



Kybernetické bezpečnostné incidenty a ich riešenie

Ján Doboš

Národné centrum kybernetickej bezpečnosti SK-CERT
Národný bezpečnostný úrad



I. ČO CHRÁNIME?



Dáta sú ukladané, spracovávané, vyhodnocované, vizualizované, ...



Dáta sú ukladané, spracovávané, vyhodnocované, vizualizované, ...
... Hardware, software, informačné systémy, procesy

I. KTO NÁS OHROZUJE?



I. KTO NÁS OHROZUJE? MOTIVÁCIA/SCHOPNOSTI



Script-kiddies, Hacktivists, ...
... Cybercriminals, APT

- Pasívne/aktívne zapojenie existujúcich hackerských skupín
- Komunitné hackerské skupiny ako nový trend
 - Verbovanie
 - Šírenie informácií a dezinformácií
 - Vzájomná výmena informácií, know-how, malwaru, ...
 - Inovatívne myšlienky
 - Absencia jednotného prístupu bezpečnostnej komunity ku komunitným akciám
- Monitorovanie aktivity hackerských skupín (dokonca aj komerčné služby)
 - <https://apt.etda.or.th/cgi-bin/listgroups.cgi> (337 APT, 49 other, 38 unknown)
 - <https://cyberknow.medium.com/update-18-2022-russia-ukraine-war-cyber-group-tracker-september-7-61c84b90f065> (použité v nasledujúcich slidoch)

I. SKUPINY AKTIVIZOVANÉ V RÁMCI UA-RU KONFLIKTU (CK)

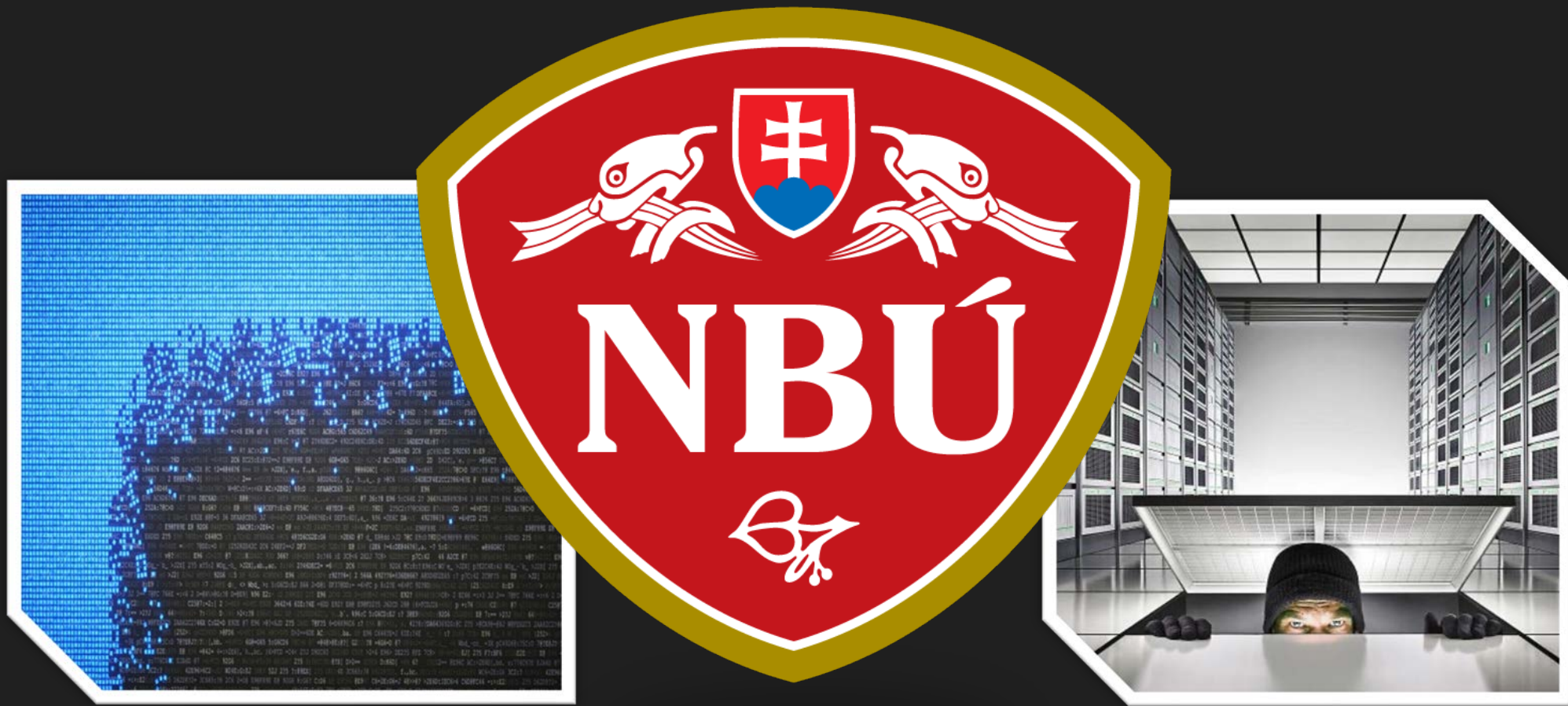
08 SEP 2022 - CYBERKNOW - CYBERTRACKER - RUSSIA - UKRAINE WAR

