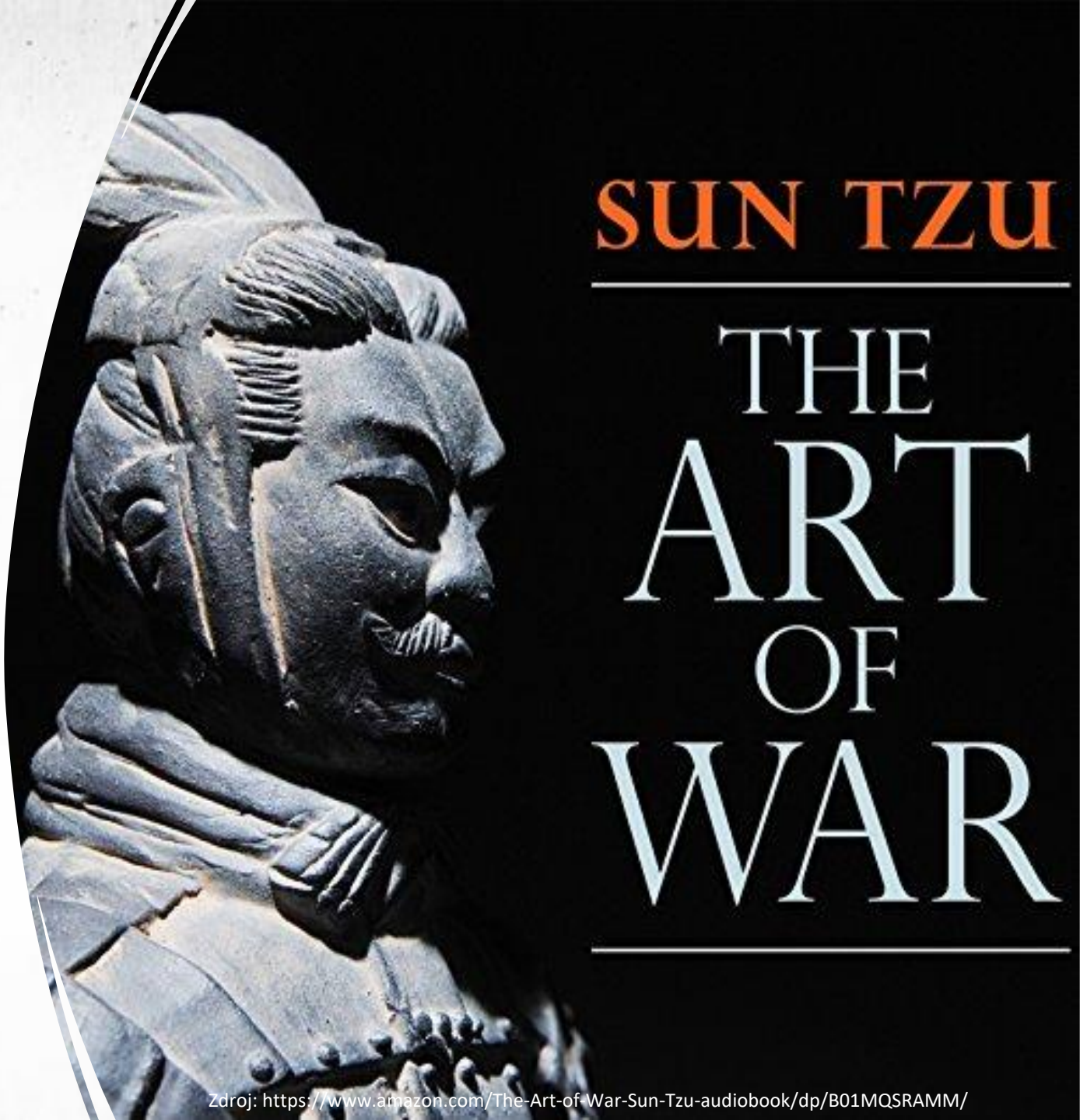
Zdroj: https://vy.technology/p/blog/21-security-testing---security-testing-everywhere, https://www.youtube.com/watch?v=Y-8ZsBaI-go&t=7s

„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

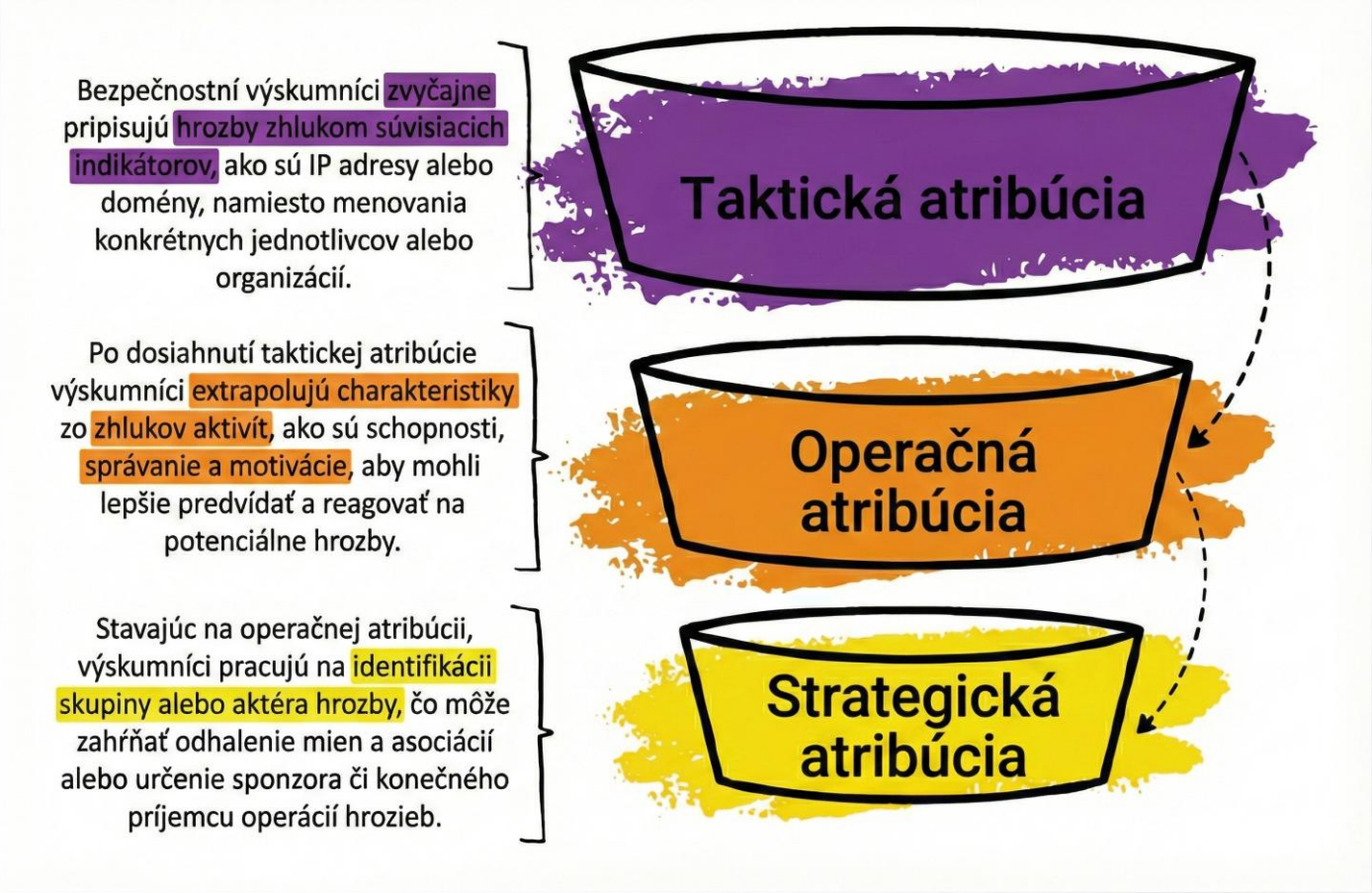


Zdroj: https://www.amazon.com/The-Art-of-War-Sun-Tzu-audiobook/dp/B01MQSRAMM/

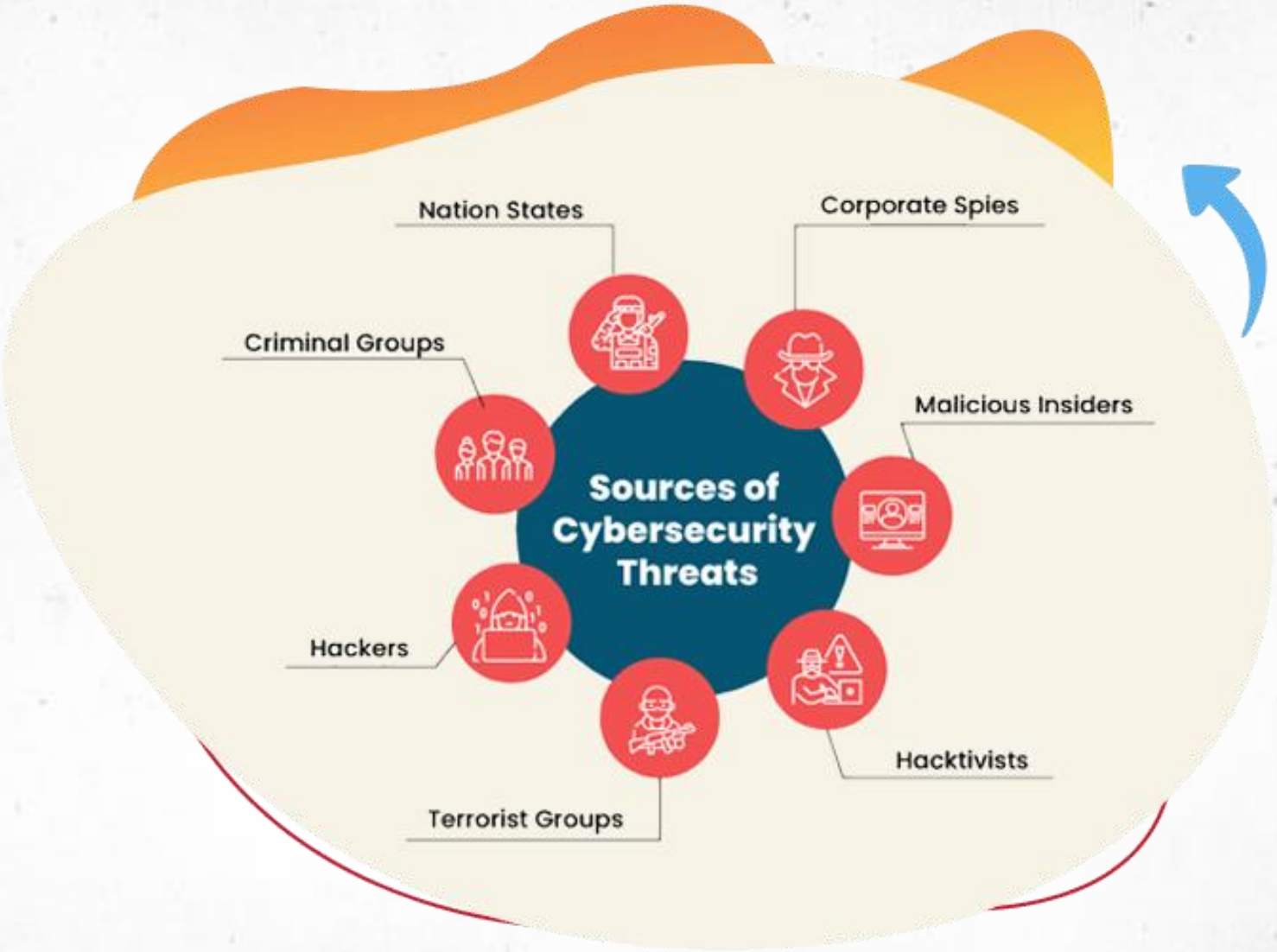
Atribúcia

Atribúcia

- je proces **určenia pôvodu a zodpovedných aktérov** za kybernetický útok
- je kľúčová pre primerané obranné aj odvetné opatrenia.
- Ide o náročnú úlohu pre anonymitu, zdieľané nástroje a techniky a geopolitické súvislosti.
- má významný geopolitický dopad – môže viesť k diplomatickým krokom, sankciám či odstrašeniu budúcich útokov a formuje strategické rozhodovanie.

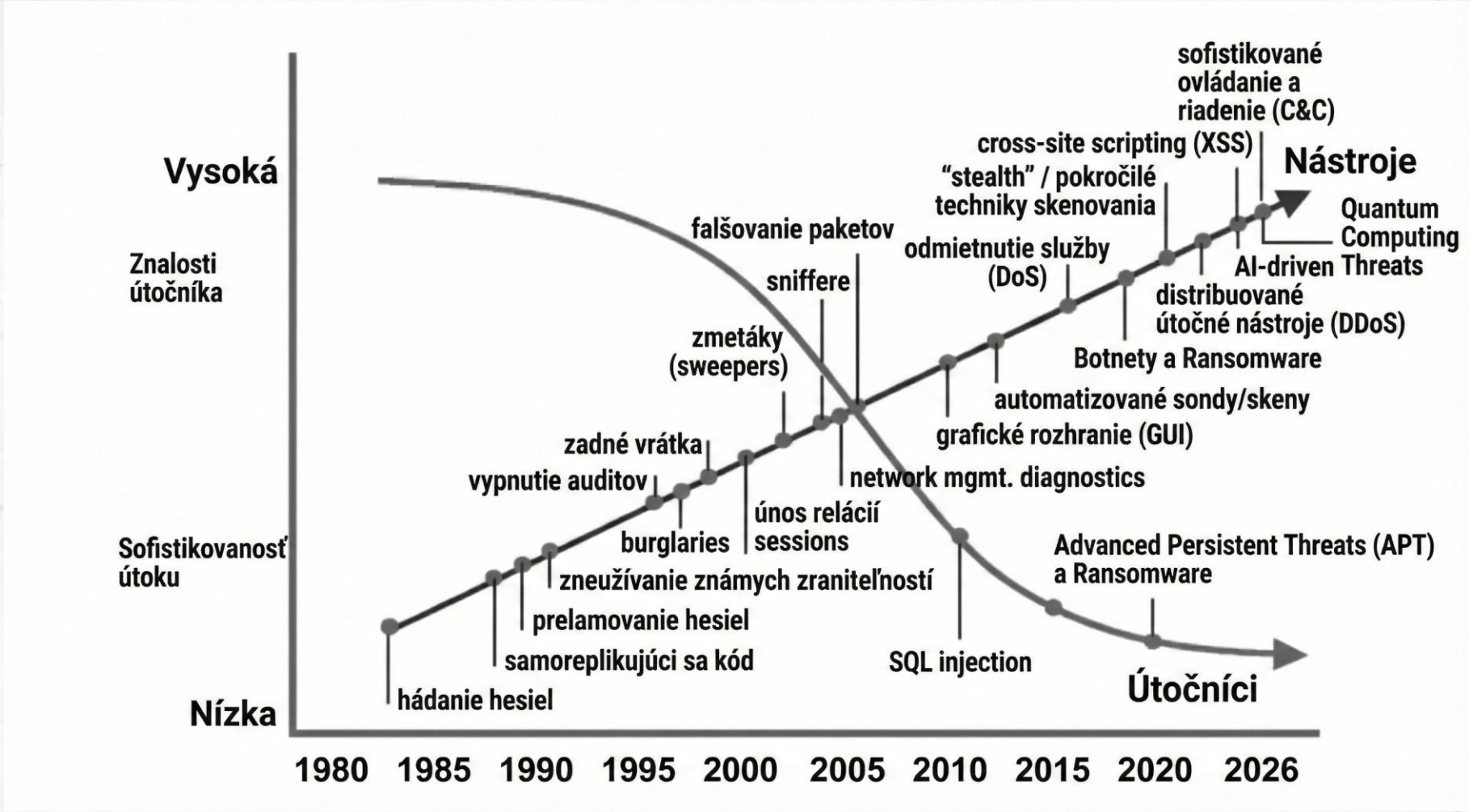


Pôvodca hrozby (I.)



Zdroj: https://www.byitcinternational.com/cyber-security-as-career/

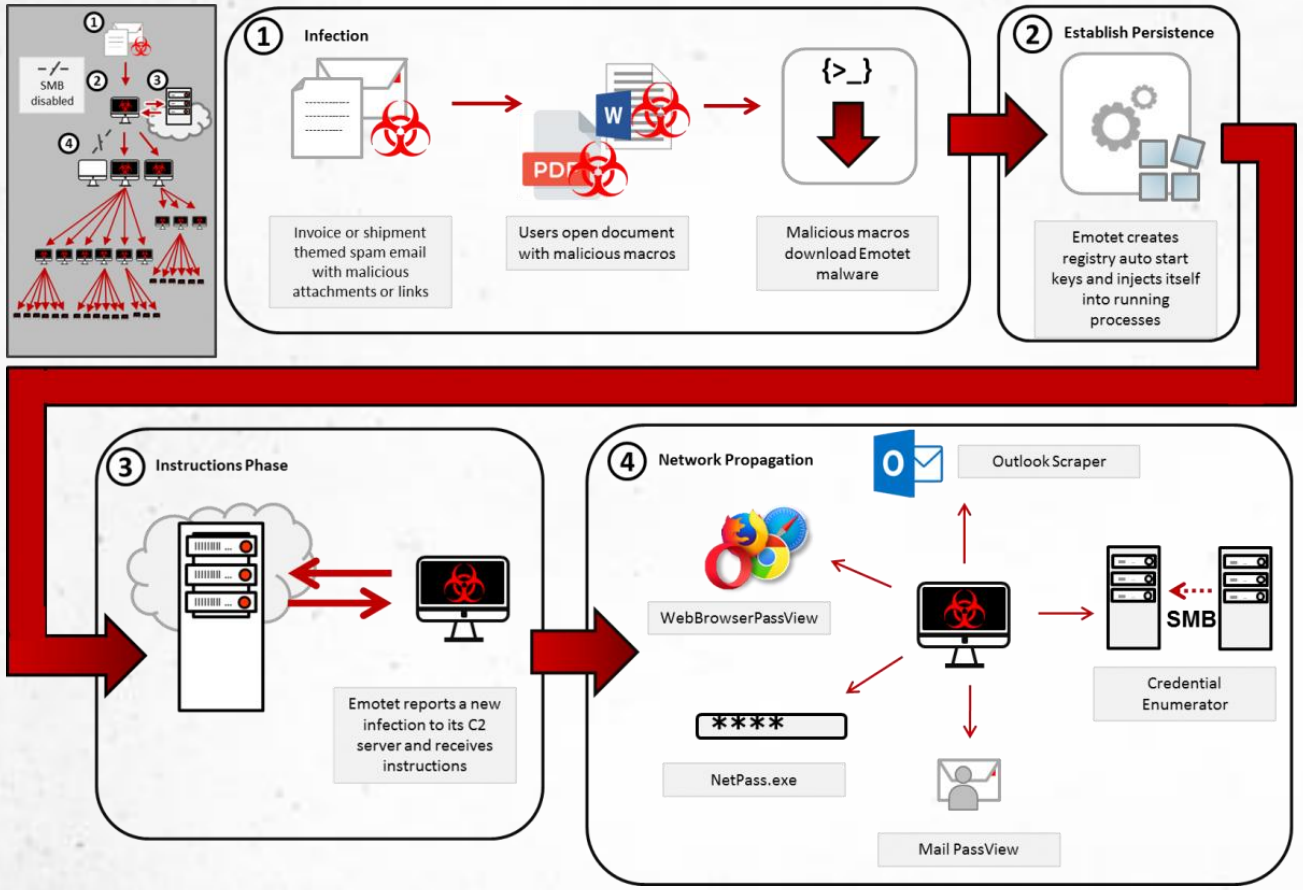
Pôvodca hrozby (II.)

