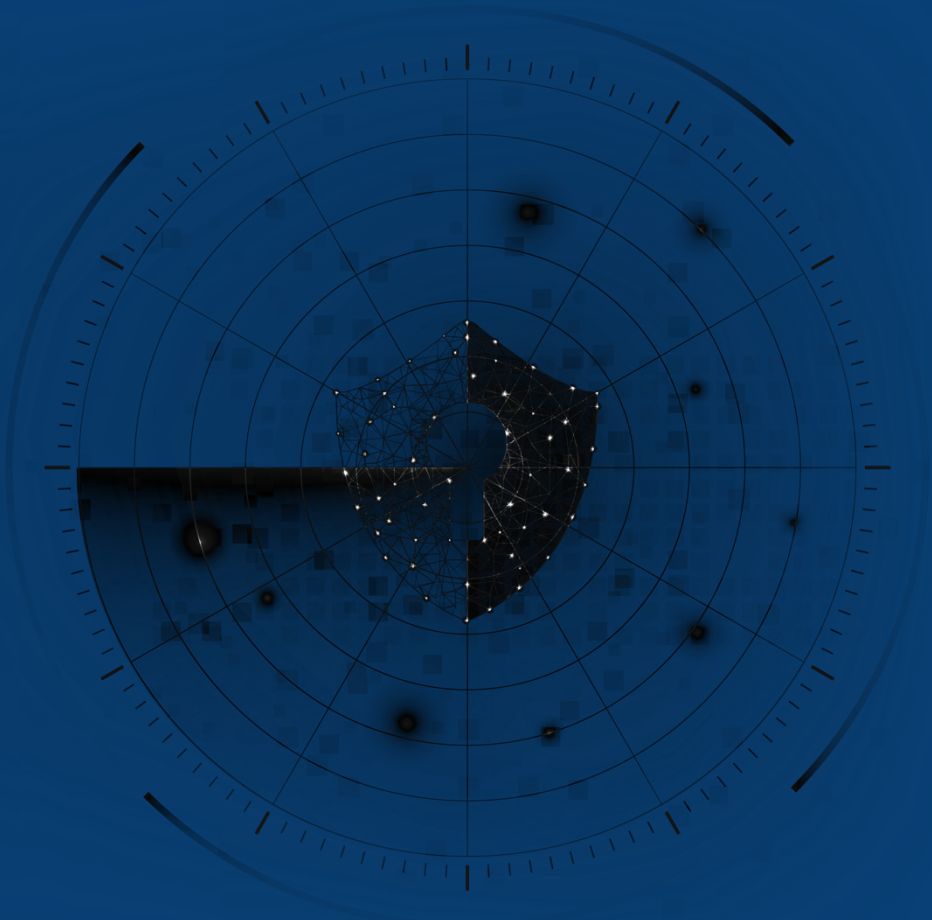
6. ročník EPI konferencie

KYBERNETICKÁ BEZPEČNOSŤ 2024

ZBORNÍK PREDNÁŠOK



Program konferencie

Jindřich Kalíšek
Päť krokov ku zlatej - ako hovoriť s top-manažmentom, aby vzal kyberbezpečnosť za svoju prioritu?

Michal Rampášek
Aktuálne výzvy pre riešenie zraniteľností a riadenie bezpečnosti tretích strán v ICS/OT prostredí

Miroslav Pikus
Etické dosahy algoritmov umelej inteligencie a posudzovanie vplyvu digitálnych technológií

Daniel Hejda
Tanec s vlkmi v kyberpriestore

Jaroslav Ďurovka
Novela zákona o kybernetickej bezpečnosti prichádza

Tomáš Hettych
Road2Cyber

Lukáš Hlavička, Roman Čupka
Keď už riešiť incident, tak poriadne a bez kompromisov!

Dušan Peško
Ako auditovať tzv. „resilience“ informačných systémov a sietí?