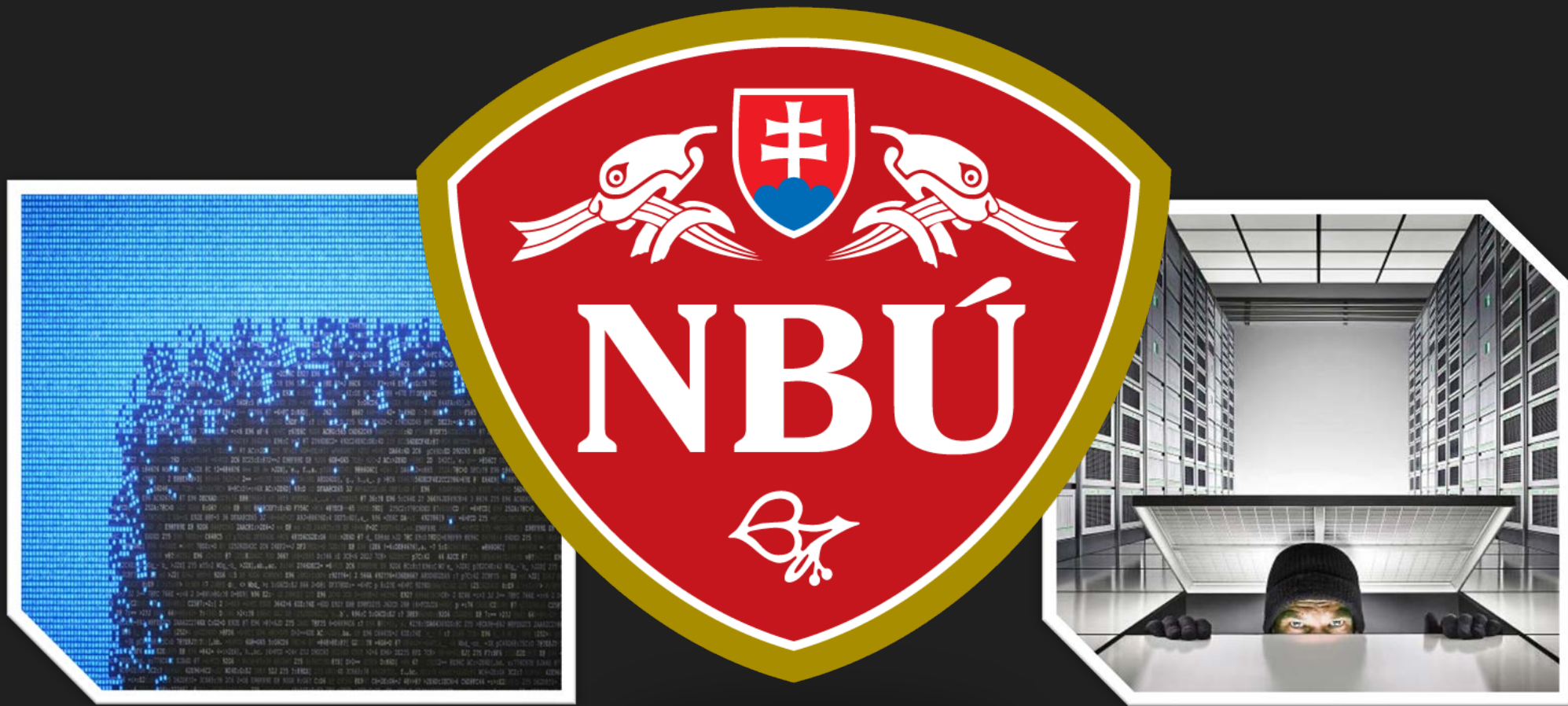
Support	Name	Actions	Comms	Support	Name	Actions	Comms	Support	Name	Actions	Comms
Ukraine	SHDWSec (Anon)	Hack/DDoS	Twitter	Russia	RaHDit	Hack	Telegram	Russia	JokerDPR	Psyops/Dox	Telegram
Ukraine	N3UR0515 (Anon)	DDoS	Twitter	Russia	Xaknet	Hack	Telegram	Russia	Vera	Botnet	Telegram
Ukraine	Shadow_Xor (Anon)	Databreach	Twitter	Russia	Killnet	DDoS	Telegram				
Ukraine	Squad303 (Anon)	DDoS/SMS	Twitter	Russia	DDoS Hacktivist Team	DDoS	Telegram	State-Sponsored			
Ukraine	GhostSec (Anon)	Hack	Twitter	Russia	Zsecnet	Dox/DDoS	Telegram	Russia	GhostWriter	Hack	UNK
Ukraine	HAL9000 (Anon)	Hack/DDoS	Twitter	Russia	DivisionZ	DDoS	Telegram	Russia	SandWorm	Hack/Wiper	UNK
Ukraine	RedCult (Anon)	Hack/DDoS	Twitter	Russia	ZOV cyber army	Hack/Psyops	Telegram	Russia	Gamaredon	Hack/Wiper	UNK
Ukraine	KelvinSecurity Hacking Team	Hack	Telegram	Russia	Cyber Front Z	Psyop/Dox	Telegram	Russia	DEV-0586	Hack/Wiper	UNK
Ukraine	SecJuice	OSINT/Psyop	Twitter	Russia	Info Front VoZddie	Psyop/DDoS	Telegram	Russia	DEV-0665	Hack/Wiper	UNK
Ukraine	Belarusian Cyber-Partisans	Ransomware	Twitter	Russia	Cyber Army of Russia	DDoS/psyops	Telegram	Russia	FancyBear/APT28	Hack/Wiper	UNK
Ukraine	BeeHive Cybersecurity	Hack/Sec	Twitter	Russia	Legion	DDoS	Telegram	Ukraine	IT Army of Ukraine	DDoS	Telegram
Ukraine	Stand for Ukraine	Hack/ DDoS	UNK	Russia	Beregini	Pysop/Dox	Telegram	Ukraine	Internet Forces of Ukraine	Pysops	UNK
Ukraine	HackenClub	DDoS/hack	Twitter	Russia	NoName057(16)	DDoS/Hack	Telegram	Ukraine	US CyberCom	Hack	UNK
Ukraine	Spot	Hack	Twitter	Russia	ZSNOSINT	Pysops/Dox	Telegram	UNK	MustangPanda	Hack	UNK