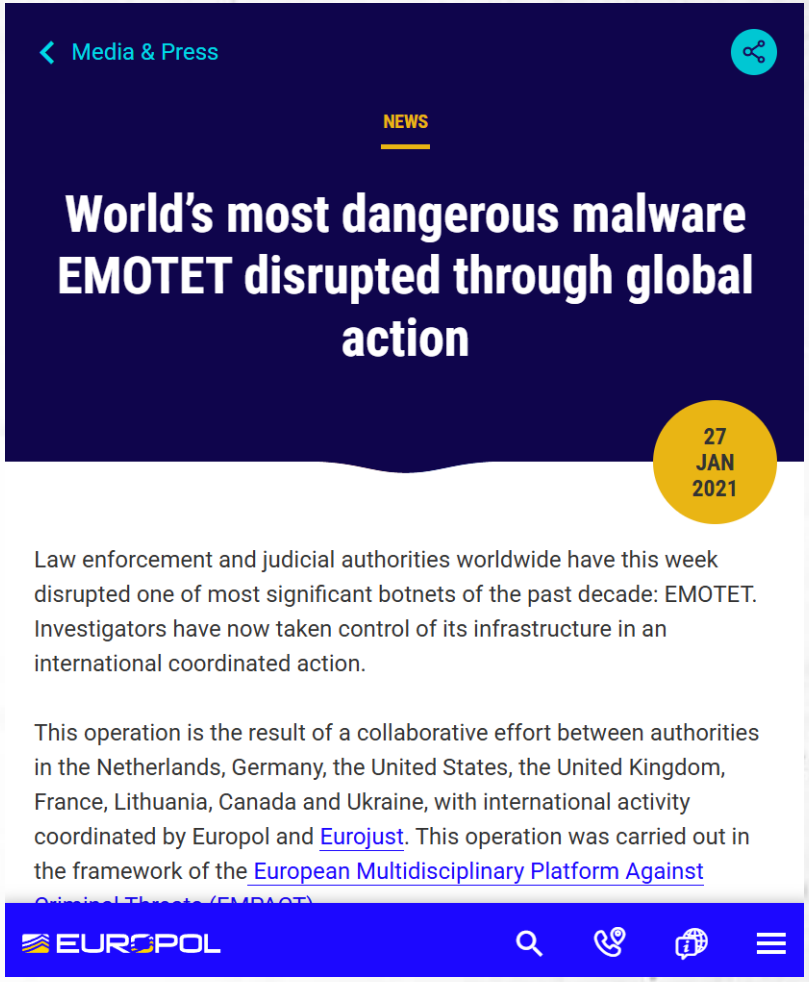


Zdroj: MEYERS, Carol; POWERS, Sarah; FAISSOL, Daniel. Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches. Lawrence Livermore National Laboratory (April 2009), 2009, 7: 1-22, Upravené pomocou GEMINI

Pôvodca hrozby (III.)

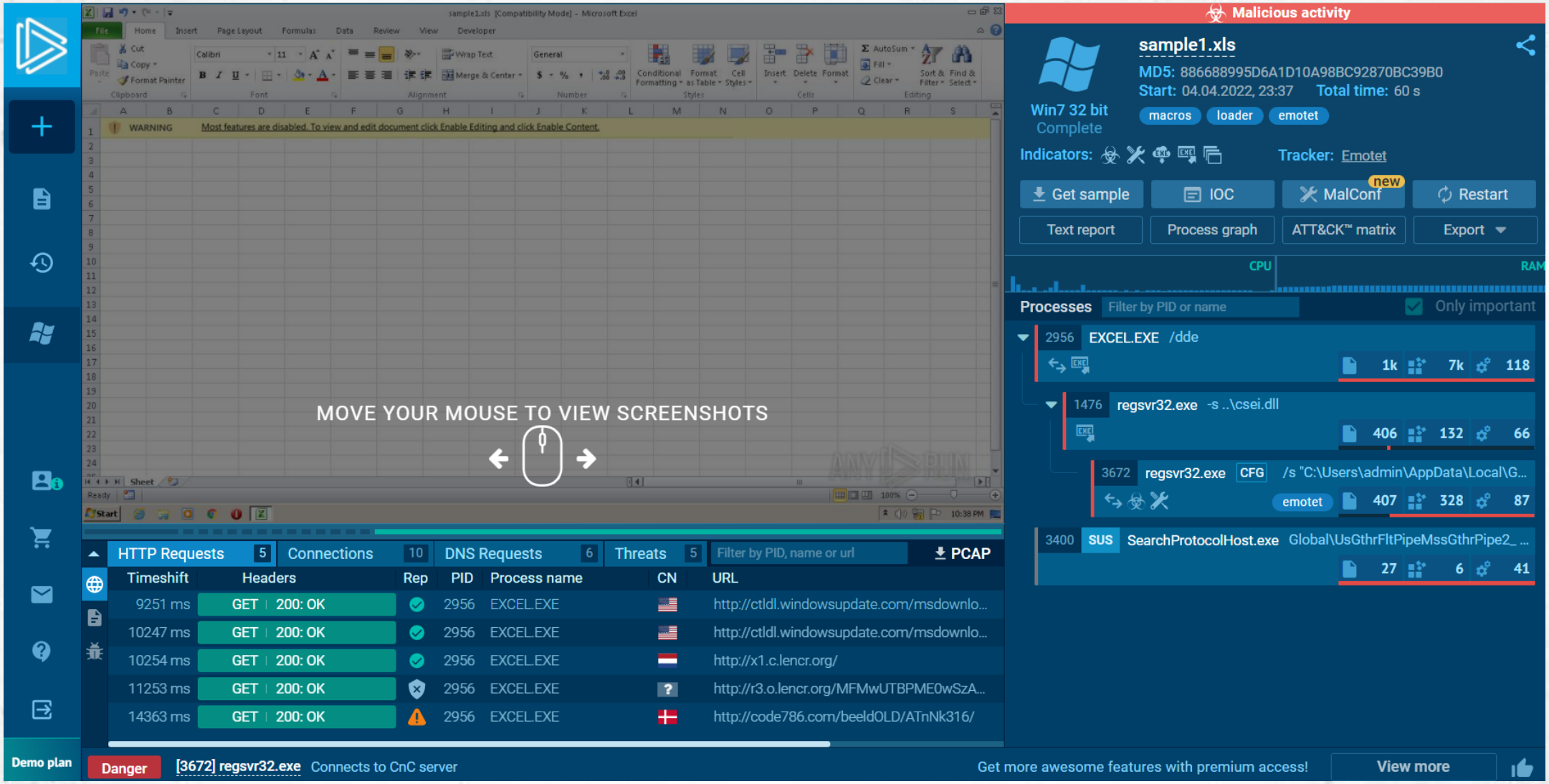
- **Emotet** - modus operandi





Zdroj: https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action, https://www.cisecurity.org/

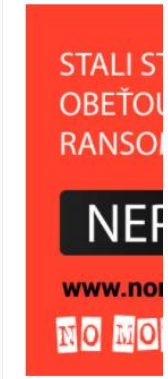
Pôvodca hrozby (IV.)

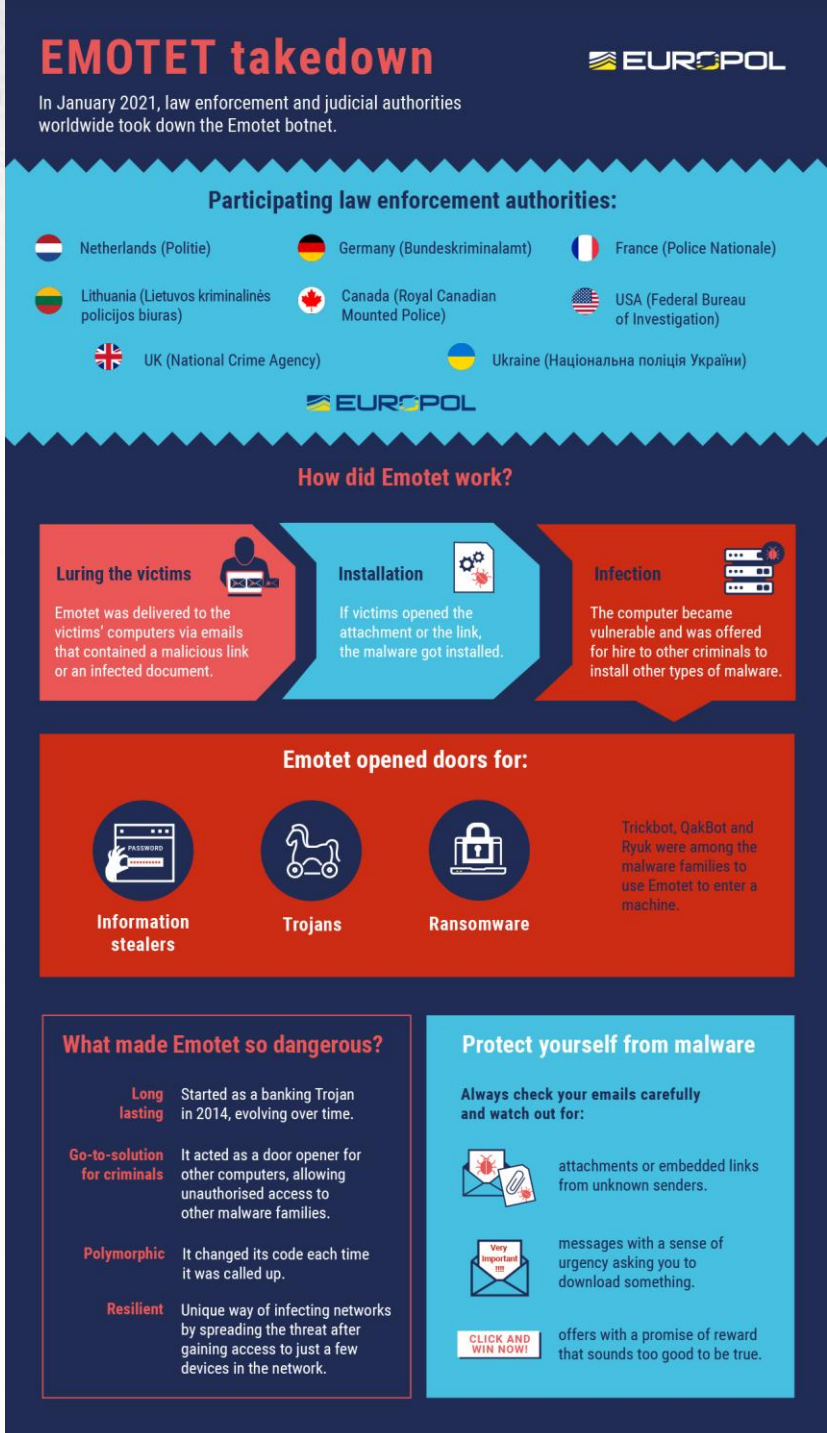


Zdroj: https://app.any.run/tasks/093af2d6-3f5e-400d-9dcc-de2706a140ed/

Pôvodca hrozby (V.)

Medzinárodný policajný tím rozvrátil notoricky známy botnet Emotet

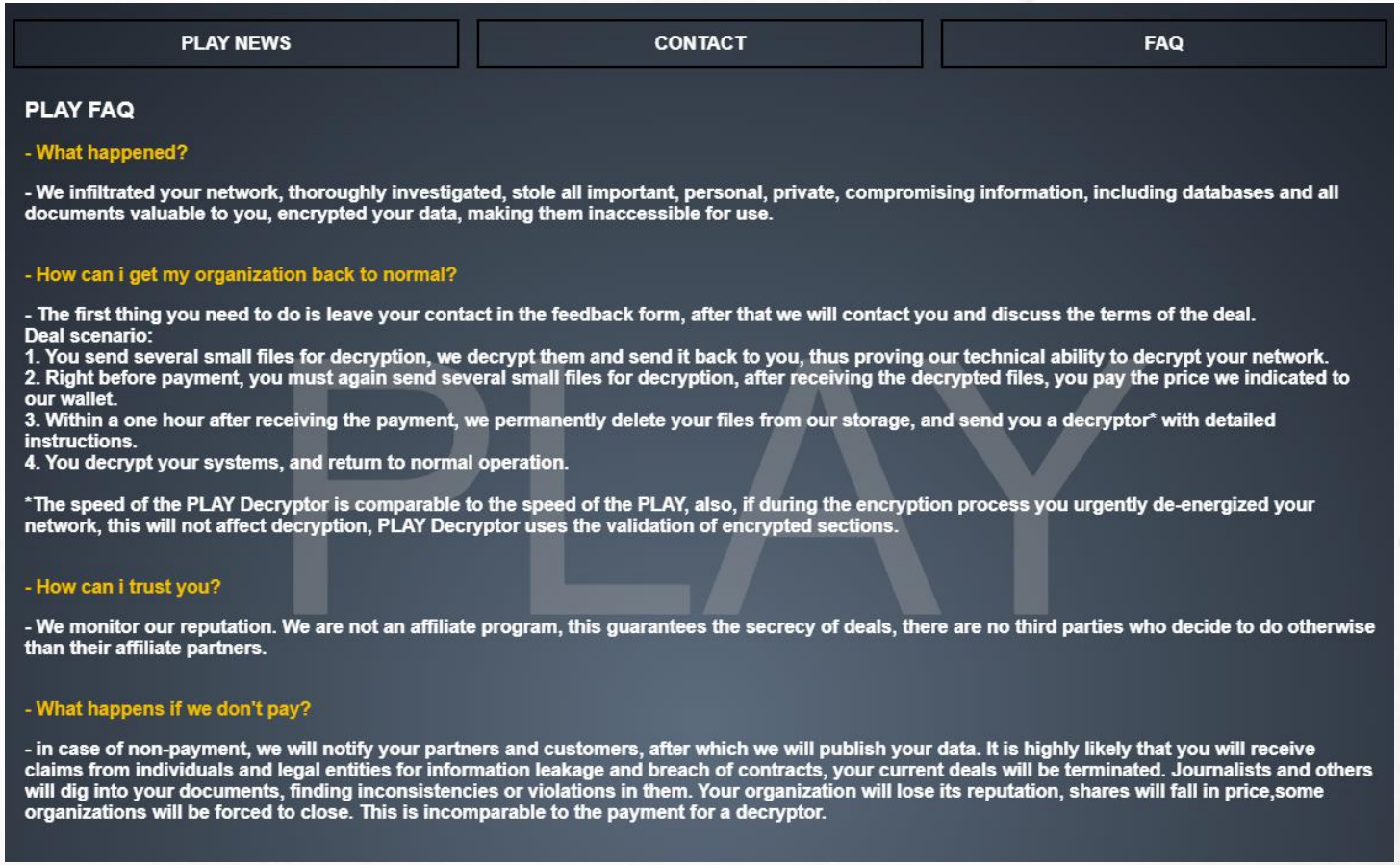




Zdroj: https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-d

Pôvodca hrozby (VI.)

- „Do not contact the FBI, police, or other government agencies. They do not care about your organization, they will not let you pay the ransom, which will entail the publication of files, after which courts, lawsuits, fines will begin.“



PLAY NEWS | CONTACT | FAQ

PLAY FAQ

- What happened?

- We infiltrated your network, thoroughly investigated, stole all important, personal, private, compromising information, including databases and all documents valuable to you, encrypted your data, making them inaccessible for use.

- How can i get my organization back to normal?

- The first thing you need to do is leave your contact in the feedback form, after that we will contact you and discuss the terms of the deal.
Deal scenario:
1. You send several small files for decryption, we decrypt them and send it back to you, thus proving our technical ability to decrypt your network.
2. Right before payment, you must again send several small files for decryption, after receiving the decrypted files, you pay the price we indicated to our wallet.
3. Within a one hour after receiving the payment, we permanently delete your files from our storage, and send you a decryptor* with detailed instructions.
4. You decrypt your systems, and return to normal operation.

*The speed of the PLAY Decryptor is comparable to the speed of the PLAY, also, if during the encryption process you urgently de-energized your network, this will not affect decryption, PLAY Decryptor uses the validation of encrypted sections.

- How can i trust you?