Ondřej Číž
DDoS útoky pod kontrolou: inovatívne stratégie pre hybridné prostredia

Martin Švéda
Praktické skúsenosti z transpozície smernice NIS2 do právneho systému Českej republiky

Jana Šimonová
Relevancia vzdelávania a využívania AI v oblasti ochrany mäkkých cieľov

Matúš Mihok
Penetračné testovanie štátnej správy a kritickej infraštruktúry v zahraničí

Zuzana Holý Omelková

Marketplace kyberbezpečnosti: rýchlejší a efektívnejší prístup k osvedčeným službám

Jozef Halcin

Prepojenie ochrany mäkkých cieľov a kybernetickej bezpečnosti: efektívne stratégie na zvládnutie súčasných hrozieb

Štefan Pilár

Riadenie dodávateľského reťazca v kontexte analýzy rizík

Marek Zeman

Úskalia implementácie systémov umelej inteligencie a hľadanie zjednodušení na základe požiadaviek právnych predpisov

Alexandra Húsková, Lukáš Balážik

Cesta od Cybergame k European Cybersecurity Challenge – príprava a vedenie národného tímu mladých kybertalentov

Václav Hřích

Interpretácia výsledkov reprezentatívneho online prieskumu kybernetická bezpečnosť 2024 - verejnosť SR

Juraj Belko

Je vaša spoločnosť schopná odolať pokročilému útoku?

Július Selecký

Moderné výzvy si žiadajú moderné riešenia: bezpečnosť s Managed Detection and Response bez stresu

Adam Gajdošík

Analýza škodlivého kódu pomocou jazykových modelov

Eva Hlušková

Ako prepojiť hodnotenie súladu kybernetickej bezpečnosti, informačnej bezpečnosti a ochrany osobných údajov?