Ukraine	DumpForums	Hack	Telegram	Russia	FRwLteam	Hack/DDoS	Telegram	UNK	Curious George	Hack	UNK
Ukraine	studentcyberarmy	DDoS	telegram	Russia	Zarya	Hack	Telegram	Russia	Turla APT	Hack	UNK
Ukraine	Joint Cyber Centre (Onefist)	Hack/DDoS	Twitter	Russia	Deadnet	DDoS	Telegram	Russia	SaintBear/TA471	Hack	UNK
Ukraine	CybWar	DDoS/Leaks	Telegram	Russia	RedHackersAlliance	DDoS	Telegram	UNK	TontoTeam	Hack	UNK
Ukraine	DarkLulz	Hack	Twitter	Russia	Blood Pirates	DDoS	Telegram	UNK	Space Pirates	Hack	UNK
Ukraine	ShadowS3c	Hack	Twitter	Russia	Wizard Spider (Trickbot Crew)	Ransomware	UNK	UNK	Scarab	Hack	UNK
Ukraine	KromSec	Hack/DDoS	Telegram	Russia	404Cyber	DDoS/Hack	Telegram	Russia	Calisto	Hack	UNK
Ukraine	KiraSec	Hack/DDoS	Twitter	Russia	Anonymous Russia	DDoS	Telegram				
Ukraine	CyberSoldier	DDoS	Telegram	Russia	NBP Hackers	DDoS/Hack	Telegram	KEY:			
Ukraine	CyberPalyanitsa	DDoS	Telegram	Russia	Phoenix	DDoS/Hack	Telegram	Total Groups	84		
Ukraine	Haydamaki	DDoS	Telegram	Russia	KillMilk	DDoS/Hack	Telegram	Added	13		
Ukraine	Ciberwars	DDoS	Telegram	Russia	Graph	DDoS	Telegram	Removed	23		
Ukraine	DDoS_separ	DDoS	Telegram	Russia	1877Team	DDoS/Deface/H	Telegram				
Ukraine	2402Team	Hack	Telegram	Russia	ALtahrea Team	DDoS/Hack	Telegram	Is for New Groups			
Ukraine	DarkWolf	DDoS/Deface	Telegram	Russia	QBotDDoS (Mirai)	DDoS/Botnet	Telegram	Pro-Russian	43	Highest ever	
Ukraine	Thraxman	Hack	Twitter	Russia	Blood Pirates Kazakhstan	DDoS/Botnet	Telegram	Pro-Ukraine	35		
Ukraine	NAFO	Psyop/Meme	Twitter	Russia	KoranAttack	DDoS/Dox	Telegram	UNK	5		
Ukraine	Op Anonymous Italia Reborn	Hack	Twitter	Russia	NEKILLNET	DDoS	Telegram				