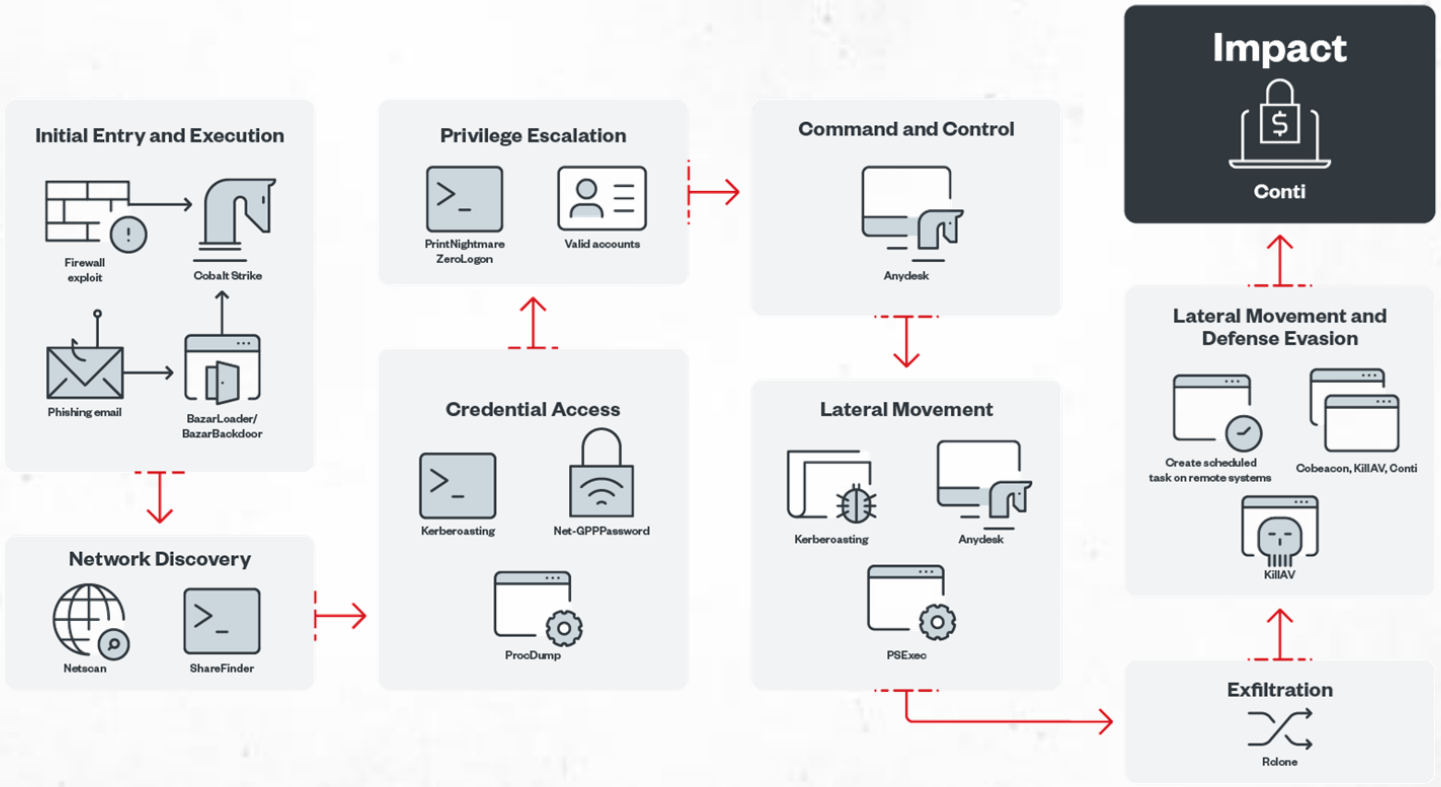
- We monitor our reputation. We are not an affiliate program, this guarantees the secrecy of deals, there are no third parties who decide to do otherwise than their affiliate partners.

- What happens if we don't pay?

- in case of non-payment, we will notify your partners and customers, after which we will publish your data. It is highly likely that you will receive claims from individuals and legal entities for information leakage and breach of contracts, your current deals will be terminated. Journalists and others will dig into your documents, finding inconsistencies or violations in them. Your organization will lose its reputation, shares will fall in price,some organizations will be forced to close. This is incomparable to the payment for a decryptor.

Conti (I.)

- jedna z najaktívnejších a najnebezpečnejších ransomware skupín
- fungovala ako **Ransomware-as-a-Service (RaaS)**
- zameriavala sa na veľké organizácie a kritickú infraštruktúru
- vysokoprofilové útoky: zdravotníctvo (Írsko) / verejný sektor (Nový Zéland)
- únik údajov – nástroje, postupy, komunikácia



Zdroj: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti

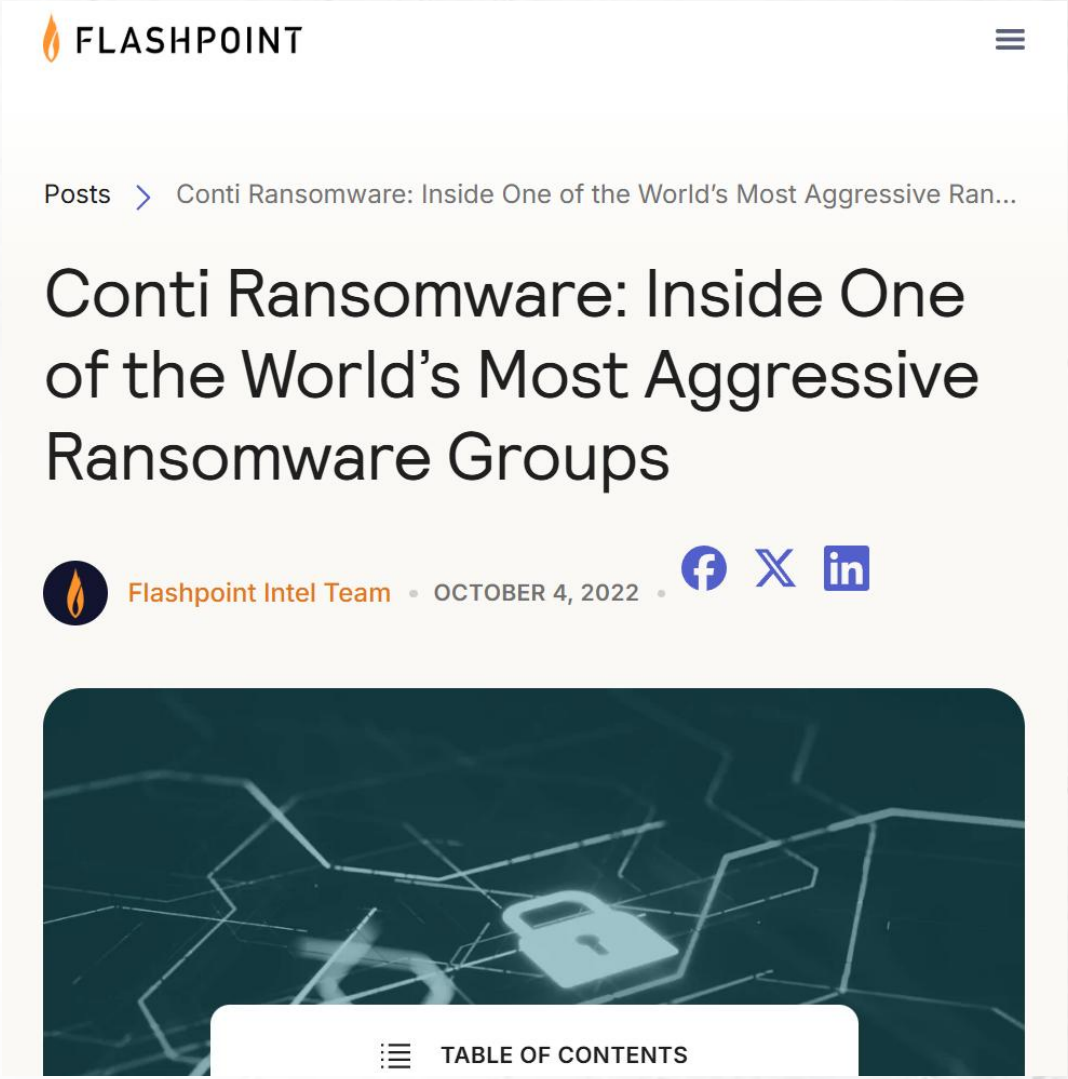
Conti (II.)

SIEŤOVÁ INFRAŠTRUKTÚRA

- Takmer každú modernú sieť je možné hacknúť.

Dôvody sú nasledovné:

- **Nadbytočnosť sietí** – veľké množstvo služieb a rôzne vstupné body do tej istej siete.
- **Priorita pohodlia pred bezpečnosťou** – väznica je bezpečná, ale veľmi neefektívna na vykonávanie činností.
- **Ľudský faktor** – chyby v konfigurácii, sociálne inžinierstvo.



Zdroj: https://flashpoint.io/blog/history-of-conti-ransomware/

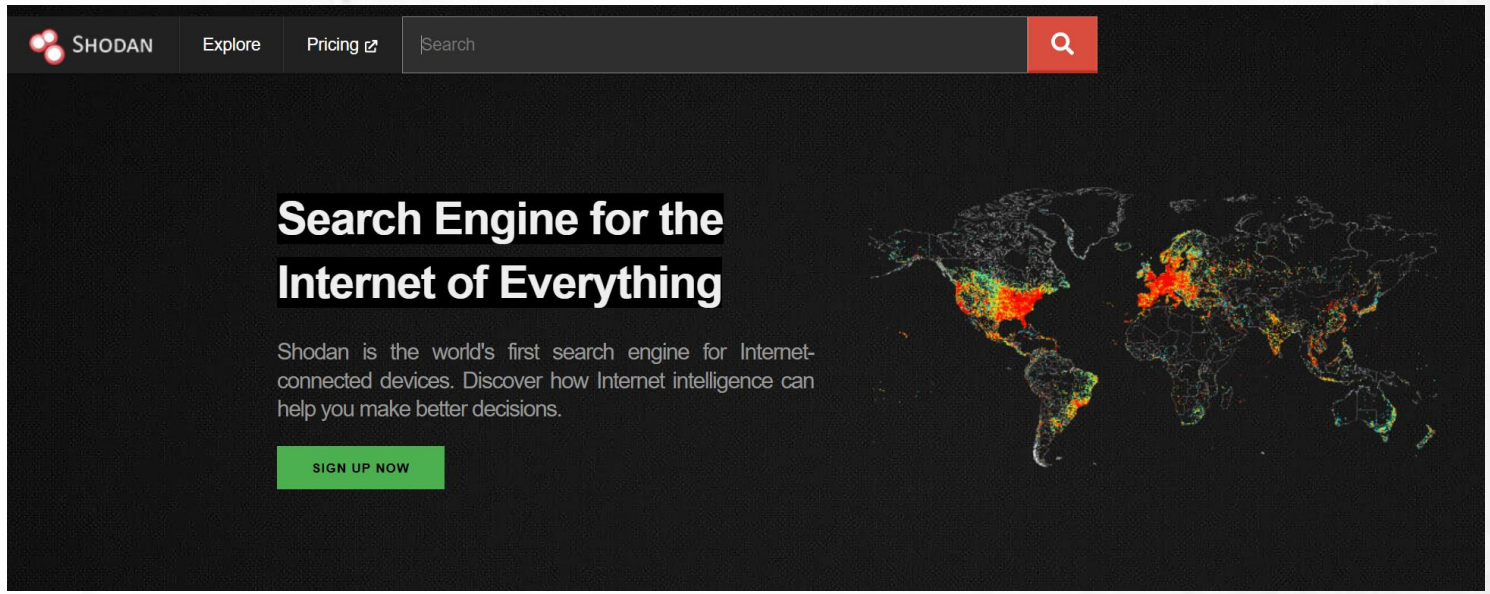
Conti (II.)

PRIESKUM A VÝBER CIEĽA

- Ak nemáte konkrétny cieľ a disponujete exploitom, môžete skenovať sieť (celý internet alebo vybrané rozsahy IP adries) s cieľom nájsť zraniteľné služby.
- Ak chcete ušetriť čas, použite známe služby ako Shodan.io, ale lepšie je mať vlastný skener.

- Pri cielenom útoku je nevyhnutný prieskum:

1.Začnite analýzou domény
2.Veľké korporácie majú vlastné autonómne systémy (AS), ...
3.Použite OSINT nástroje na **získanie údajov o cieľovej organizácii a jej zamestnancoch.**



Zdroj: https://www.shodan.io/

Conti (III.)

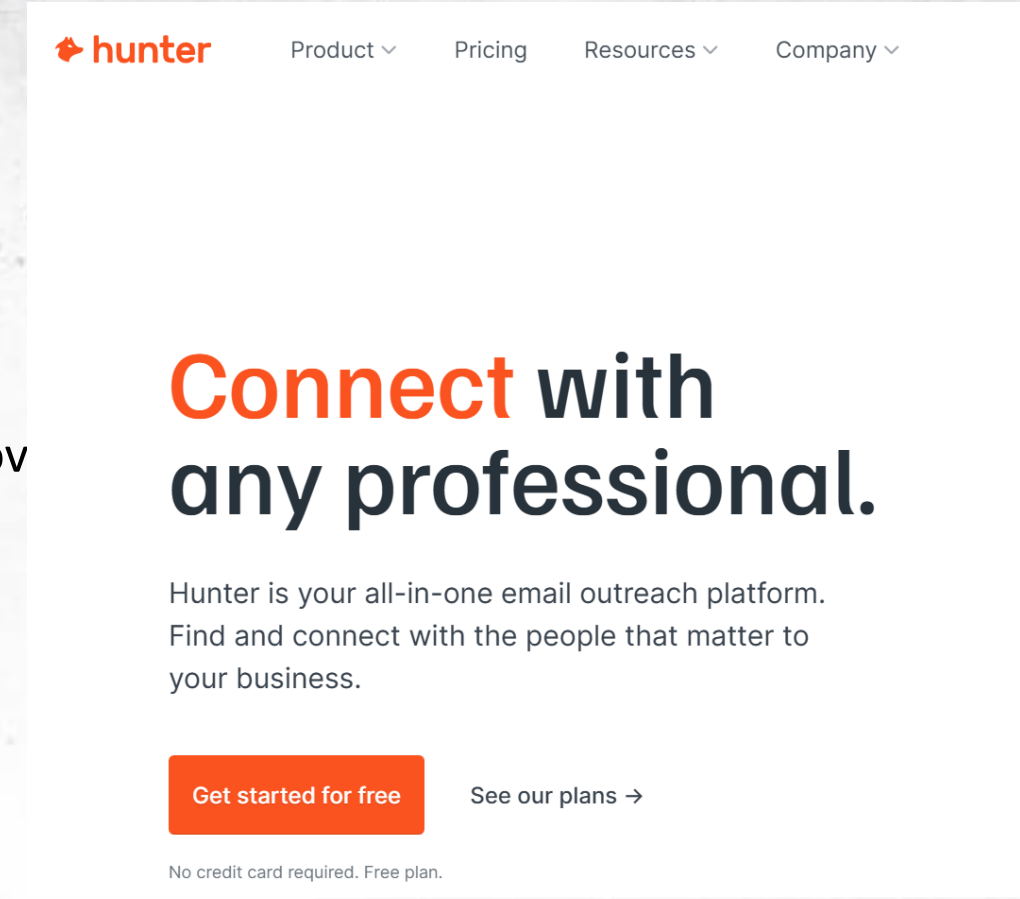
NÁSTROJE OSINT

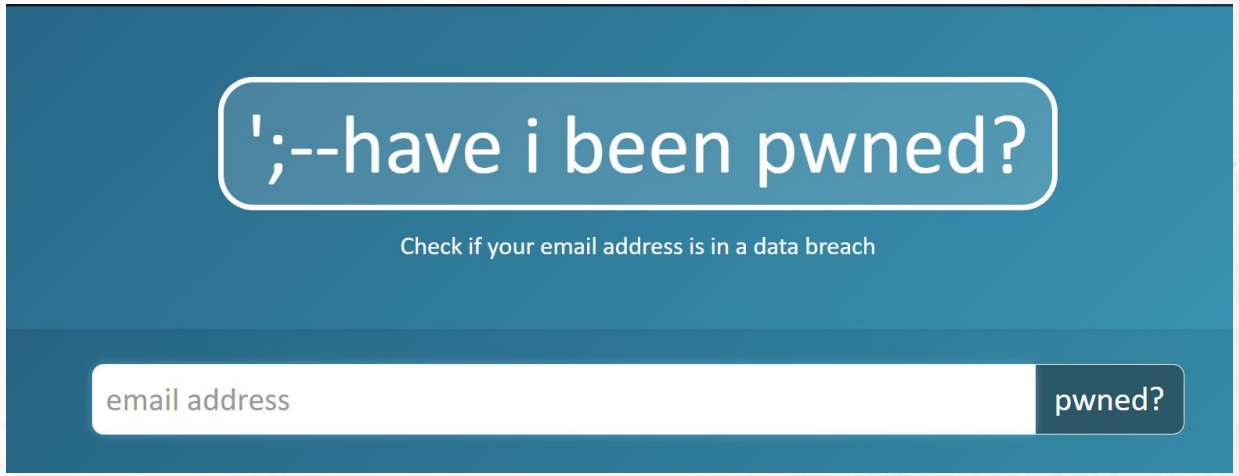
Vyhľadávače informácií:
- theHarvester – zber emailov, subdomén, otvorených portov
- SpiderFoot – OSINT analýza
- hunter.io – zbiera emaily podľa domény

Vyhľadávanie firiem:
- ZoomInfo – firemné dáta
- OpenCorporates – databáza firiem

Vyhľadávanie používateľských mien:
- Namechk

Vyhľadávanie emailov:
- Have I Been Pwned





Zdroj: https://hunter.io/
https://haveibeenpwned.com/

Conti (IV.)

Dátum: 2021-03-15T16:09:16.675Z
Od: Kalinka
Správa: Chlapi, viete mi povedať, ako vypnúť ESET File Security?

Dátum: 2021-03-15T15:14:23.771Z
Od: t3chnolog
Správa: dtssync je mizerná voľba v každom prípade)

Dátum: 2021-03-15T15:14:07.896Z
Od: Rosette
Správa: Zhromažďuje Sophos Windows logy? Je to len proti malvéru?

Dátum: 2021-03-15T15:13:30.907Z
Od: Slice
Správa: Ako nenápadná je možnosť vykonať DCSync na konkrétnych používateľoch, ak je na DC Sophos?

Dátum: 2021-03-15T14:39:56.903Z
Od: Andy
Správa: Jasné, vďaka, teraz to skúsim

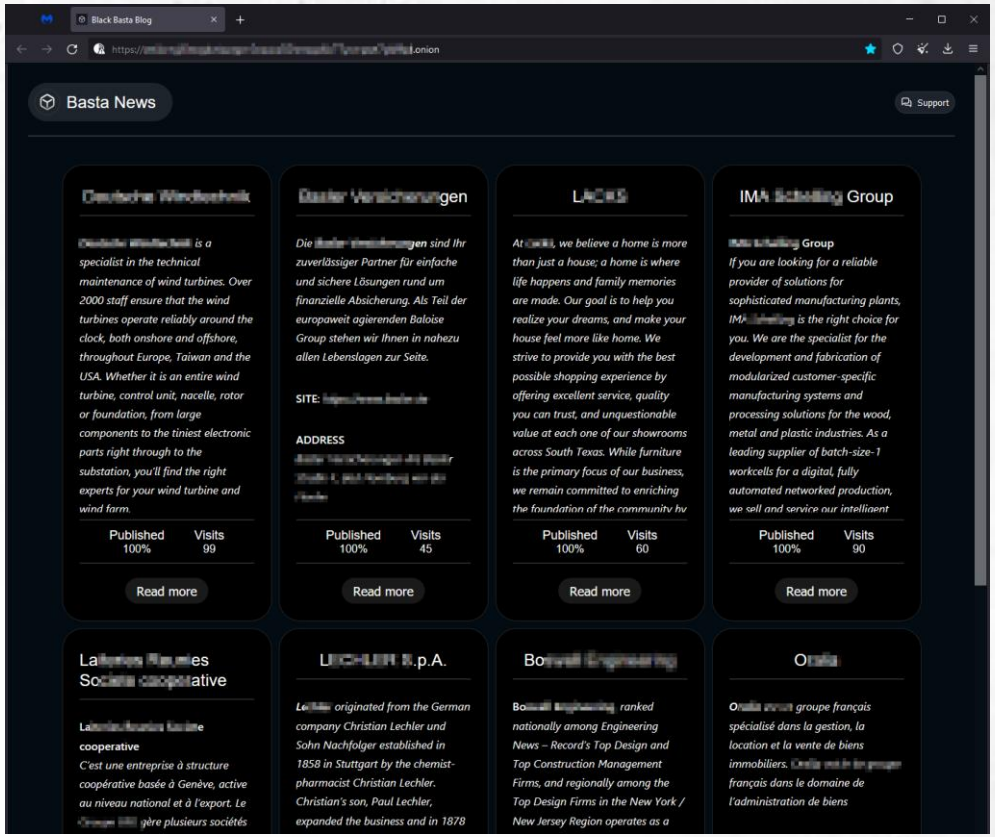
Conti (V.)