Michal Ďorda

Nie je audit ako audit

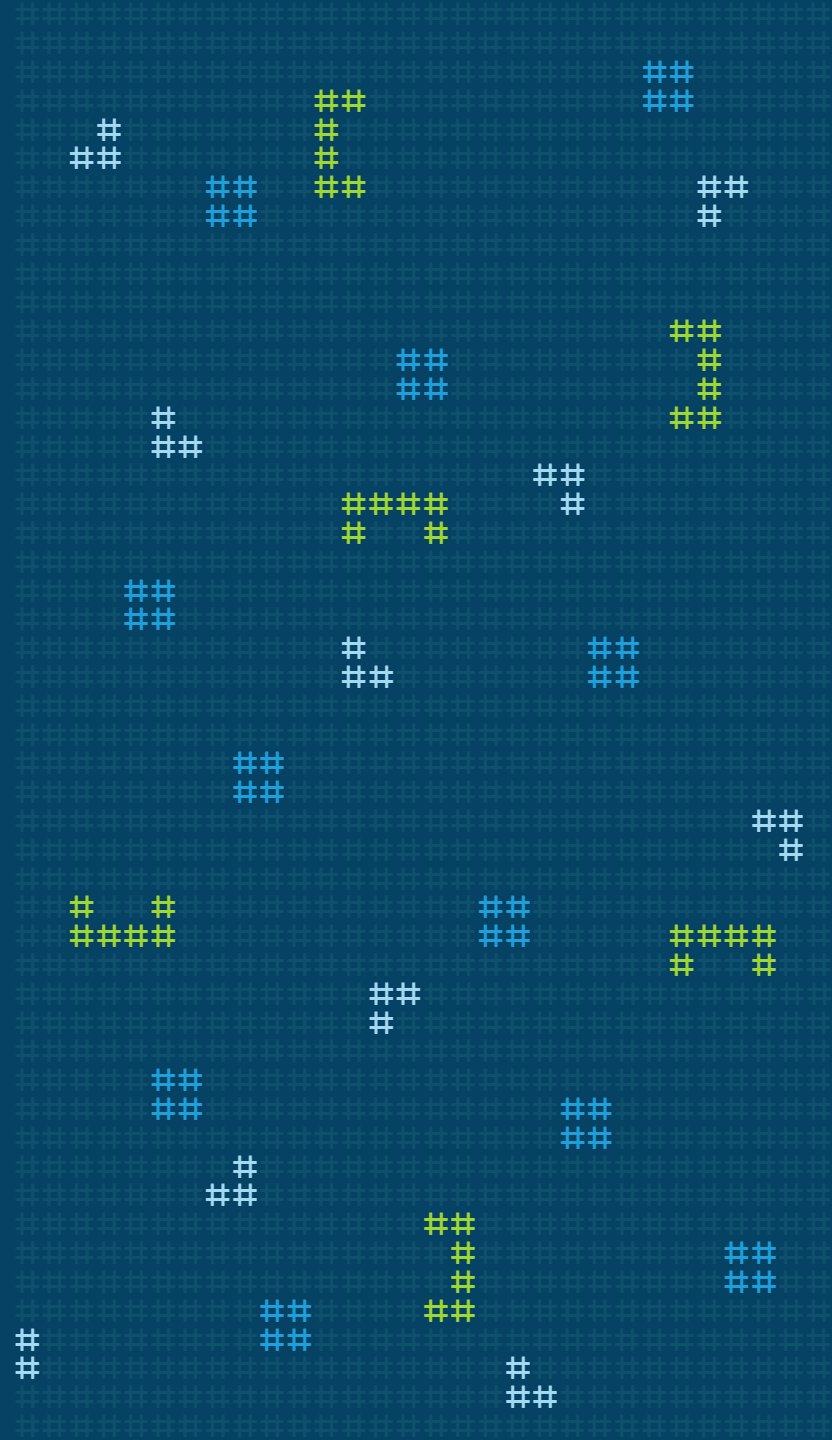
#CY83RL4WY3R

PÄŤ KROKOV KU ZLATEJ

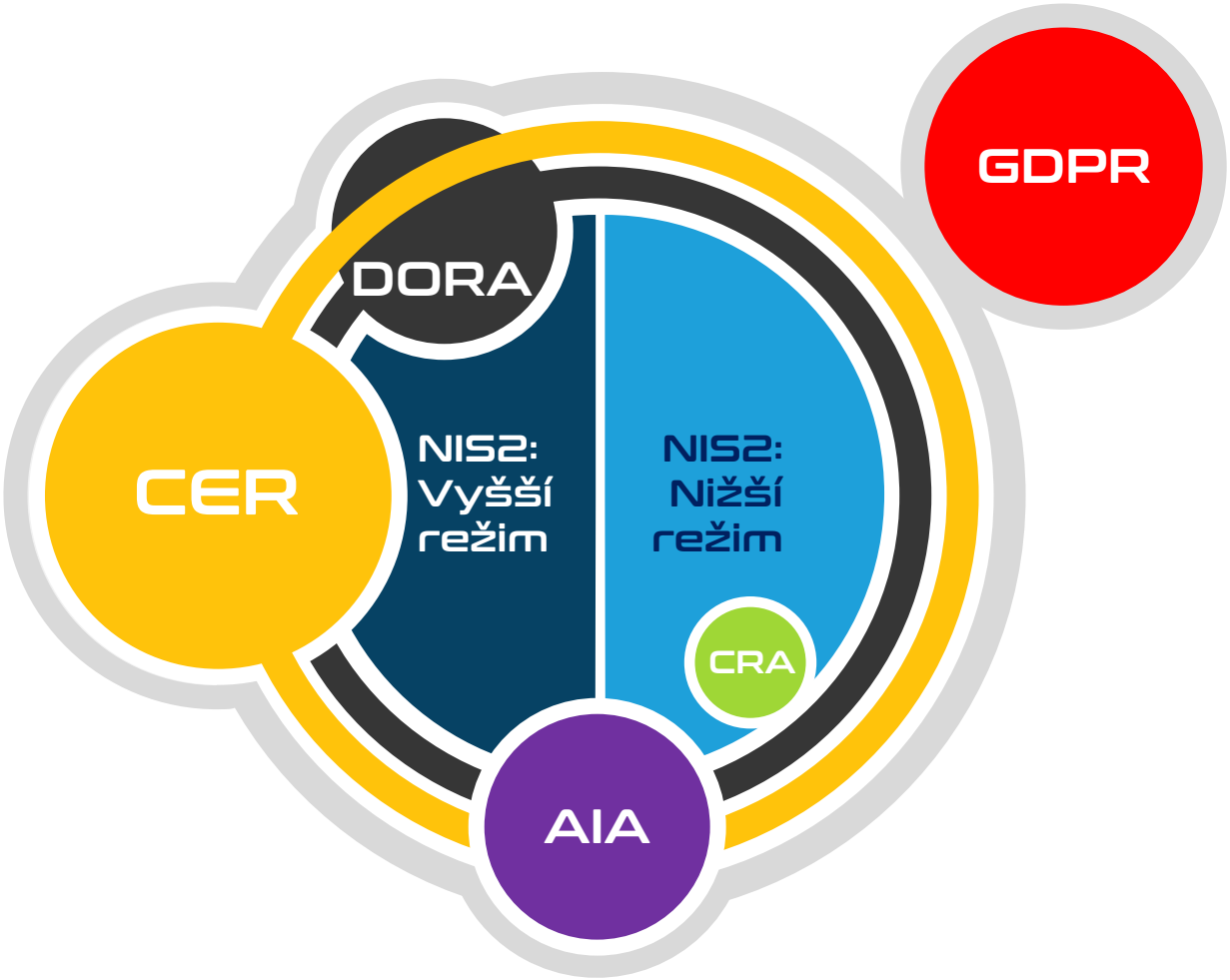
Ako hovoriť s top-manažmentom, aby vzal kyberbezpečnosť za svoju prioritu?