I. KTO NÁS OHROZUJE?







Zabezpečenie kybernetickej bezpečnosti IKT systémov a dát
Potreba vyhodnocovania obsahu informácií





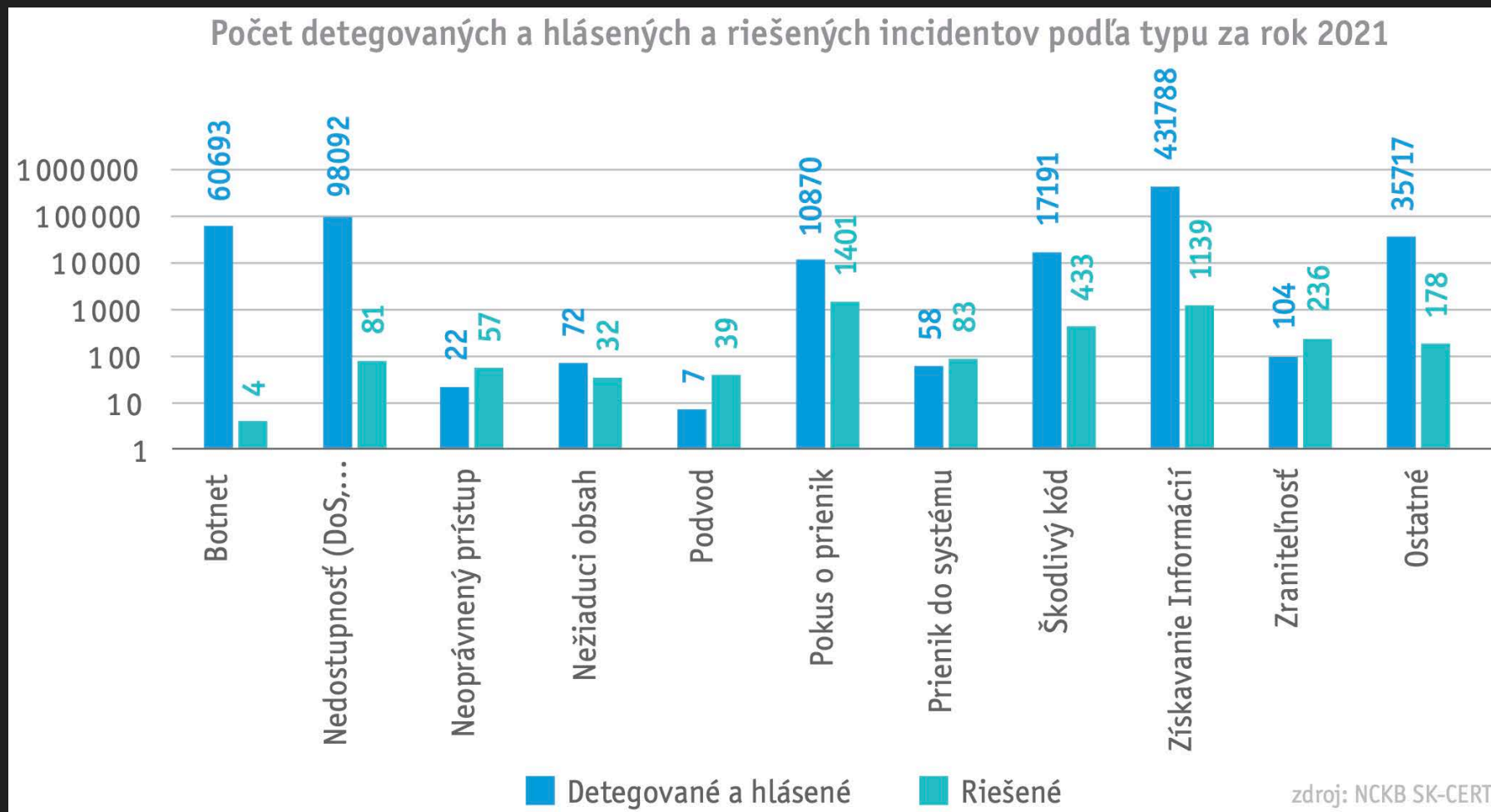
Akákoľvek udalosť s negatívnym vplyvom na kybernetickú bezpečnosť...
... Porušenie triády CIA, bezpečnostnej politiky alebo záväznej metodiky

- k) kybernetickým bezpečnostným incidentom akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je
1. strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,
 2. obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
 3. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
 4. ohrozenie bezpečnosti informácií,

§ 3, Zákon o kybernetickej bezpečnosti, 69/2018, písmeno k)

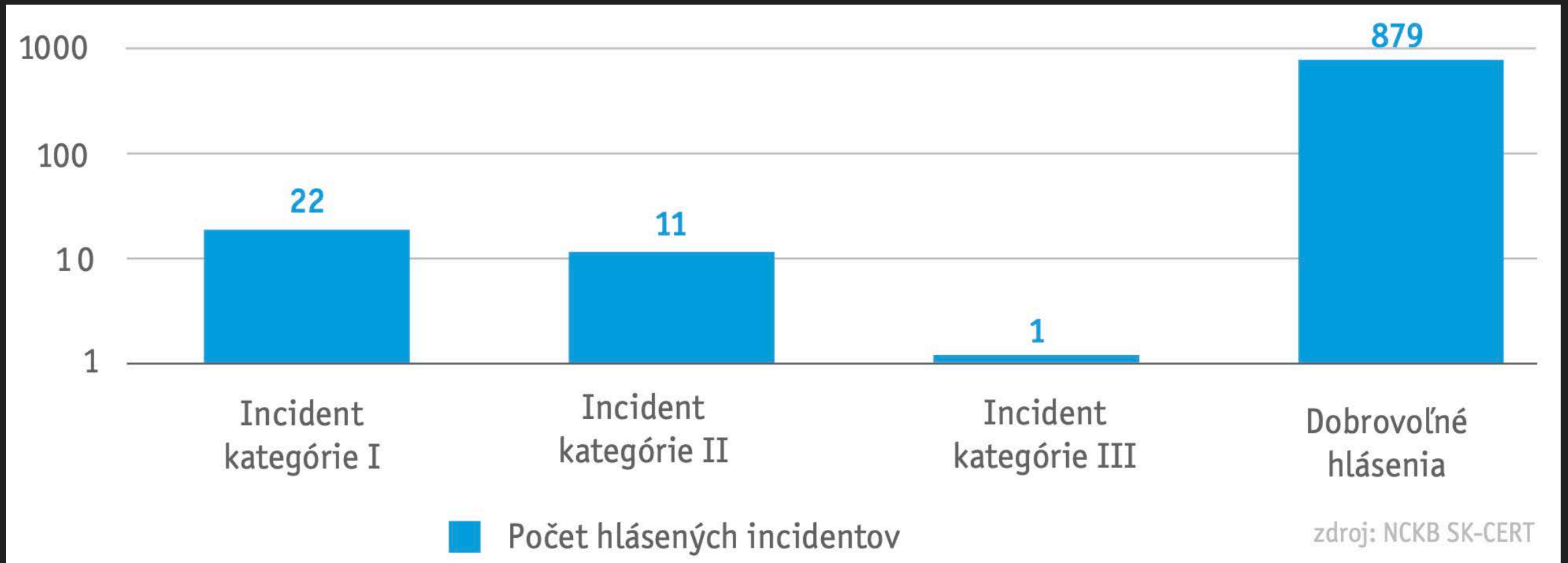
<https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/>