Dátum: 2021-06-28T11:08:00.394568
Od: ***@q3.onion
Komu: ***@q3.onion
Správa:
Vyvinuli sme jednoduchší koncept analýzy dát a volaní\ vydierania. Navrhol som nasledovnú schému:
Máme samostatnú prieskumnú raketovú spoločnosť. Prenesieme ju na analytikov, ktorí vypracujú správu o spise. Ak sú potrebné vydierania\volania, túto úlohu pridelíme volajúcim. Aby volajúci pracovali efektívne a **nevolali len do prázdna, ako sa to deje teraz**, sú v kontakte s analytikmi a môžu si **od nich vyžiadať akékoľvek dodatočné údaje**,
povedzme časť zoznamu dátumov alebo nejaké informácie o počítačoch\heslách.

Ak **spoločnosť neodpovie, jej údaje sa odovzdajú na zverejnenie na stránke** (na to je potrebné pridať do tohto chatu buď manažéra, alebo niekoho z jeho podporného tímu).

Black Basta (I.)

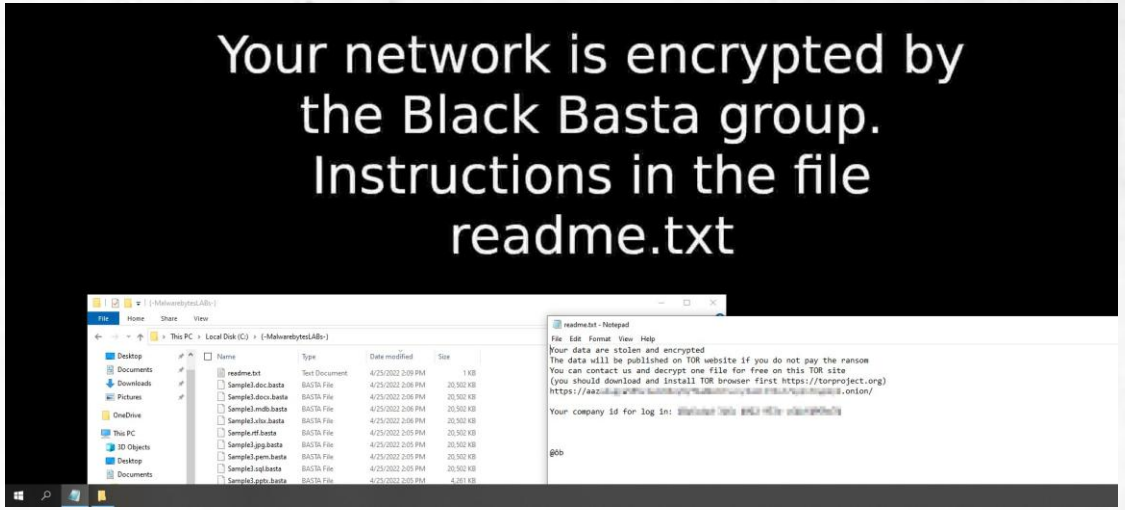
- Ransomware-as-a-Service (RaaS) skupina aktívna od apríla 2022
- pravdepodobne vznikla ako rebrand alebo pokračovanie inej skupiny (napr. väzby na Conti)
- disponovala sieťou affiliate partnerov, ktorí realizovali útoky
- používala „double extortion“: šifrovanie dát exfiltrácia a vyhrážanie sa zverejnením (leak site „Basta News“)
- využívala prístup „name-and-shame“ (verejné zverejňovanie obetí)



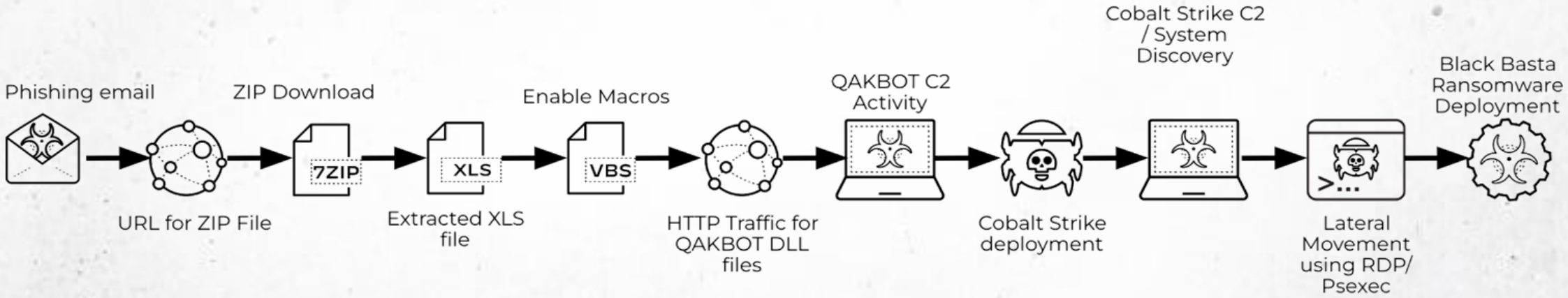
Zdroj: https://x.com/MarceloRivero/status/1519398885193654273/photo/1

Black Basta (II.)

- často využívali malware **QBot (Qakbot)**
- rýchla eskalácia útoku – dôraz na rýchle šifrovanie a lateral movement



Black Basta Attack Lifecycle

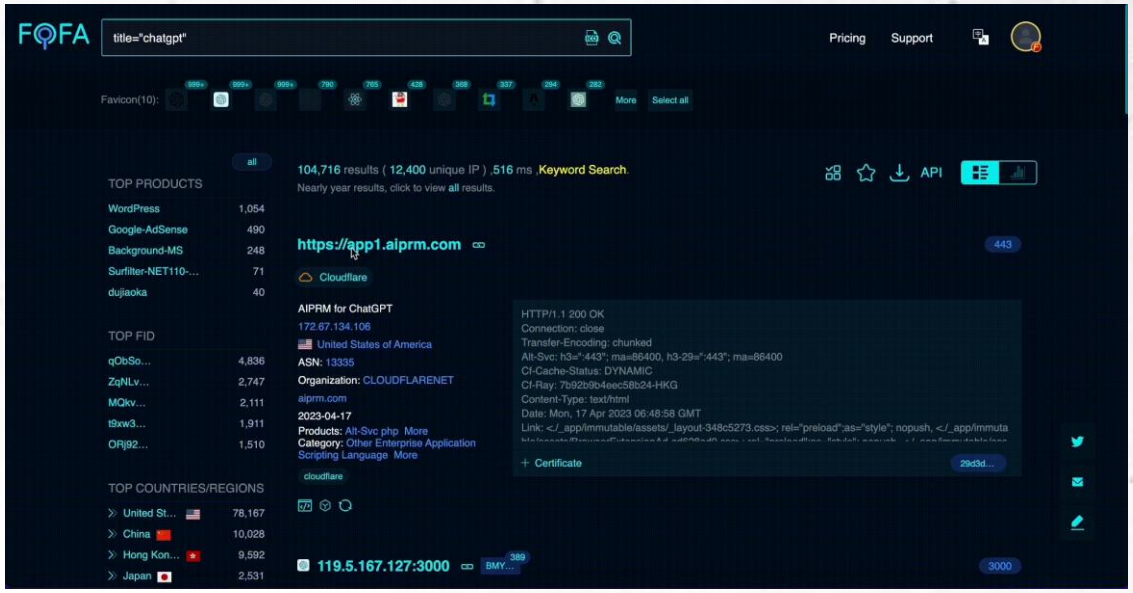


Zdroj: https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/, https://x.com/MarceloRivero/status/1519398885193654273/photo/2

Black Basta (III.)

- **aktívneho skenovania a validácie cieľov**:

- [2024-03-01 11:04:28] ***: Aké linky sú tam zabudované?
- [2024-03-01 11:04:32] ***: Len root používateľ
- [2024-03-01 11:04:51] ***: Spusť to
- [2024-03-01 11:06:20] ***: Cez noc to nič nenašlo, čo je zlé
- [2024-03-01 11:06:24] ***: Asi toho veľa nenájde
- [2024-03-01 11:09:29] ***: (nájdené endpointy s root prístupmi)
- [2024-03-01 11:09:31] ***: Našlo toto
- [2024-03-01 11:09:47] ***: Toto je ESXi, ktorý asi akceptuje akékoľvek heslo
- [2024-03-01 11:13:54] ***: Treba získať viac IP Jenkins
- [2024-03-01 11:14:07] ***: Aj cez FOFA a Shodan



MITRE ATT&CK techniky:

- T1595 – Active Scanning
- T1590 – Gather Victim Network Info
- T1110 – Brute Force
- T1190 – Exploit Public-Facing App

Zdroj: https://github.com/D4RK-R4BB1T/BlackBasta-Chats, https://github.com/followthesapper/black-basta-chats-translated, https://medium.com/@fofabot/get-started-with-fofa-a-beginners-guide-3e4d3576d14d

Black Basta (IV.)

- **testovanie phishing kampane:**

- [2024-04-22 21:09:19] ***: Link je prázdny
- [2024-04-22 21:09:34] ***: Vyzerá to zle
- [2024-04-22 21:10:11] ***: Treba to opraviť
- [2024-04-22 21:11:42] ***: Skontrolujte prechod cez link
- [2024-04-22 21:11:50] ***: Scan linku ešte beží
- [2024-04-22 21:13:25] ***: Ak toho pošleme veľa
- [2024-04-22 21:13:33] ***: Doména pôjde rýchlo na blacklist
- [2024-04-22 21:15:03] ***: Poďme najprv cielene
- [2024-04-22 21:15:19] ***: Najprv vyberieme firmy na test
- [2024-04-22 21:15:23] ***: Potom ostrá prevádzka

MITRE ATT&CK techniky:

- T1566.002 – Phishing (Link)
- T1583.001 – Acquire Infrastructure (Domains)
- T1036 – Masquerading

Zdroj: https://github.com/D4RK-R4BB1T/BlackBasta-Chats, https://github.com/followthesapper/black-basta-chats-translated

Black Basta (IV.)

- **rozšírenie útoku o sociálne inžinierstvo cez telefón**:

- [2024-06-03 18:10:02] ***: Dá sa spraviť, aby hovor vyzeral ako z IT oddelenia?
- [2024-06-03 18:10:12] ***: Áno, práve to robíme
- [2024-06-03 18:13:32] ***: Zatiaľ voláme na prístupy čo máme
- [2024-06-03 18:14:21] ***: Pripravím testovací call cez call centrum

MITRE ATT&CK techniky:

- T1566.004 – Phishing (Voice)
- T1656 – Impersonation
- T1204 – User Execution

Zdroj: https://github.com/D4RK-R4BB1T/BlackBasta-Chats, https://github.com/followthesapper/black-basta-chats-translated

Aktuálne APT skupiny (I.)

1) Mustang Panda (APT27) – China-Aligned

- Čína-spojená APT skupina s aktívnym pôsobením od 2017.
- cieli na NGO, think tanky a vládne entity v rôznych regiónoch.
- používa sociálne inžinierstvo a pokročilé malvérové taktiky

2) APT41 (Double Dragon) – China-Aligned

- kombinuje štátom sponzorovanú špionáž a finančne motivované útoky.
- pôsobí v rôznych odvetviach a regiónoch.
- 2025 aktivity zahŕňali spear-phishing a kompromitácie systémov.

Zdroj: https://socradar.io/blog/top-10-apt-groups-in-2025/

Aktuálne APT skupiny (II.)

3) APT29 (Cozy Bear / Midnight Blizzard) – Russia-Aligned

- Ruská špionážna skupina spojená s SVR (Foreign Intelligence Service).
- cieli na vládne, diplomatické a infraštruktúrne siete USA/EÚ.
- 2025: watering hole kampane a zber poverení.

4) Lazarus Group – North Korea-Aligned

- Severokórejská APT skupina s rôznymi aliasmi ako Hidden Cobra, Zinc alebo Guardians of Peace.
- globálne operácie kombinujú špionáž aj finančnú kriminalitu.
- 2025: veľká krádež kryptomien (napr. Upbit).

Zdroj: https://socradar.io/blog/top-10-apt-groups-in-2025/, https://www.ria.ee/en/russian-bears-cyberspace

Aktuálne APT skupiny (III.)

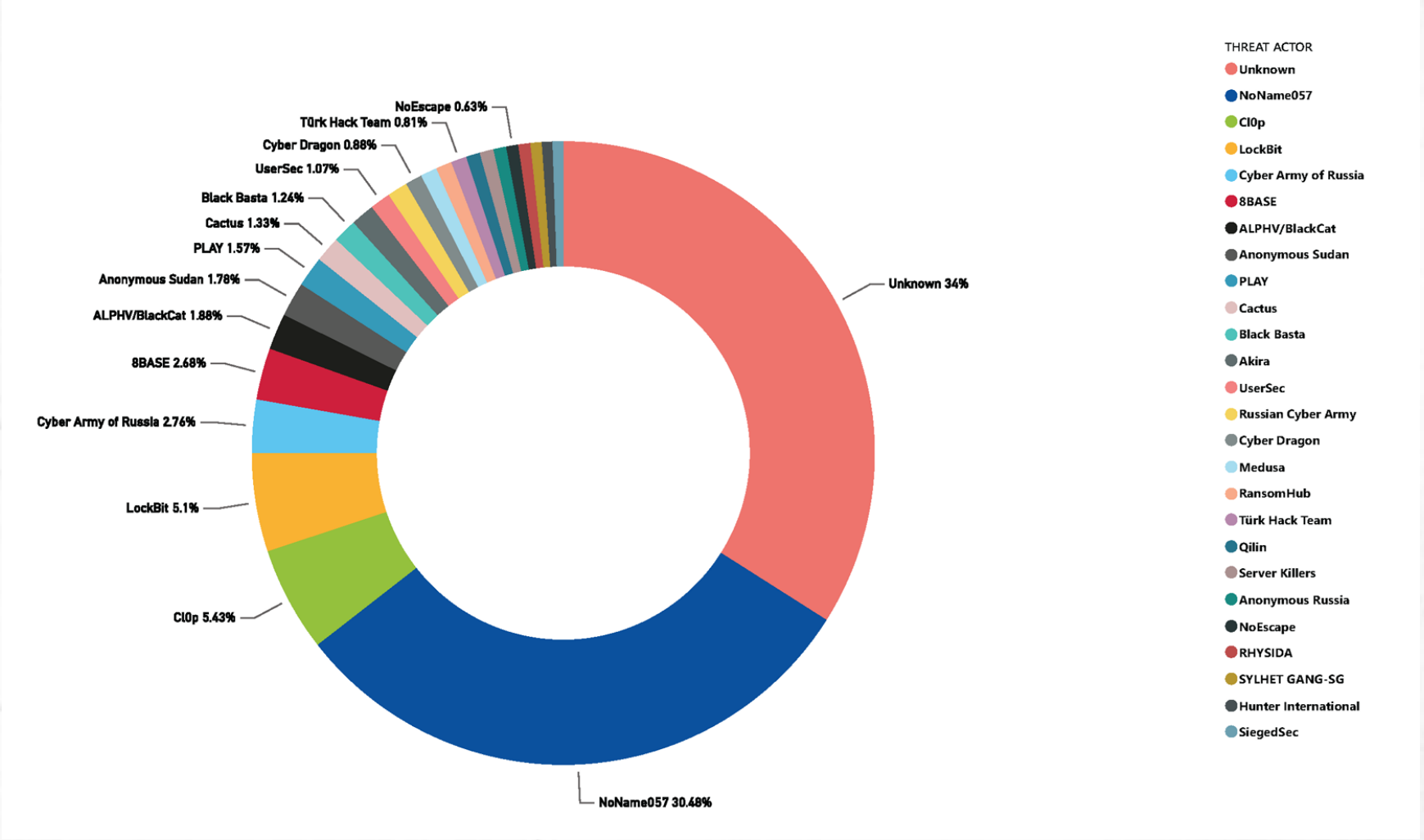
A1 | Naming Taxonomies

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	**Naming Taxonomies**																
2	Country / Selector	FireEye / Mandiant / Trellix	CrowdStrike	Kaspersky	DELL SecureWorks	DELL SecureWorks (old)	Palo Alto Unit 42 (2022-*)	Check Point	Trend Micro Labs	Cisco Talos	Verisign iDefense	Microsoft Windows Defender Research	Microsoft (2023-*)	Symantec	360	Dragos	Thalos Gr
3	Name Space		Animals		Metals	Threat Group (TG)	Star Constellations + modifier word		Elements		Fish Names	Elements, Trees, Volcano, DEV	Environmental Hazards	Bug Names		Minerals	
4	Generic	APT[X]				TG-[X]				Group [X]					APT-C-[X]		ATK-[#]
5	China		[X] Panda	[X] Dragon*	BRONZE [X]		[X] Taurus						Typhoon				
6	Russia		[X] Bear	[X] Duke*	IRON [X]		[X] Ursa						Blizzard				
7	North Korea		[X] Chollima		NICKEL [X]		[X] Pisces						Sleet				
8	South Korea		[X] Crane		TUNGSTEN [X]								Hail				
9	Iran		[X] Kitten		COBALT [X]		[X] Serpens						Sandstorm				
10	India		[X] Tiger		ZINC [X]		[X] Gemini										
11	Vietnam		[X] Buffalo		TIN [X]								Cyclone				
12	Lebanon							[X] Cedar					Rain				
13	Syria		[X] Hawk														
14	Arab Countries			[X] Falcon					~~[X] Viper **~~								
15	Pakistan		[X] Leopard		COPPER [X]		[X] Draco										
16	Georgia		[X] Lynx														
17	Turkey		[X] Wolf										Dust				
18	Colombia		[X] Ocelot														
19	Egypt		[X] Sphinx														
20	Kasakhstan		[X] Saiga														
21	Criminal / Financial	FIN[X]	[X] Spider		GOLD [X]		[X] Libra		Water [X]			Volcanos, e.g.	Tempest				
22	Activists		[X] Jackal				[X] Virgo		Wind [X]								