EPI konferencia Kybernetická bezpečnosť 2024

30. 9. 2024 | Demänovská Dolina



REGULACE JE/NENÍ* PROBLÉM



DORA, NIS2 a CER

> Komplexní rámec pro ochranu kritické infrastruktury a kybernetické bezpečnosti

GDPR

> Specifické požadavky na režim nakládání s osobními údaji

AIA a CRA

> Produktová regulace
> Ochrana spotřebitele

*** Nehodící se škrtněte**

PŠTROSÍ OPTIMUM KONČÍ

- # Odpovědnost za stav kybernetické bezpečnosti
  - > Recitály 133, 137 a čl. 20 NIS2
  - > Přičitatelná řídícímu orgánu → **Nelze delegovat ani outsourcovat?**
  - > Přímá odpovědnost za nastavení politik, zavedení a dodržování opatření
- # Povinné vzdělávání
  - > Aktuální rizika a hrozby → Stačí to?
- # Nezbytný reporting

1 | TOP MANAGEMENT VÁM NEROZUMÍ

Kyberbezpečnost je šamanství

Mluvte jejich jazykem

> Pokud vám nebudou rozumět, nebudou vám věřit

> Popisujte situaci s důrazem na objasnění podstaty

> Vynechejte zbytečné technikálie

Triáda srozumitelné komunikace

> **Simplifikace × Adjustace × Edukace**

2 | BARVY PATŘÍ NA SEMAFOR

Top management musí kvalifikovaně rozhodovat o rizicích

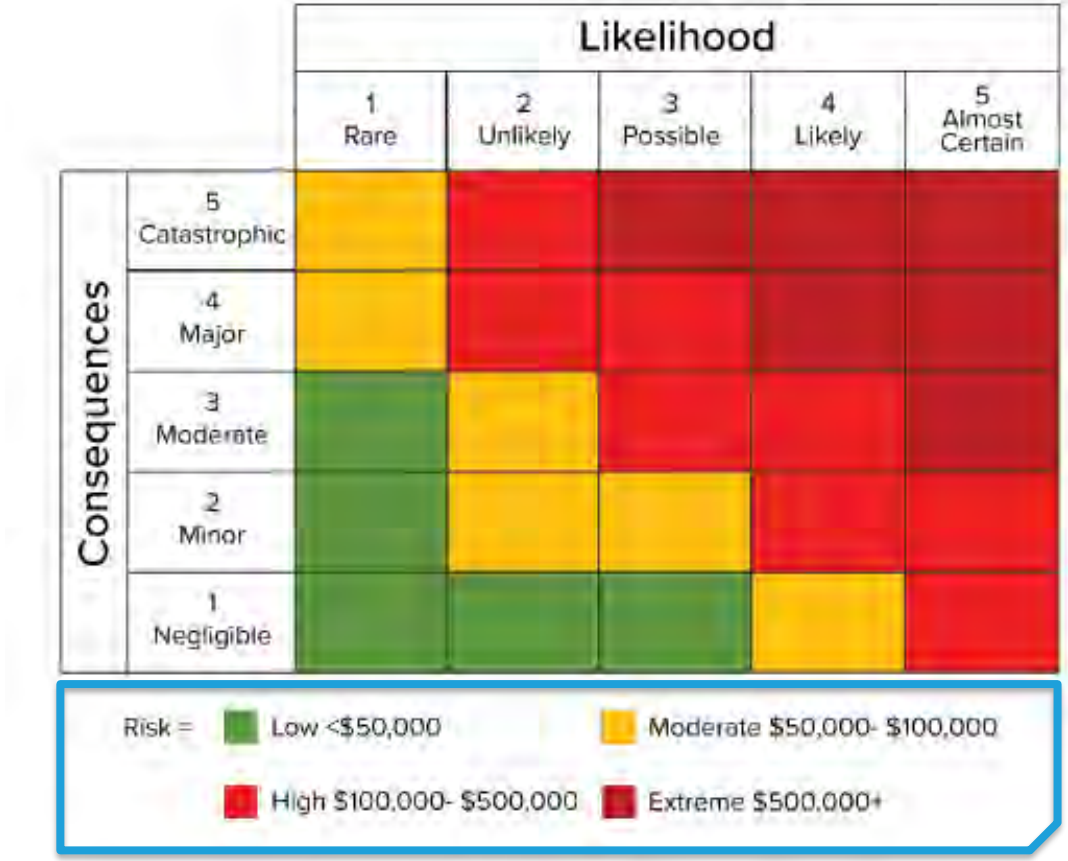
> Musí jim rozumět, chápat jejich povahu, rozsah a možné dopady