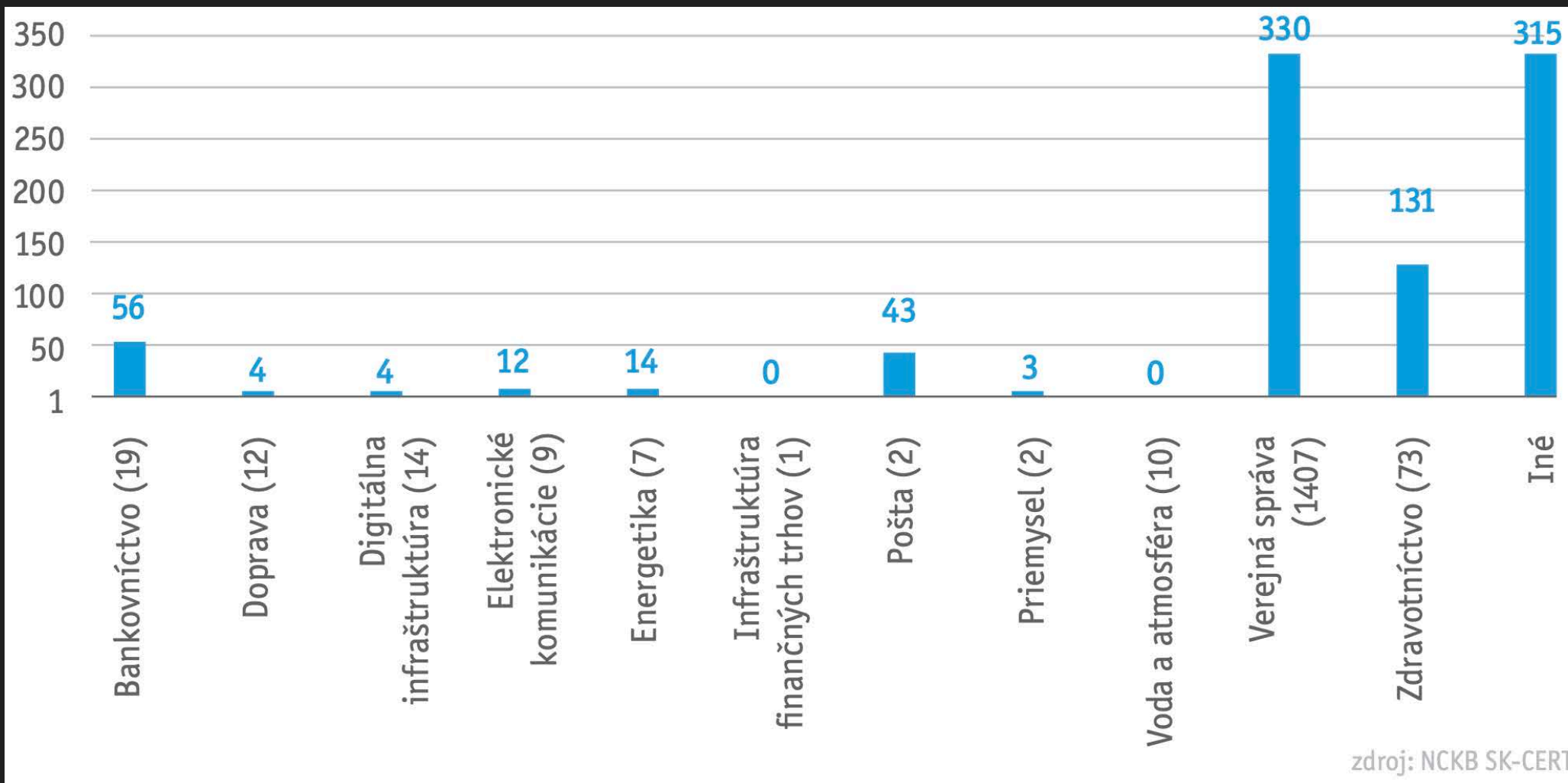




https://www.nbu.gov.sk/wp-content/uploads/urad/Vyrocne_spravy/Sprava-o-KB-SR-2021.pdf







NEBOJME SA INCIDENTY HLÁSIŤ !!!