Zdroj: https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit?gid=1864660085#gid=1864660085

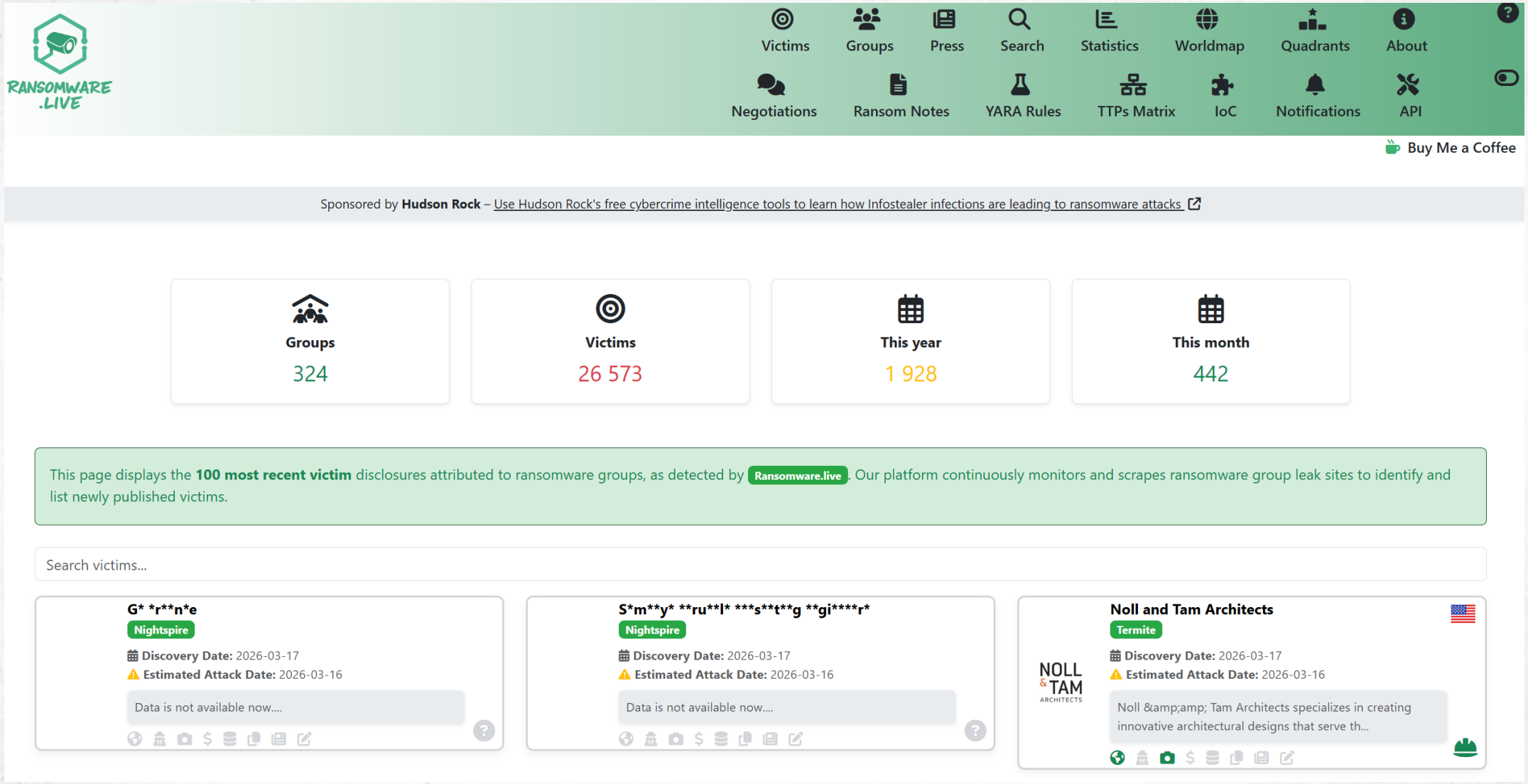
Aktuálne APT skupiny (IV.)

- skupiny útočníkov, júl 2023 – jún 2024



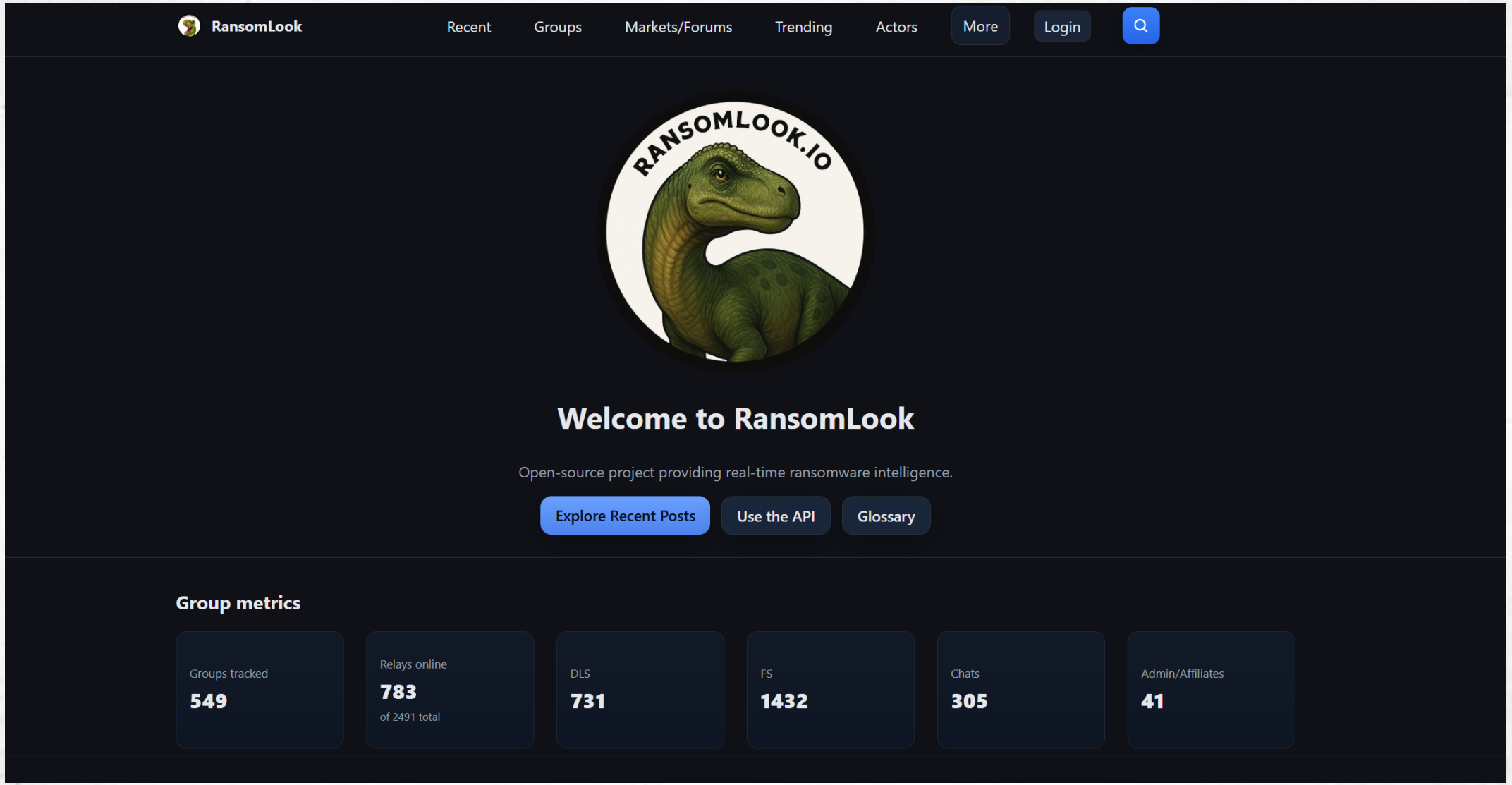
Zdroj: ENISA Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Platformy (I.)



Zdroj: https://www.ransomware.live/

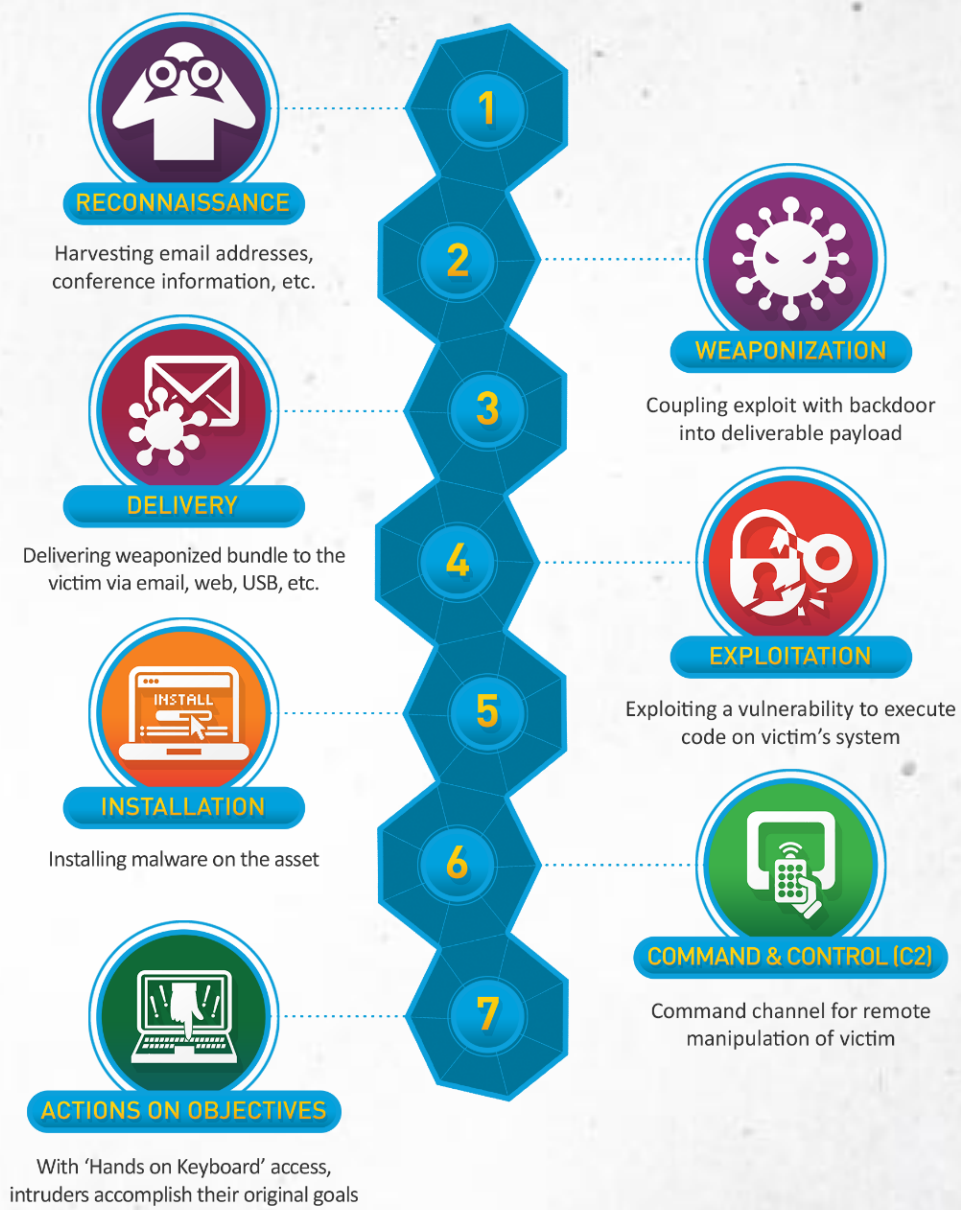
Platformy (II.)



Zdroj: https://www.ransomlook.io/

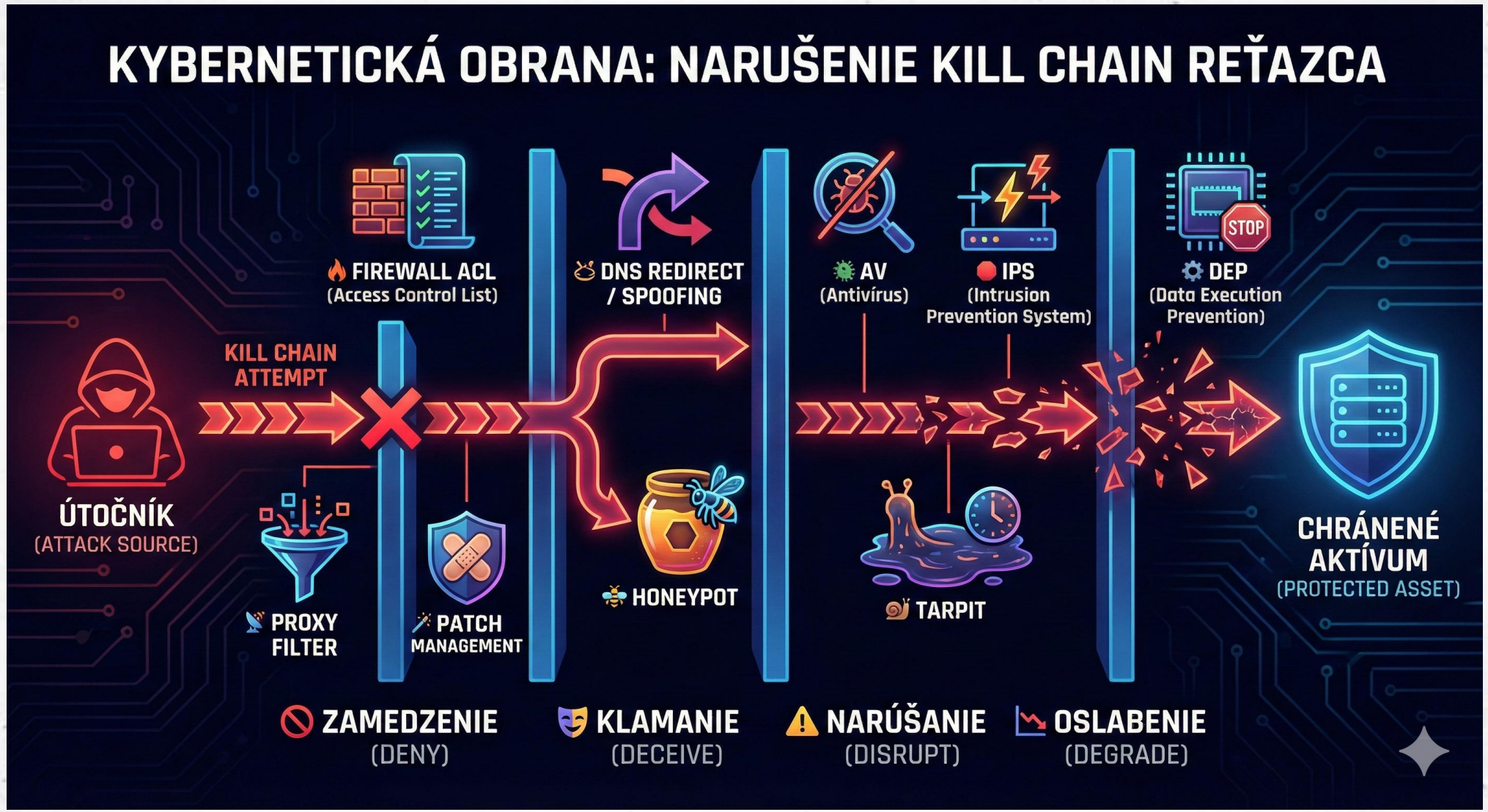
Kill-chain model (I.)

- kill chain predstavuje proces, prostredníctvom ktorého útočníci realizujú kybernetické útoky.
- spoločnosť Lockheed Martin adaptovala koncept „kill chain“ z vojenského prostredia do oblasti informačnej bezpečnosti a využila ho ako metódu modelovania prienikov do počítačových sietí.
- slúži na identifikáciu a prevenciu aktivít kybernetických prienikov.
- model identifikuje kroky, ktoré musí útočník splniť, aby dosiahol svoj cieľ.



Zdroj: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Kill-chain model (II.)

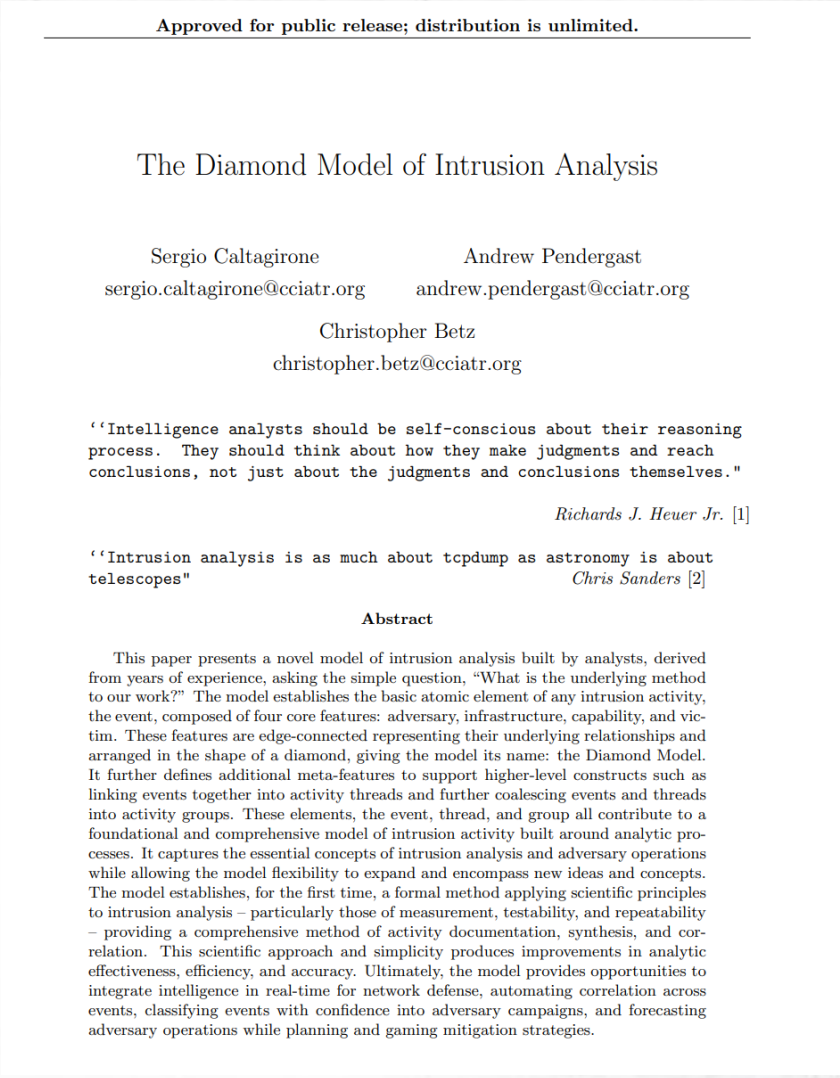


Zdroj: Obrázok vygenerovaný AI - Gemini

Diamond model (I.)