> Ze standardní kvalitativní analýzy / matice rizik to nevyčte

Rizika vždy kvantifikujte

> Nejlépe v penězích a ve scénářích

> Krom rizik a nákladů na jejich mitigaci vyčíslujte i příležitosti na zlepšení



3 | PRIORITY A TO OSTATNÍ

Klíčem k úspěchu není prioritizovat všechny položky v diáři,
*ale **přizpůsobit diář vašim prioritám**.*

Stephen R. Covey

Prioritizujte, prioritizujte, prioritizujte...
> Rizika
> Opatření
> Investice

Nikdy nebudete #1
> Vysvětlujte proč

4 | BĚŽÍTE MARATON, NE SPRINT

5 | NECHTE JE ZAZÁŘIT

Tone from the Top

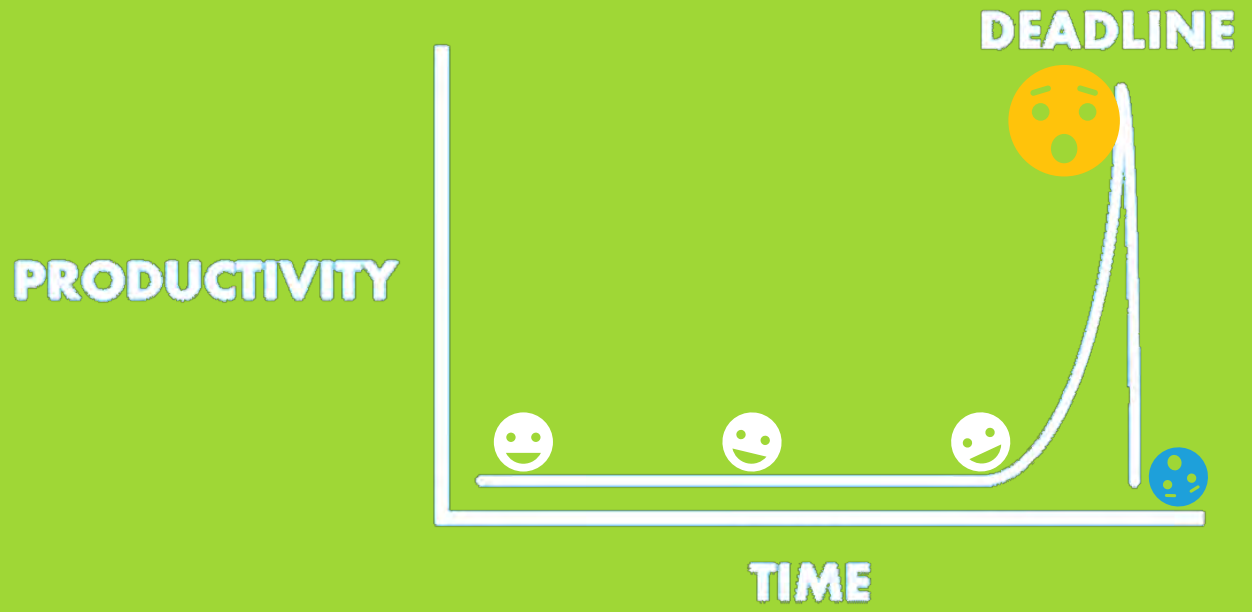
Lead by Example

#CY83RL4WY3R

A CO KDYŽ SE ZEPTAJÍ...