NEBOJME SA INCIDENTY HLÁSIŤ !!!

**PREHLBUJME SPOLUPRÁCU V OBLASTI VÝMENY INFORMÁCIÍ O
INCIDENTOCH A IOC !!!**



- Najpočetnejšie typy incidentov:
 - **Nežiadúci obsah a získavanie informácií**
 - Malware
 - Skenovanie a pokusy o prienik
 - **Zraniteľnosti a nesprávna konfigurácia zariadení a systémov**

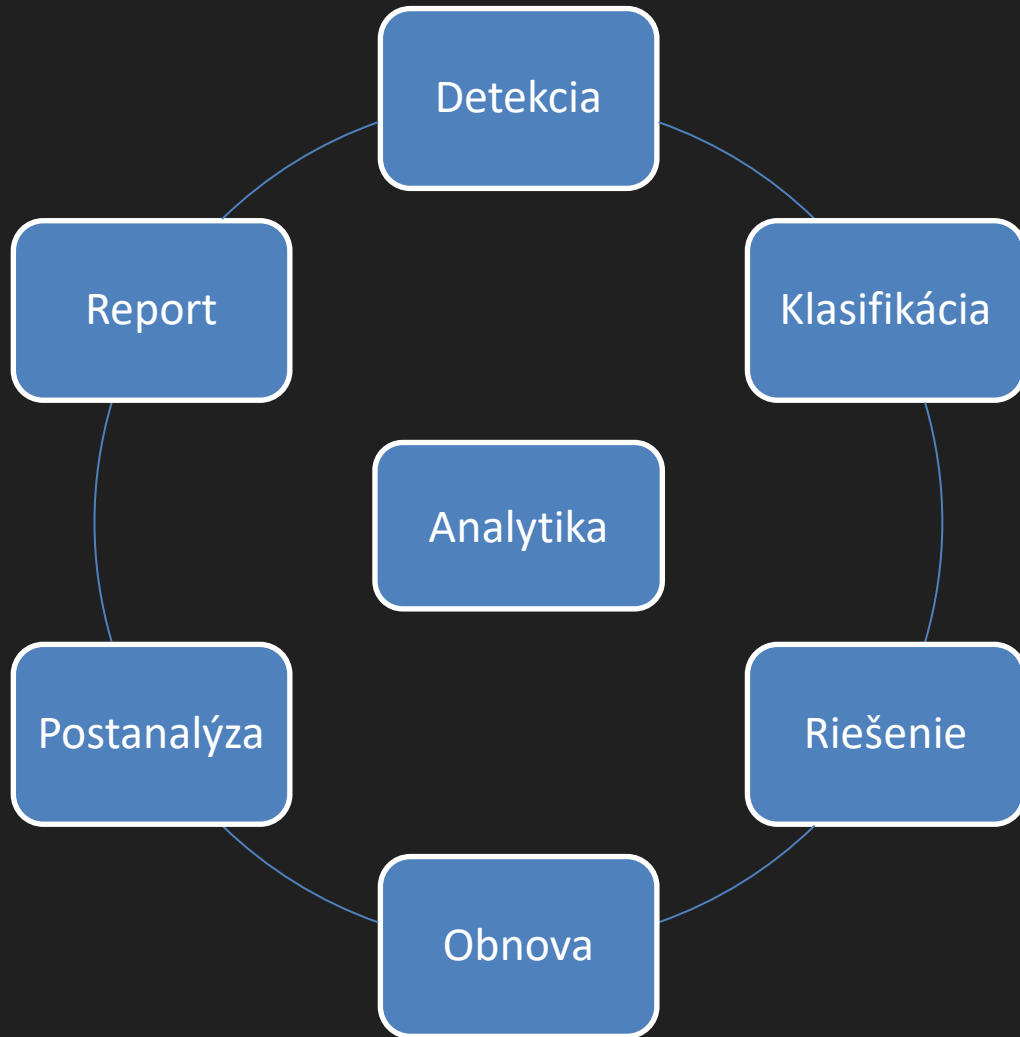
- Útok kombinujúci technické vedomosti s princípmi sociálneho inžinierstva
- Primárne ciele
 - Získavanie citlivých údajov
 - Šírenie rôznych foriem malwaru
- Sekundárne ciele
 - Zneužitie získaných údajov a infikovaných zariadení na ďalšiu škodlivú činnosť
 - Obchodovanie

Všetci sme o nich počuli, napriek tomu je obetí stále veľa...

- Definícia
 - Úmyselná alebo neúmyselná chyba HW, SW alebo P ktorú môže byť zneužitá a viesť k vzniku kybernetického bezpečnostného incidentu
 - Nesprávna konfigurácia zariadenia alebo systému
- Faktory
 - Človek
 - Ekonomický tlak a tlak zákazníkov na vývojárov a výrobcov
 - Komplexnosť aktuálneho stavu IKT a kybernetického priestoru
 - Komplexné systémové architektúry a frameworky
 - Brotnobyte-y dát

Ako zraniteľnosti mitigovať? Ako chrániť svoje aktíva?