Diamond Model

- je analytický rámec používaný v spravodajstve o hrozbách na analýzu bezpečnostných incidentov a profilovanie útokov.
- pomáha analytikom systematicky zbierať, triediť a prepájať informácie o priebehu útoku a identifikovať medzery v znalostiach.
- analýzou vzťahov medzi prvkami je možné pochopiť motivácie útočníka, ciele útoku a rozsah kampane.
- Ide o dynamický proces, ktorý umožňuje „pivotovanie“ medzi prvkami modelu a tvorbu analytických hypotéz počas vyšetrovania.



Approved for public release; distribution is unlimited.

The Diamond Model of Intrusion Analysis

Sergio Caltagirone
sergio.caltagirone@cciatr.org

Andrew Pendergast
andrew.pendergast@cciatr.org

Christopher Betz
christopher.betz@cciatr.org

''Intelligence analysts should be self-conscious about their reasoning process. They should think about how they make judgments and reach conclusions, not just about the judgments and conclusions themselves."

Richards J. Heuer Jr. [1]

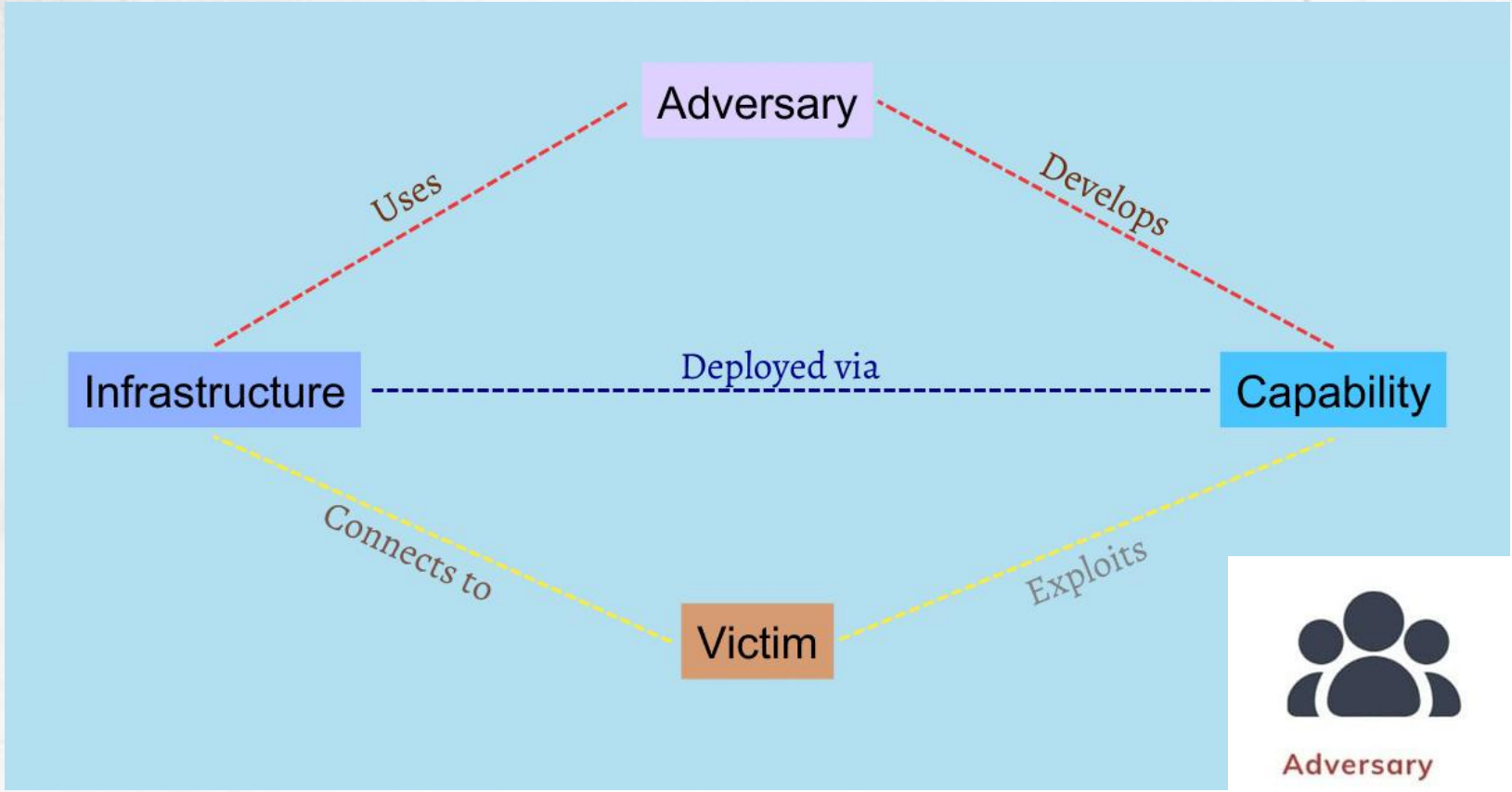
''Intrusion analysis is as much about tcpdump as astronomy is about telescopes" *Chris Sanders* [2]

Abstract

This paper presents a novel model of intrusion analysis built by analysts, derived from years of experience, asking the simple question, “What is the underlying method to our work?” The model establishes the basic atomic element of any intrusion activity, the event, composed of four core features: adversary, infrastructure, capability, and victim. These features are edge-connected representing their underlying relationships and arranged in the shape of a diamond, giving the model its name: the Diamond Model. It further defines additional meta-features to support higher-level constructs such as linking events together into activity threads and further coalescing events and threads into activity groups. These elements, the event, thread, and group all contribute to a foundational and comprehensive model of intrusion activity built around analytic processes. It captures the essential concepts of intrusion analysis and adversary operations while allowing the model flexibility to expand and encompass new ideas and concepts. The model establishes, for the first time, a formal method applying scientific principles to intrusion analysis – particularly those of measurement, testability, and repeatability – providing a comprehensive method of activity documentation, synthesis, and correlation. This scientific approach and simplicity produces improvements in analytic effectiveness, efficiency, and accuracy. Ultimately, the model provides opportunities to integrate intelligence in real-time for network defense, automating correlation across events, classifying events with confidence into adversary campaigns, and forecasting adversary operations while planning and gaming mitigation strategies.

Zdroj: https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Diamond model (II.)



Zdroj: https://cipherssecurity.com/diamond-model-of-intrusion-analysis/, https://kravensecurity.com/diamond-model-analysis/

Diamond model (III.)

Model sa zameriava na štyri kľúčové prvky:

- **útočník (adversary)**
  - aktér hrozby (interný/external, jednotlivec, skupina, organizácia), ktorý sa snaží kompromitovať systémy alebo siete s cieľom dosiahnuť svoj zámer.
- **schopnosti (capabilities)**
  - nástroje, taktiky, techniky a postupy (TTPs) útočníka, vrátane jeho arzenálu, možností zneužitia zraniteľností obete a schopnosti Command and Control (C2) – riadenia a kontroly útoku.
- **Infraštruktúra (infrastructure)**
  - fyzická a logická infraštruktúra používaná na doručovanie a riadenie útoku. Typ I: priamo kontrolovaná útočníkom Typ II: sprostredkovaná treťou stranou (napr. botnet)
- **obete (victims)**
  - cieľ útoku – zahŕňa **identitu (personu)**, **aktíva/útočný povrch** (interné a cloudové systémy) a **zraniteľnosti a vystavenia**, ktoré môže útočník zneužiť.

Zdroj: https://kravensecurity.com/diamond-model-analysis/

Diamond model (IV.)

- **7 axióm** týkajúcich sa udalostí prienikov, útočníkov a obetí (tieto axiómy je užitočné mať na pamäti pri vyšetrovaní a analýze aktivít protivníka):
  - **(1) Pre každú udalosť prieniku existuje útočník**, ktorý podniká krok smerom k zamýšľanému cieľu, pričom využíva určitú schopnosť prostredníctvom infraštruktúry proti obeti s cieľom dosiahnuť konkrétny výsledok.
  - **(2) Existuje množina útočníkov** (interní aj externí, jednotlivci, skupiny a organizácie), ktorí sa snažia kompromitovať počítačové systémy alebo siete s cieľom presadiť svoj zámer a naplniť svoje potreby.
  - **(3) Každý systém**, a tým aj každý majetok obete, **obsahuje zraniteľnosti a vystavenia**.

Diamond model (V.)

- **(4) Každá škodlivá aktivita pozostáva z dvoch alebo viacerých fáz**, ktoré musia byť úspešne vykonané postupne, aby bol dosiahnutý požadovaný výsledok.

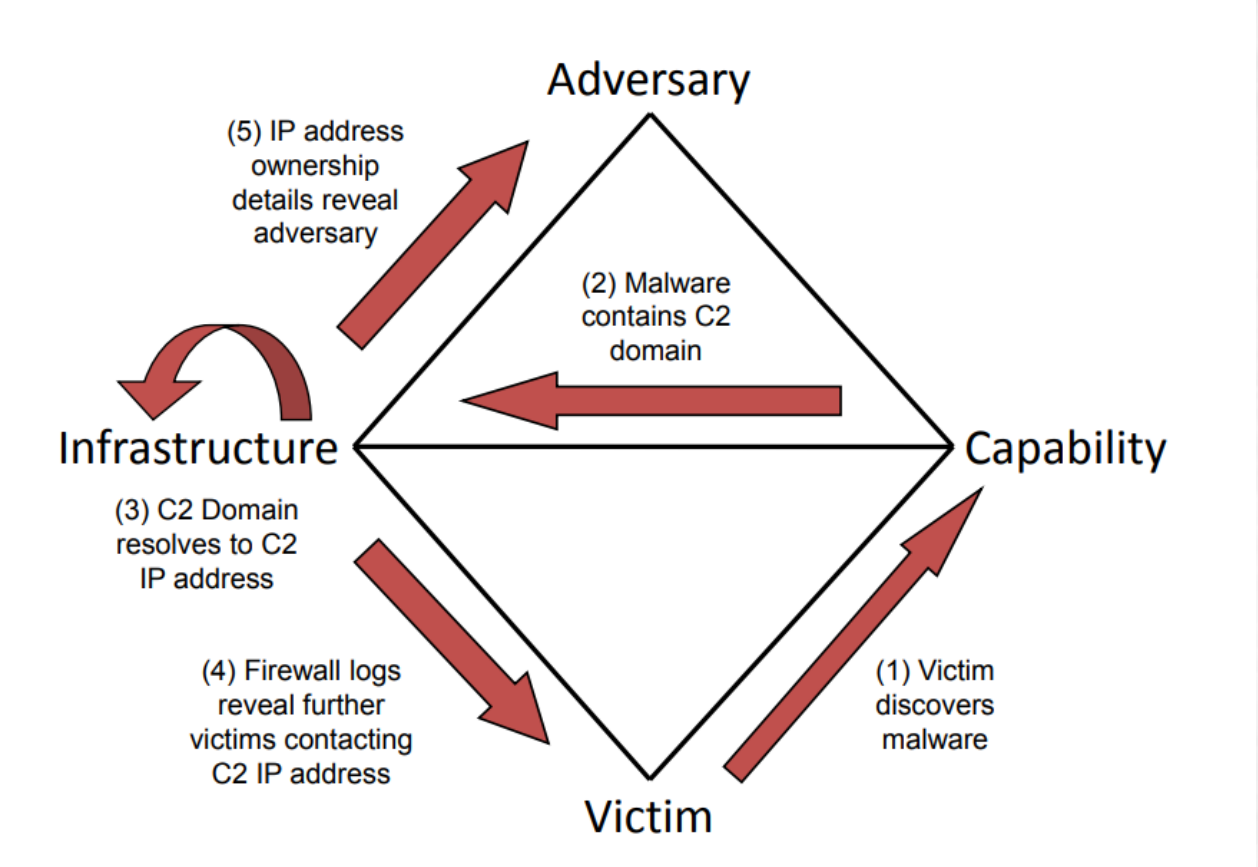
- **(5) Každá udalosť prieniku si vyžaduje jeden alebo viac externých zdrojov**, ktoré musia byť zabezpečené pred dosiahnutím úspechu.

- **(6) Medzi útočníkom a jeho obeťou (obeťami) vždy existuje vzťah**, aj keď je vzdialený, krátkodobý alebo nepriamy.

- **(7) Existuje podmnožina útočníkov**, ktorí majú motiváciu, zdroje a schopnosti dlhodobo udržiavať škodlivé účinky voči jednej alebo viacerým obetiam a zároveň odolávať zmierňujúcim opatreniam. Vzťahy medzi útočníkom a obeťou v tejto podmnožine sa označujú ako **perzistentné vzťahy útočník – obeť**.

Diamond model (VI.)

- **Obeť (Victim)** - Obeť deteguje škodlivý kód (malware) vo svojom prostredí. Ide o počiatočný bod analýzy incidentu.
- **Schopnosti (Capability)** - Analýza malvéru odhalí, že obsahuje C2 doménu (Command and Control), ktorú útočník používa na riadenie útoku.
- **Infraštruktúra (Infrastructure)** - C2 doména je preložená (DNS resolúcia) na konkrétnu C2 IP adresu, ktorá predstavuje infraštruktúru používanú útočníkom.
- **Rozšírenie na ďalšie obete** - Analýza firewallových logov ukáže, že na tú istú C2 IP adresu komunikujú aj ďalšie obete, čo naznačuje širší rozsah kampane.
- **Útočník (Adversary)** - Analýza vlastníctva IP adresy a súvisiace registračné údaje umožní identifikovať alebo bližšie profilovať útočníka.



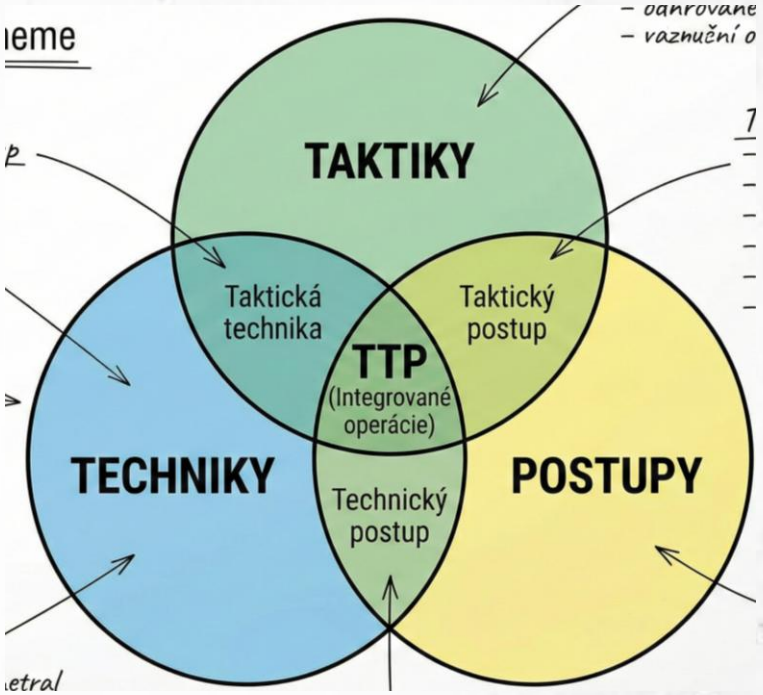
Zdroj: https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Taktiky, techniky, postupy

Tactics, Techniques and Procedures (TTPs)

- analýza TTPs slúži na pochopenie **spôsobu útoku a schopností útočníka** prostredníctvom hodnotenia jeho správania a operácií.
  - **taktiky** predstavujú strategické ciele a fázy útoku (napr. získanie prístupu, krádež dát), ktoré pomáhajú predvídať ďalšie kroky útočníka.
  - **techniky** sú konkrétne metódy a nástroje používané na realizáciu taktík (malvér, sociálne inžinierstvo), pričom ich analýza odhaľuje zraniteľnosti systému.
  - **postupy** opisujú detailné postupy, ako útočník techniky vykonáva, a poskytujú vhľad do jeho cieľov a spôsobu práce v cieľovej infraštruktúre.