- **Počkáme a uvidíme?**

- Máte rádi stres?
- Není důvod otálet
  - > Základní principy legislativy jsou jasné a výrazně se nezmění
  - > Na trhu chybí kompetence i kapacita
    - > Stovky specialistů?
    - > Lidé nebudou ani ve střednědobém horizontu → digitalizace / virtualizace



Schatz, I.: *Student Syndrome: Why People Delay Until Right Before Deadlines*, Solving procrastination (2024), dostupné zde.

A CO KDYŽ SE ZEPTAJÍ...

Proč tolik peněz?

Řadě oblastí se můžeme začít věnovat hned, s rozumnými* náklady

- > Zmapování procesů, poskytovaných služeb a jejich klasifikace podle legislativy
- > Analýza rizik v oblasti zpracování a bezpečnosti informací a osobních údajů
- > Common Baseline (minimální standard počítačové hygieny a bezpečnosti)
- > Vzdělávání zaměstnanců a top managementu

* Rozuměj: „minimálními“

Q&A

Jindřich Kalíšek, advokát

Zakládající partner #CYBERLAWYER

kalisek@cyberlawyer.cz

#CY83RL4WY3R

JUDr. Ing. JINDŘICH KALÍŠEK, Ph.D. CIPP/E CIPM FIP

Advokát | Mediátor | Pověřenec pro ochranu osobních údajů

E kalisek@cyberlawyer.cz E (+420) 775 877 046

#CY83RL4WY3R

- # Butikové právní poradenství pro kybernetickou bezpečnost, ochranu informací a osobních údajů, AI, compliance management a ESG
- # Hluboká právní expertíza a zkušenost
- # Efektivní přístup podle potřeb byznysu
- # Nadšení pro technologie

CYBERSECURITY
DATAPROTECTION
AI
COMPLIANCE
ESG
DIGITAL

www.cyberlawyer.cz

Powered by **cysensic.cz**

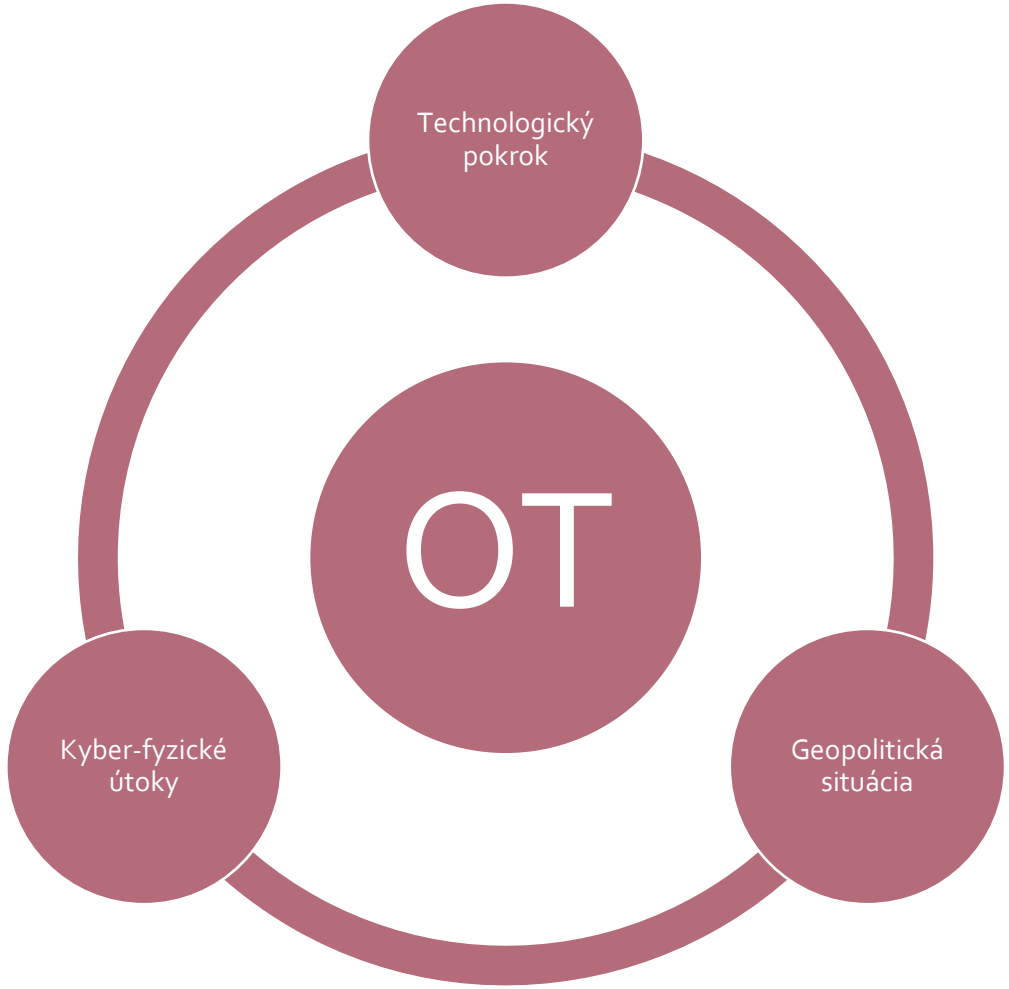
PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