- Zjednodušené:
 - Proces, ako incident vyriešiť a obnoviť pôvodný stav
- Detailný pohľad:
 - Určiť typ a závažnosť
 - Zastaviť prebiehajúci útok
 - Obnoviť stav a funkcionality pred útokom
 - Identifikovať útočný vektor a útočníka
 - Implementovať protiopatrenia





- Ako sa o incidente dozvieme?

- Štandardné komunikačné kanály
- Špecializované technické prostriedky
- Vlastná analytická činnosť

- Interné subjekty
- Externé subjekty

- <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (Chapter 3.2.3 Sources of Precursors and Indicators)



- Aké sú základné informácie o incidente?
 - Udalosť vs. incident
 - Má dopady na kybernetický priestor SR?
 - Spadá riešenie incidentu pod nás?
 - Technický typ incidentu
 - Kategorizácia podľa zákona
 - Eskalačné procesy
 - Reputačné riziko
 - Získať doplňujúce informácie
 - Rozsah škôd a dopady
 - Vzorky správ a malwaru



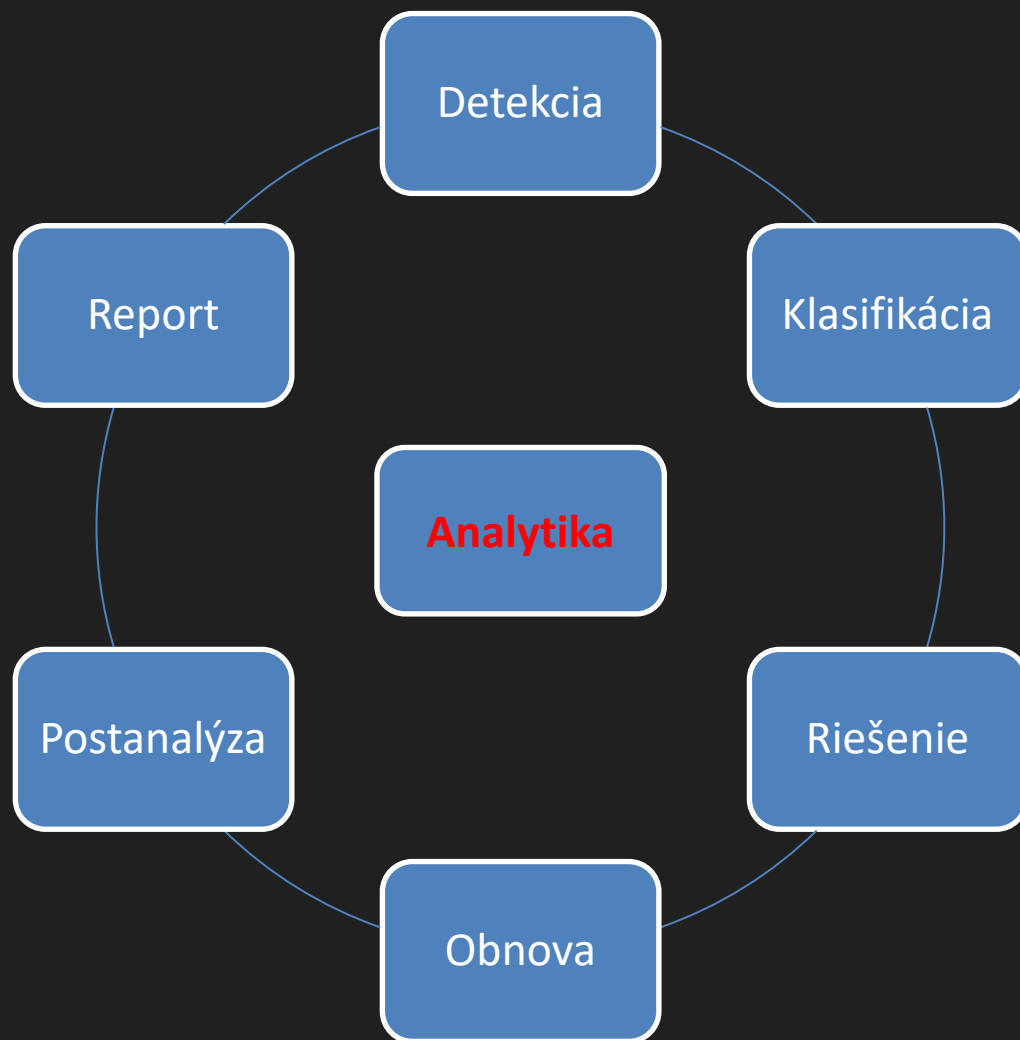
- Čo je potrebné urýchlene vykonať?
 - Zaistiť dôkazy, logy a digitálny materiál pre ďalšiu analýzu
 - Nesprávna analýza môže znehodnotiť dôkazy
 - Zastaviť prebiehajúci útok
 - Odrezať útočníka, izolovať infikované zariadenia, odstrániť phishingový obsah, ...
 - ABUSE proces a odstránenie podozrivého/phishingového/škodlivého obsahu
 - Procesy a krízové riadenie