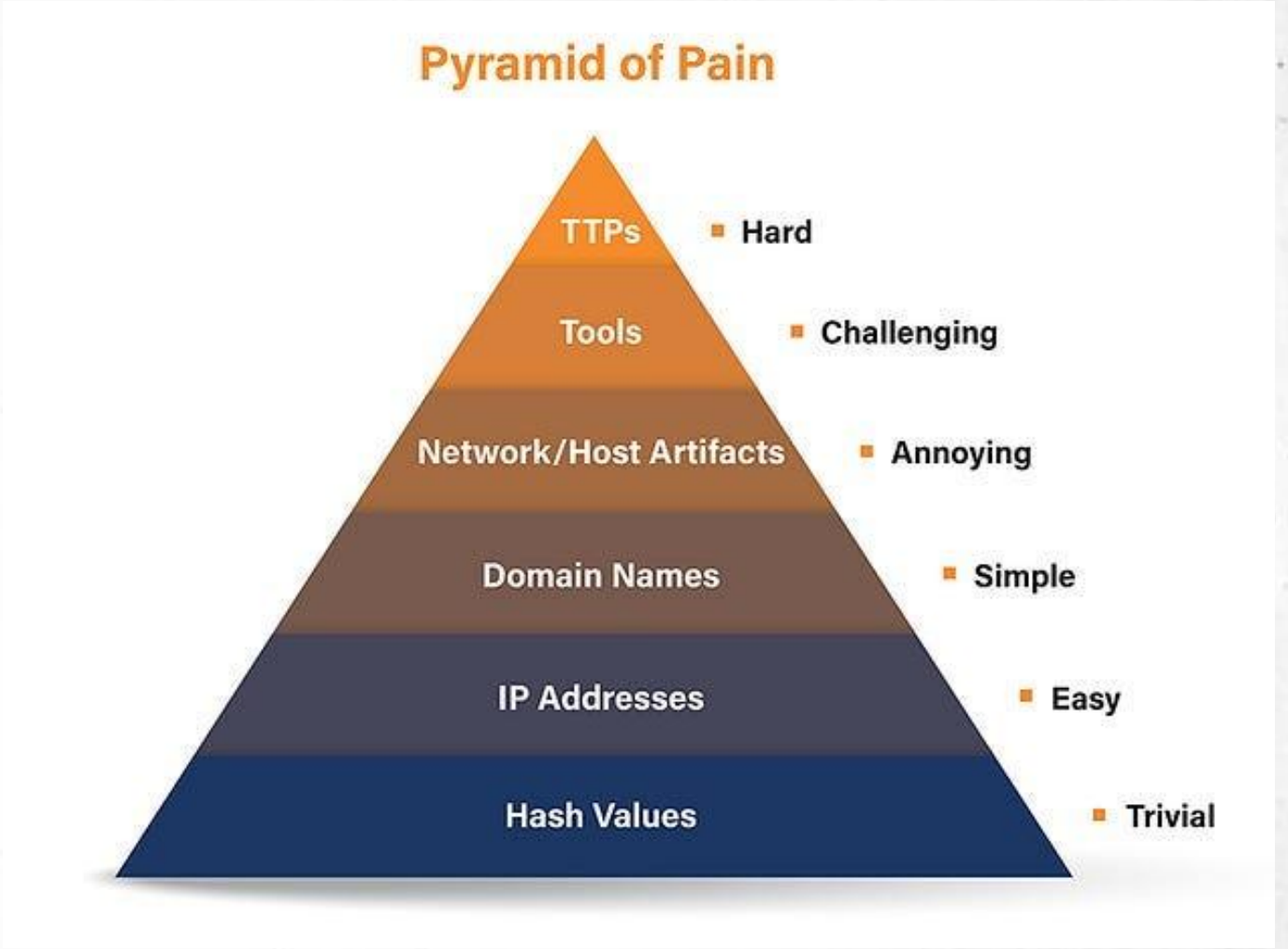
- Analýza TTPs umožňuje identifikovať jednotlivé fázy útoku, zostaviť časovú os incidentu a lepšie porozumieť rozhodovaniu a správaniu útočníka počas celého cyklu útoku.



Zdroj: Obrázok vygenerovaný AI - Gemini

Pyramída bolesti

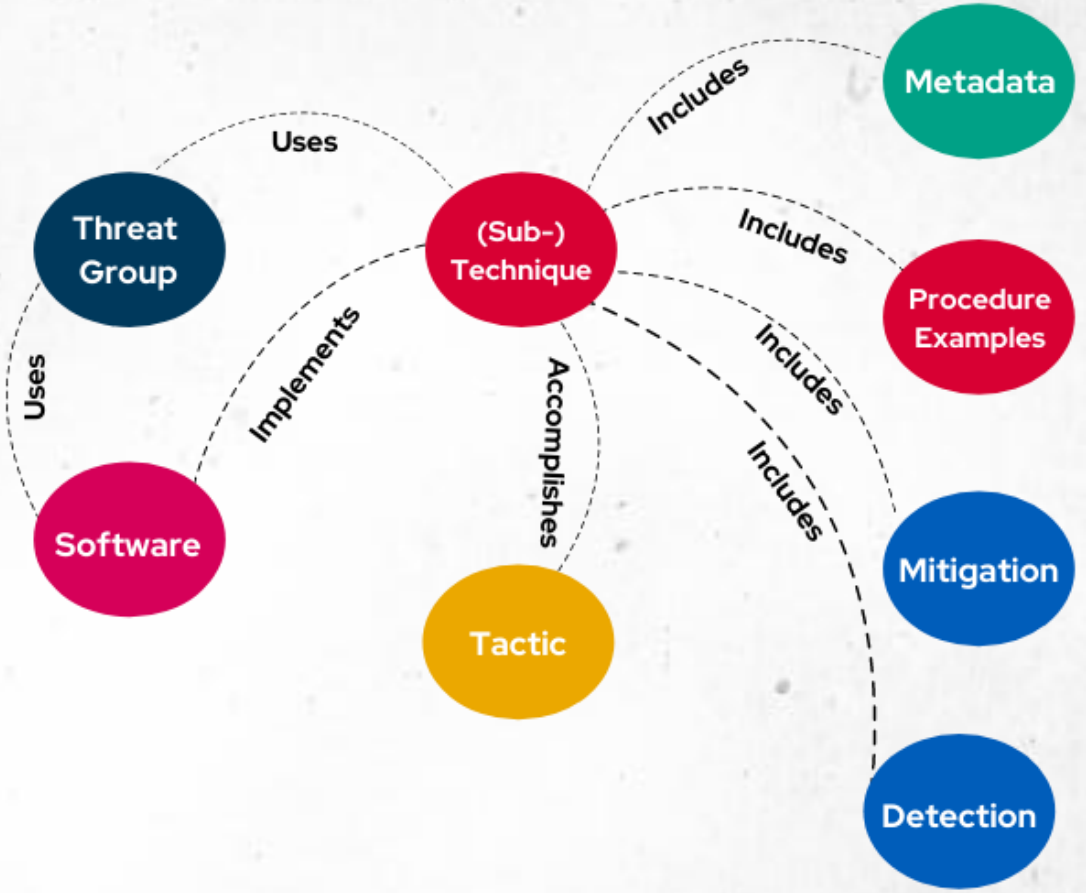
- **Pyramid of Pain**
  - konceptuálny model na klasifikáciu a prioritizáciu indikátorov kompromitácie (IOCs) podľa ich hodnoty pri detekcii a narušení útokov.
  - Nižšie úrovne (hashy, IP adresy, domény) sú ľahko získateľné, ale pre útočníka jednoduché na zmenu.
  - Vyššie úrovne (artefakty, nástroje a techniky) poskytujú hlbší pohľad na spôsob útoku a sú pre útočníka nákladnejšie na obchádzanie.
  - zameranie sa na vrchol pyramídy umožňuje efektívnejšie narušiť činnosť útočníka



Zdroj: Zdroj: https://medium.com/@fraudas/en-indicator-of-compromised-ioc-indicator-of-attack-ioa-pyramid-of-pain-2881adff6911

MITRE ATTACK RÁMEC (I.)

- **MITRE ATT&CK** je otvorený rámec (matica) vyvinutý organizáciou MITRE na profilovanie taktík a techník útočníkov a hodnotenie bezpečnostných rizík.
- jeho cieľom je zlepšiť detekciu útočníkov po kompromitácii
- pokrýva celý životný cyklus útoku, od prieskumu a prvotného prístupu až po exfiltráciu dát a dopad útoku.
- slúži ako štandardný nástroj pre threat hunterov, red tímy a obrancov a predstavuje spoločnú znalostnú bázu pre analýzu TTPs.
- vyžaduje pravidelné aktualizácie a nemusí zachytávať všetky existujúce alebo nové útočné techniky.



Zdroj: https://www.picussecurity.com/resource/blog/mitre-attack-framework-beginners-guide

MITRE ATTACK RÁMEC (II.)

MITRE | ATT&CK®

Matrices | Tactics | Techniques | Defenses | CTI | Resources | Benefactors | Contribute | Blog | Search

ATT&CK®

Get Started | Take a Tour

Contribute | Blog

FAQ | Random Page

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

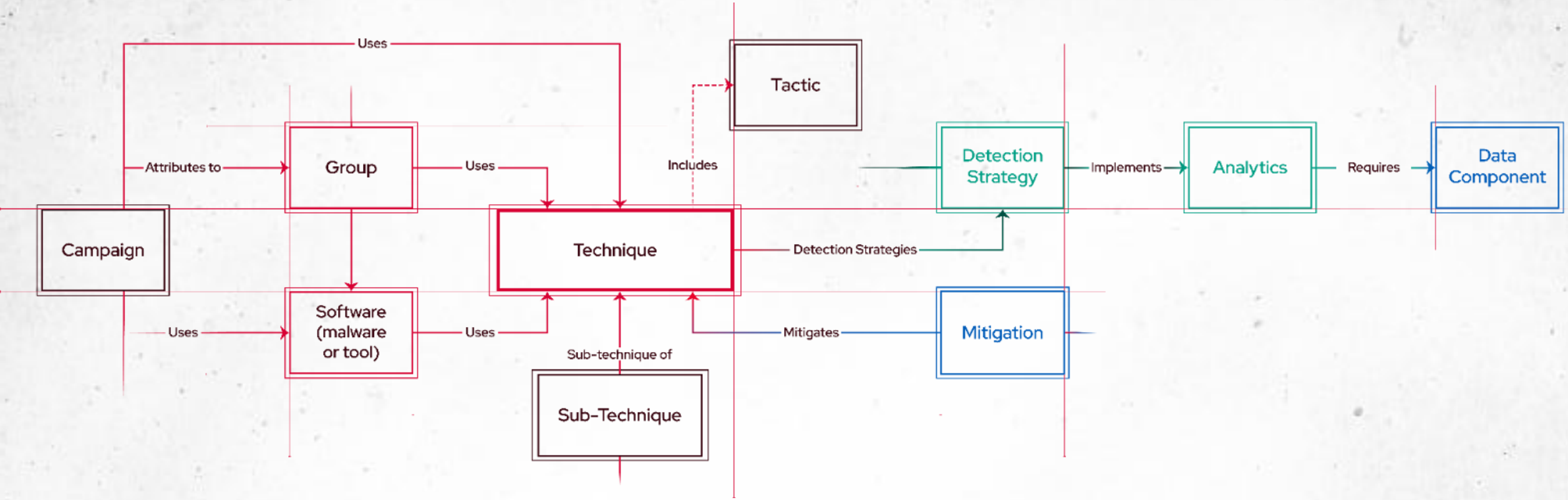
ATT&CK Matrix for Enterprise

layout: side | show sub-techniques | hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques	18 techniques	9 techniques	15 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (13)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote		Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart	Build Image on Host	Exploitation for Credential	Cloud Infrastructure Discovery	Remote Service	Automated Collection		Exfiltration	Data Manipulation (3)
	Develop					Debugger Evasion		Cloud Service					

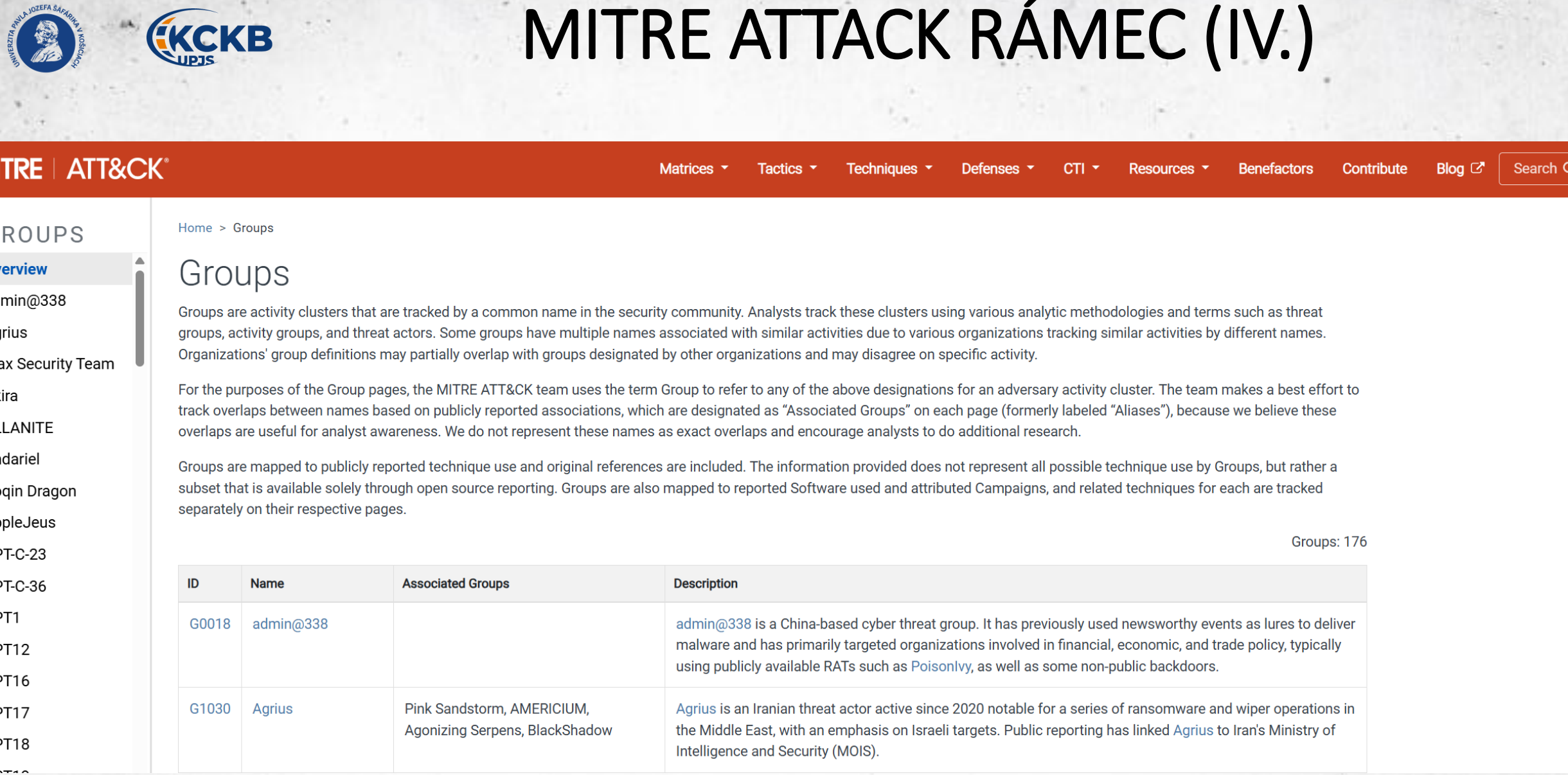
Zdroj: https://attack.mitre.org/

MITRE ATTACK RÁMEC (III.)



Zdroj: https://www.picussecurity.com/resource/blog/mitre-attack-framework-beginners-guide

MITRE ATTACK RÁMEC (IV.)



Zdroj: https://attack.mitre.org/

MITRE ATTACK RÁMEC (V.)

SOFTWARE

Software

Software is a generic term for custom or commercial code, operating system utilities, open-source software, or other tools used to conduct behavior modeled in ATT&CK. Some instances of software have multiple names associated with the same instance due to various organizations tracking the same set of software by different names. The team makes a best effort to track overlaps between names based on publicly reported associations, which are designated as "Associated Software" on each page (formerly labeled "Aliases"), because we believe these overlaps are useful for analyst awareness.

Software entries include publicly reported technique use or capability to use a technique and may be mapped to Groups who have been reported to use that Software. The information provided does not represent all possible technique use by a piece of Software, but rather a subset that is available solely through open source reporting.

- Tool - Commercial, open-source, built-in, or publicly available software that could be used by a defender, pen tester, red teamer, or an adversary. This category includes both software that generally is not found on an enterprise system as well as software generally available as part of an operating system that is already present in an environment. Examples include PsExec, Metasploit, Mimikatz, as well as Windows utilities such as Net, netstat, Tasklist, etc.

- Malware - Commercial, custom closed source, or open source software intended to be used for malicious purposes by adversaries. Examples include PlugX, CHOPSTICK, etc.

Software: 910

ID	Name	Associated Software	Description
S0066	3PARA RAT		3PARA RAT is a remote access tool (RAT) programmed in C++ that has been used by Putter Panda.
S0065	4H RAT		4H RAT is malware that has been used by Putter Panda since at least 2007.
S0677	AADInternals		AADInternals is a PowerShell-based framework for administering, enumerating, and exploiting Azure Active Directory. The tool is publicly available on GitHub.
S0469	ABK		ABK is a downloader that has been used by BRONZE BUTLER since at least 2019.

Zdroj: https://attack.mitre.org/

MITRE ATTACK RÁMEC (VI.)

MITRE | ATT&CK®

Matrices | Tactics | Techniques | Defenses | CTI | Resources | Benefactors | Contribute | Blog | Search

MITIGATIONS

- Enterprise
  - Account Use Policies
  - Active Directory Configuration
  - Antivirus/Antimalware
  - Application Developer Guidance
  - Application Isolation and Sandboxing
  - Audit
  - Behavior Prevention on Endpoint
  - Boot Integrity
  - Code Signing
  - Credential Access Protection
  - Data Backup
  - Data Loss Prevention
  - Disable or Remove Feature or Program
  - Do Not Mitigate
  - Encrypt Sensitive Information
  - Environment Variable Permissions

Home > Mitigations > Enterprise

Enterprise Mitigations

Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.

Mitigations: 44

ID	Name	Description
M1036	Account Use Policies	Account Use Policies help mitigate unauthorized access by configuring and enforcing rules that govern how and when accounts can be used. These policies include enforcing account lockout mechanisms, restricting login times, and setting inactivity timeouts. Proper configuration of these policies reduces the risk of brute-force attacks, credential theft, and unauthorized access by limiting the opportunities for malicious actors to exploit accounts. This mitigation can be implemented through the following measures:
M1015	Active Directory Configuration	Implement robust Active Directory (AD) configurations using group policies to secure user accounts, control access, and minimize the attack surface. AD configurations enable centralized control over account settings, logon policies, and permissions, reducing the risk of unauthorized access and lateral movement within the network. This mitigation can be implemented through the following measures:
M1049	Antivirus/Antimalware	Antivirus/Antimalware solutions utilize signatures, heuristics, and behavioral analysis to detect, block, and remediate malicious software, including viruses, trojans, ransomware, and spyware. These solutions continuously monitor endpoints and systems for known malicious patterns and suspicious behaviors that indicate compromise. Antivirus/Antimalware software should be deployed across all devices, with automated updates to ensure protection against the latest threats. This mitigation can be implemented through the following measures:
M1013	Application Developer Guidance	Application Developer Guidance focuses on providing developers with the knowledge, tools, and best practices needed to write secure code, reduce vulnerabilities, and implement secure design principles. By integrating security throughout the software development lifecycle (SDLC), this mitigation aims to prevent the introduction of exploitable weaknesses in applications, systems, and APIs. This mitigation can be implemented through the following measures:

Zdroj: https://attack.mitre.org/

MITRE ATTACK RÁMEC (VII.)