Aktuálne výzvy pre riešenie zraniteľností a riadenie bezpečnosti tretích strán v ICS/OT prostredí

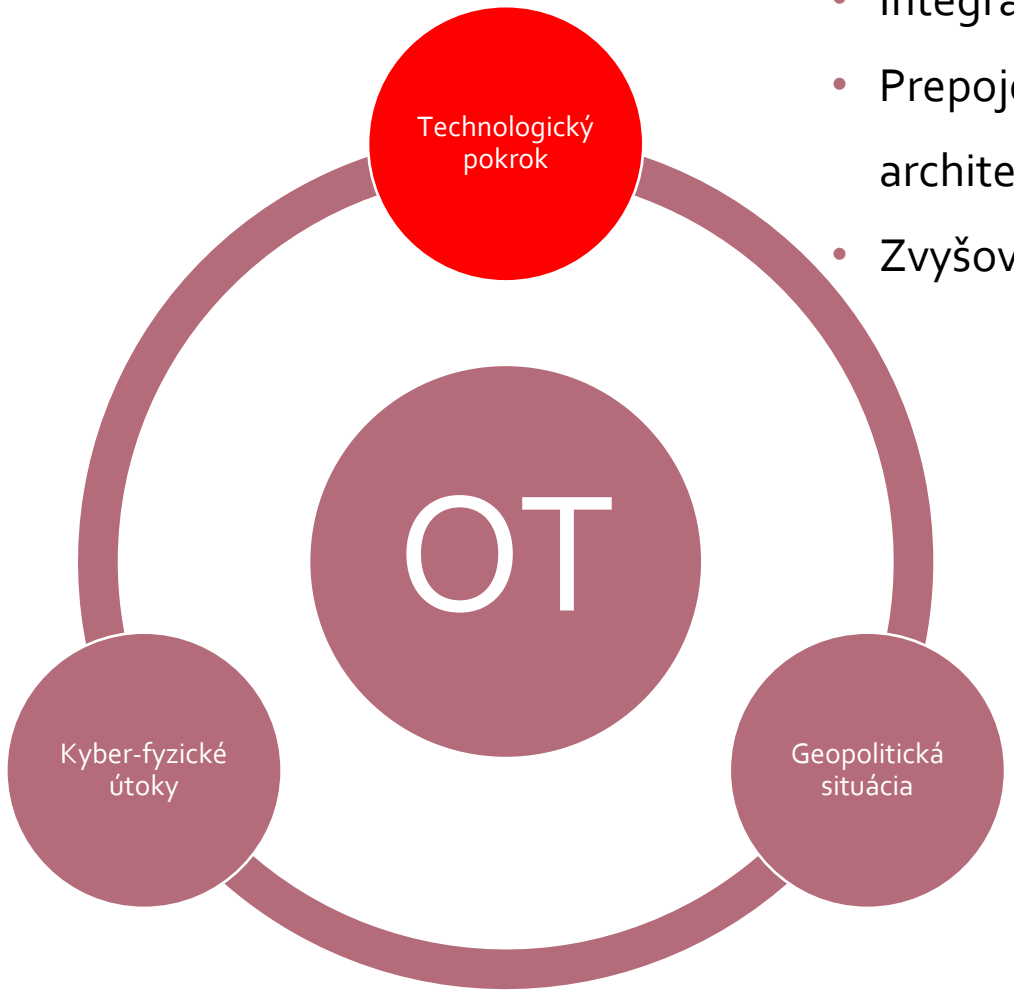
JUDr. Michal Rampášek

Táto práca bola podporená Agentúrou na podporu výskumu a vývoja na základe zmluvy č. APVV-23-0137.