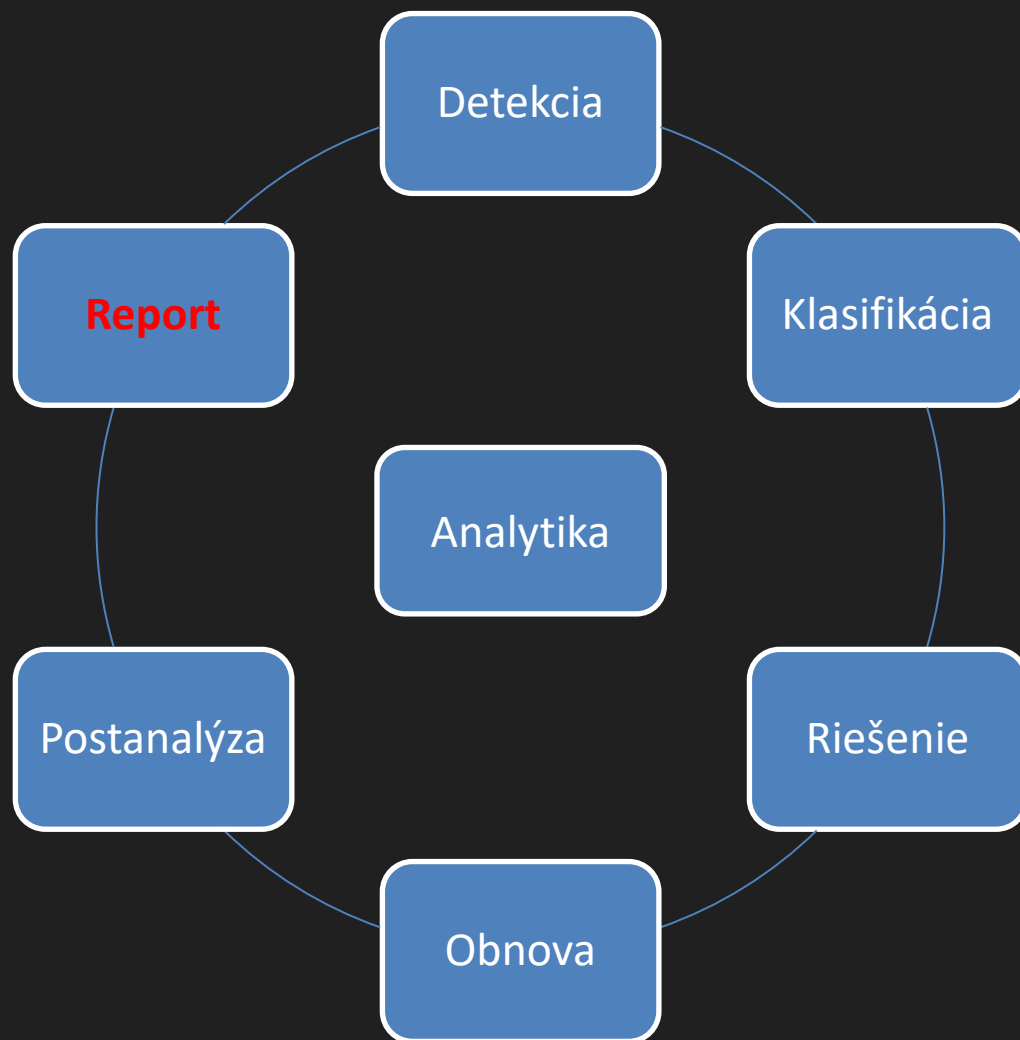
- Ako zaistíme obnovu do pôvodného stavu?
 - Obnova zo zálohy, reinštalácia zariadení, výmena poškodených komponentov, rozšifrovanie dát, ...
- Ako zabránime zopakovaniu incidentu?
 - Zmena prihlasovacích údajov a kryptografického materiálu
 - Hardening systému
 - Nasadenie dodatočných protipatrení
 - Procesy, metodiky



- Postupovali sme správne a efektívne?
 - Čo sme mohli spraviť lepšie a efektívnejšie?
 - Ako zabezpečiť, aby sa podobný incident nezopakoval?
 - Čo nemáme? Čo je potrebné zaviesť? Čo je potrebné zohnať a zabezpečiť?



- Čo všetko sprevádza základné fázy?
 - Stanovenie útočného vektora, prvotného vektora prieniku, modusu operandi útočníka, atď.
 - Forenzná analýza
 - Malwarová analýza
 - Threat intelligence, obohacovanie a korelácia dát
 - Práca s IOC



- Ako zistenia prezentovať?
 - Základné informácie o subjekte
 - Manažérske zhrnutie incidentu
 - Časová os riešenia incidentu
 - Analytické zistenia
 - Odporúčania
 - Zoznam indikátorov kompromitácie (IOC)

- Triviálne incidenty a ich riešenie môžu byť v skutočnosti komplikované
- Pohotová reakcia a efektívne riešenie situácie dostupnými zdrojmi
- Analytické, kreatívne a out-of-the-box myslenie
- Komunikácia a výmena informácií na firemnej, národnej i medzinárodnej úrovni

KONTINUÁLNA POTREBA ZLEPŠOVAŤ SA

Ďakujem za pozornosť.