MITRE | ATT&CK®

Matrices Tactics Techniques Defenses CTI Resources Benefactors Contribute Blog Search

ANALYTICS

Overview

Home > Analytics

Analytics

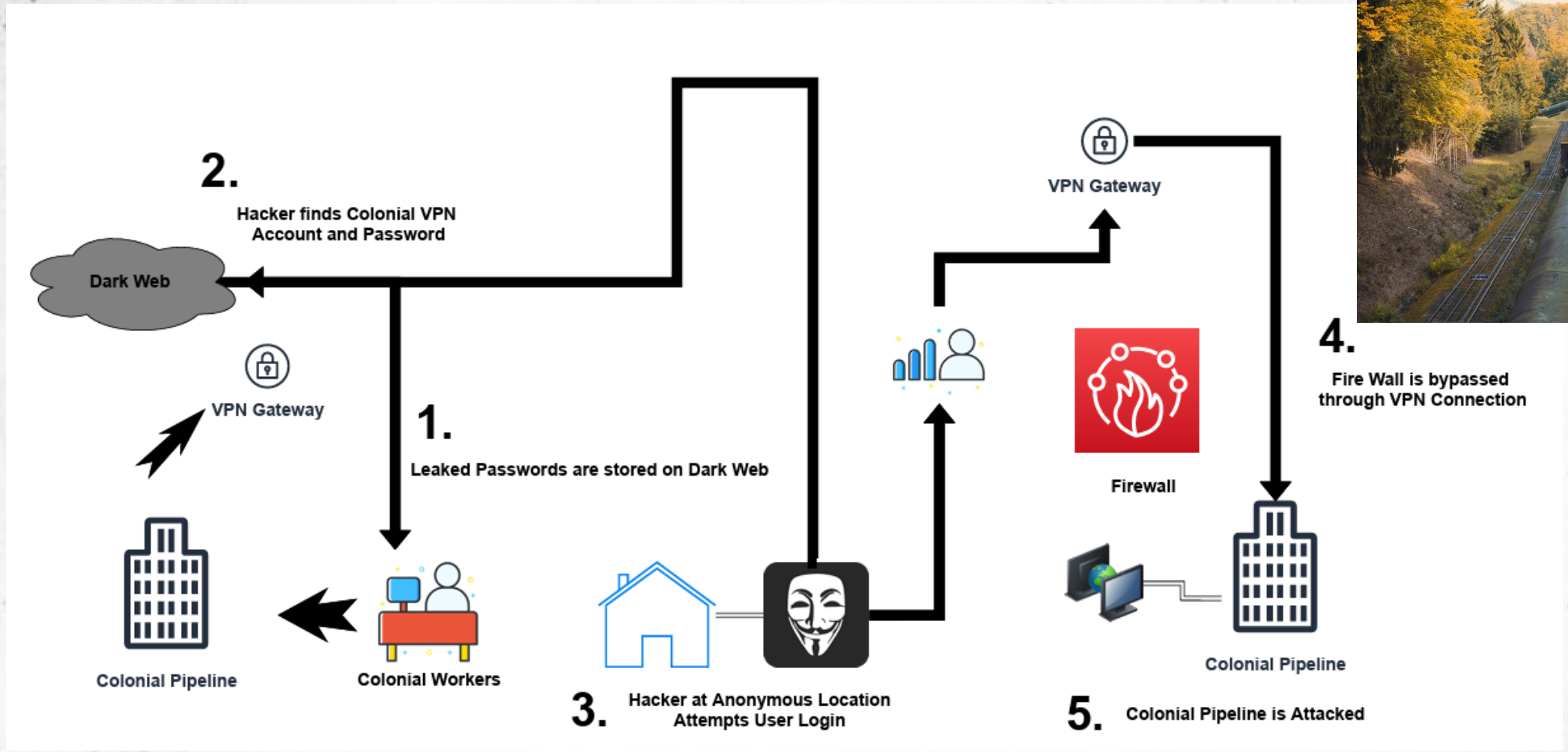
Analytics contain platform-specific detection logic and represent the implementation details of a detection strategy.

Analytics: 2032

ID	Platform	Domain ▼	Detection Strategy	Description
AN0001	IaaS	Enterprise	DET0001	Detects access attempts to cloud instance metadata endpoints (e.g., 169.254.169.254) from virtual machines or containerized workloads. This includes both direct access and SSRF exploitation patterns.
AN0002	Windows	Enterprise	DET0002	Detects non-standard processes (e.g., PowerShell, python.exe, rundll32.exe) making outbound connections using publish/subscribe protocols (e.g., MQTT, AMQP) over non-browser, encrypted channels, often beaconing to message brokers.
AN0003	Linux	Enterprise	DET0002	Detects CLI tools (e.g., mosquitto_pub, nc, python scripts) interacting with pub/sub brokers using unusual topic names, high-frequency publication rates, or obfuscated payloads to non-standard hosts.
AN0004	macOS	Enterprise	DET0002	Detects osascript, curl, or custom binaries interacting with XMPP/MQTT brokers in unapproved destinations with encrypted payloads or frequent POST-like requests to broker URIs.
AN0005	Network Devices	Enterprise	DET0002	Detects pub/sub traffic over unusual ports, high-frequency topic publications, and connections to known-bad or dynamic broker endpoints outside allowlisted infrastructure.
AN0006	Windows	Enterprise	DET0003	Adversary uses built-in tools such as 'net user /add /domain' or PowerShell to create a domain user account. The behavior chain includes: (1) suspicious process execution on a domain controller followed by (2) user account creation event (Event ID 4720) on the same host.

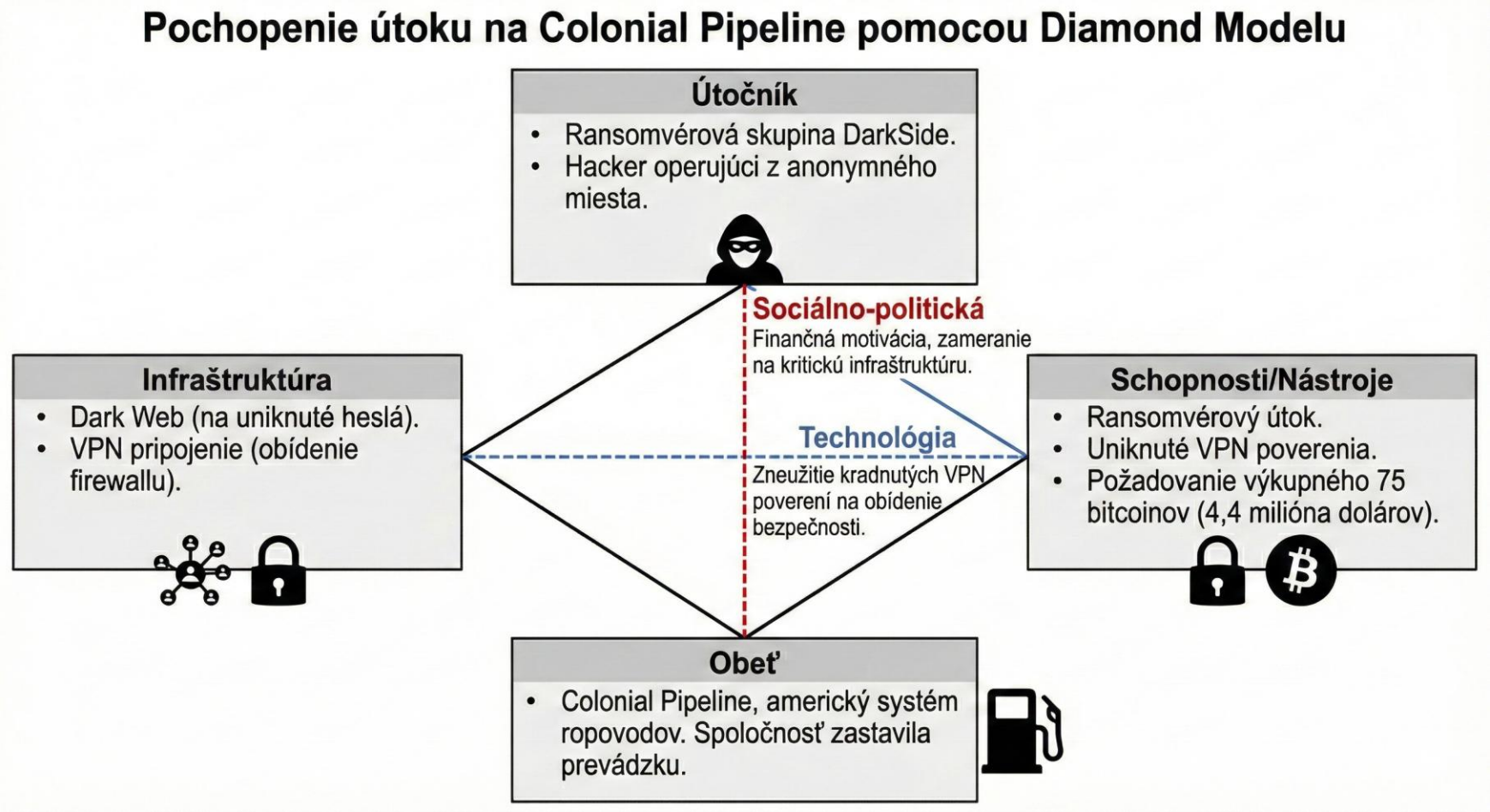
Zdroj: https://attack.mitre.org/

Colonial pipeline (I.)



Zdroj: Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023, May). A review of colonial pipeline ransomware attack. In *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)* (pp. 8-15). IEEE, https://medium.com/@tahirbalarabe2/colonial-pipeline-cyber-attack-root-causes-impact-and-key-takeaways-f9587d26f19f

Colonial pipeline (II.)



Zdroj: Obrázok generovaný AI - Gemini

Colonial pipeline (III.)

- **Adversary (Útočník)**
  - útok uskutočnila ransomvérová skupina známa ako **DarkSide**.
  - útočník operoval z „anonymného miesta"

- **Victim (Obeť)**
  - primárnou obeťou bola spoločnosť **Colonial Pipeline**, americký systém ropovodov.
  - útok spôsobil zastavenie prevádzky spoločnosti.

- **Capability (Schopnosti/Nástroje)**
  - hlavnou použitou technikou bol **ransomvérový útok**, ktorý zašifroval dáta a požadoval výkupné.
  - na získanie počiatočného prístupu útočník použil **uniknuté heslá** a účet k **Colonial VPN**, ktoré našiel na Dark Webe.
  - spoločnosť nakoniec zaplatila výkupné vo výške 75 bitcoinov (4,4 milióna dolárov).

Colonial pipeline (IV.)

- **Infrastructure (Infraštruktúra)**
  - útočníci využili **Dark Web** na nájdenie a uloženie uniknutých prihlasovacích údajov.
  - na obídenie firewallu a získanie prístupu do siete Colonial Pipeline bolo použité **VPN pripojenie** cez VPN Gateway.

- **Prepojenia (Axes):**
  - **social-Political (motivácia) -** motivácia bola primárne finančná, zameraná na získanie vysokého výkupného od kritickej infraštruktúry.
  - **technology (technológia) -** technologický postup spočíval v zneužití platných (aj keď kradnutých) VPN poverení na obídenie bezpečnostných prvkov, ako je firewall, čo umožnilo následné nasadenie ransomvéru.

Colonial pipeline (V.)

Ransomvérový útok na Colonial Pipeline (2021)

- **popis:** Ransomvérová skupina DarkSide sa zamerala na spoločnosť Colonial Pipeline, čo spôsobilo narušenie dodávok palív na východnom pobreží USA a odhalilo zraniteľnosti kritickej infraštruktúry.

MITRE ATT&CK rámec:

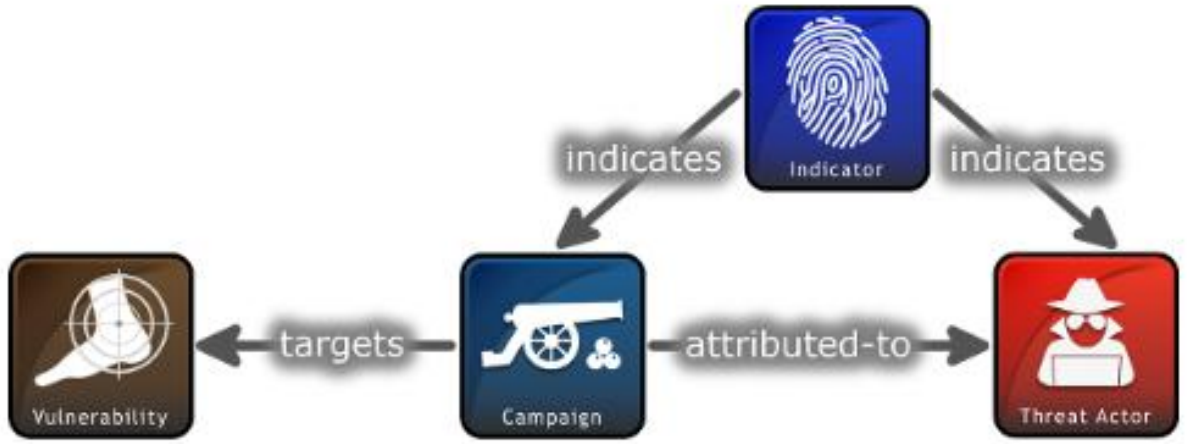
- **phishing (T1566):** Pravdepodobný počiatočný prístup prostredníctvom kompromitovaných prihlasovacích údajov alebo phishingových e-mailov.
- **zneužitie vzdialených služieb (T1210):** Boli zneužité sieťové zraniteľnosti.
- **šifrovanie dát s cieľom dosiahnuť dopad (T1486):** Ransomvér zašifroval kritické systémy.
- **exfiltrácia (TA0010):** Ukradnuté dáta boli použité ako páka na vymáhanie výkupného.

STIX

Structured Threat Information Expression (STIX) is a language and serialization format used to exchange cyber threat intelligence (CTI).

STIX enables organizations to share CTI with one another in a consistent and machine readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks

STIX is designed to improve many different c collaborative threat analysis, automated threa detection and response, and more.



STIX Relationship Example

Zdroj: https://oasis-open.github.io/cti-documentation/

On February 10, Threat Analysis Group discovered two distinct North Korean
• Threat Actor

government-backed attacker groups exploiting a remote code execution
• Attack Patte...

vulnerability in

Chrome, CVE-2022-0609 . These groups' activity has been publicly tracked as
• Tool • Vulnerabilit...

Operation
• Campaign

Dream Job and Operation AppleJeus .
• Campaign

We observed the campaigns targeting U.S. based organizations spanning
• Identity

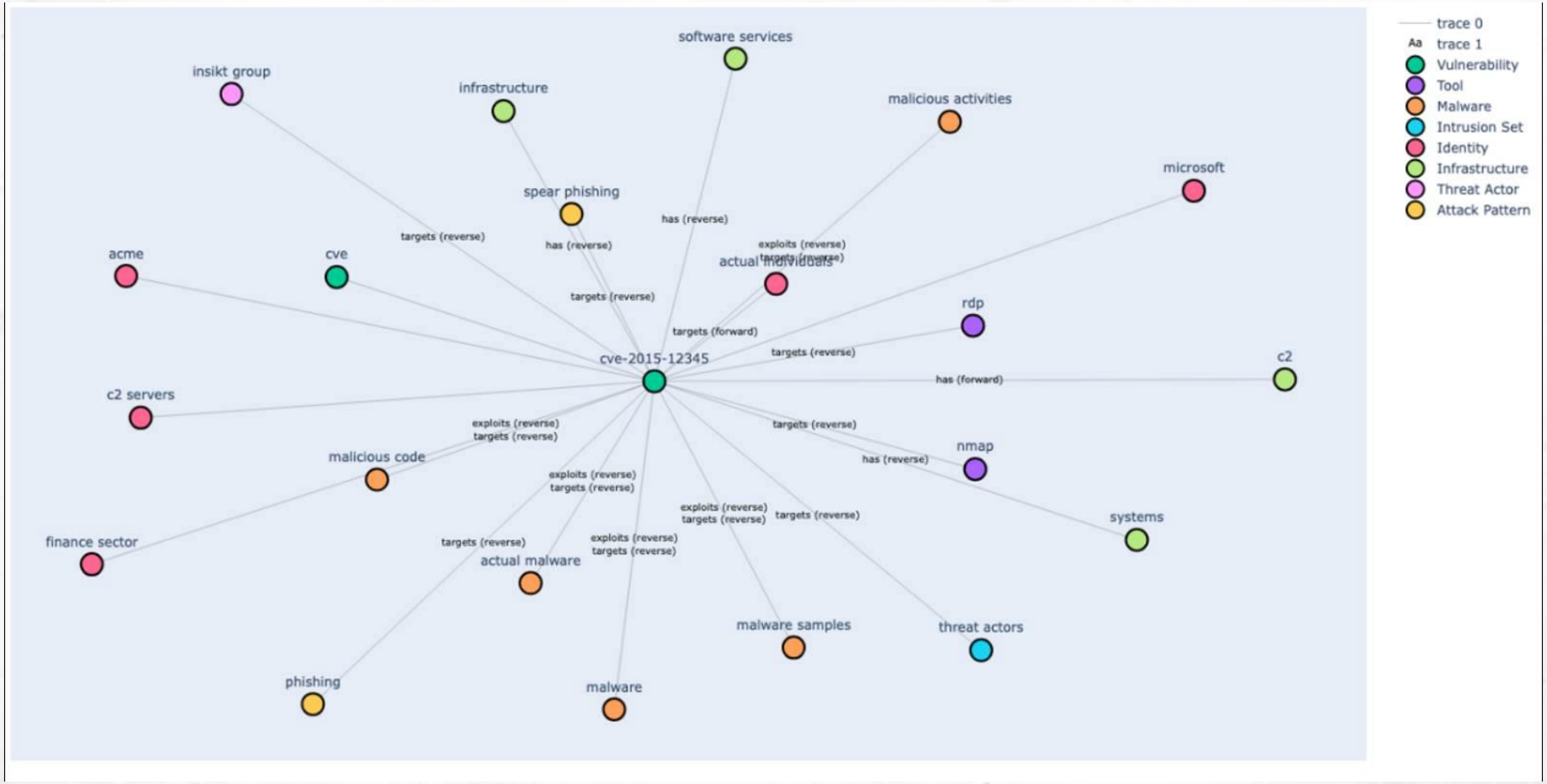
news media,

Label Types

- Attack Pattern a
- Campaign c
- Course of Action 2
- Grouping g
- Identity i
- Indicator 3
- Infrastructure 4
- Intrusion Set s
- Location l
- Malware m
- Malware Analysis n
- Note o
- Observed Data d
- Opinion p
- Report r
- Threat Actor t
- Tool 0
- Vulnerability u

Aktivita

- Worok
- Výber atribútov + grafová reprezentácia
- Vynechať atribúty: Grouping, Intrusion Set, Note, Opinion, Report (+ ďalšie nerelevantné)



KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

meno.priezvisko@upjs.sk

https://cyberawareness.sk