Hrozby a OT


Technologický pokrok
OT
Kyber-fyzické útoky
Geopolitická situácia

Hrozby a OT

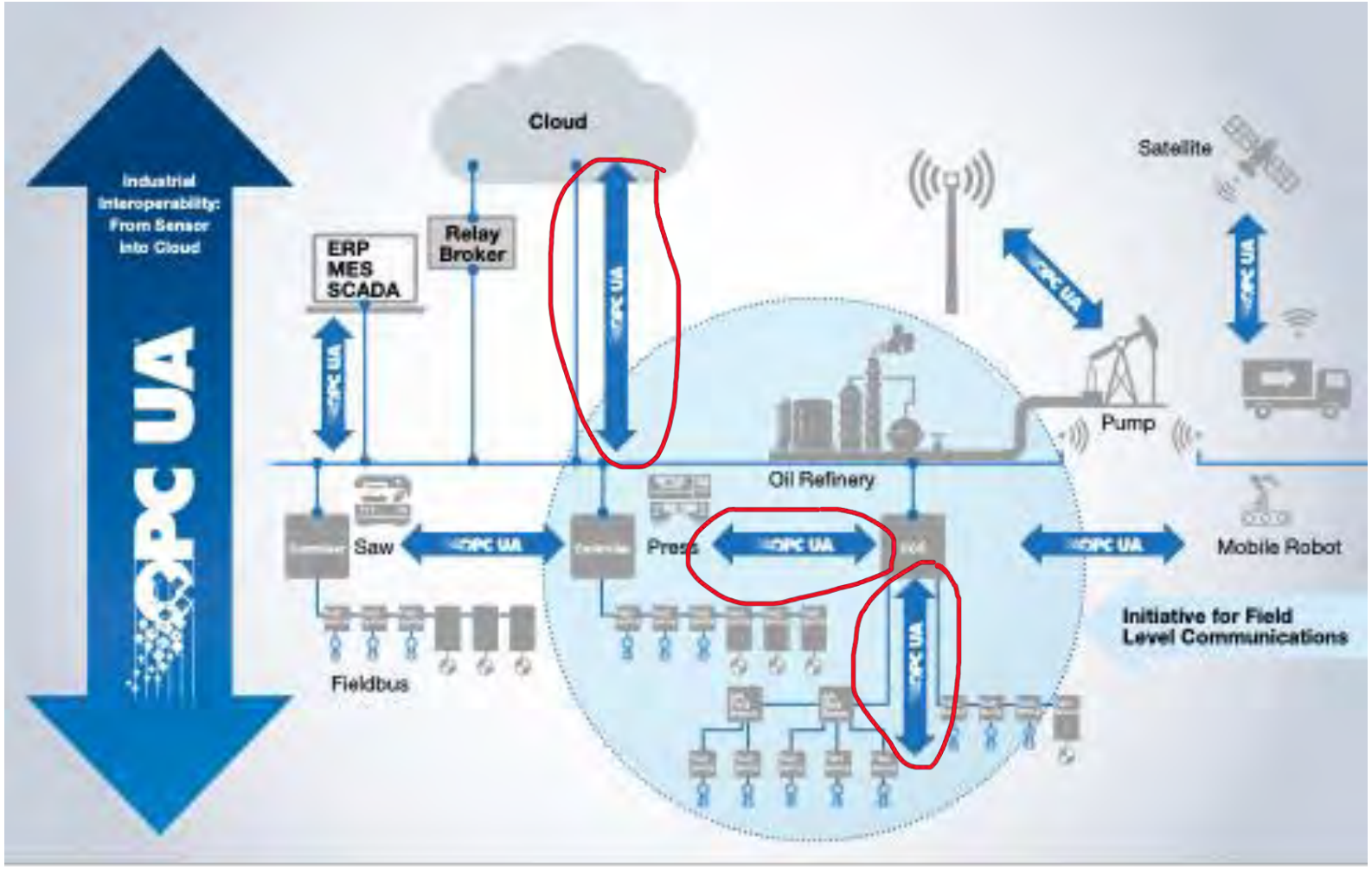


- Integrácia IIoT do OT prostredí.
- Prepojenie OT s cloudovými (hyperscale) architektúrami a vendor lock-in
- Zvyšovanie zraniteľností

Purdue model + IIoT?

Revised Purdue Model Zdroj: ENISA, Good Practices for Security of Internet of Things in the context of Smart Manufacturing, 2018

Nové architektúry - OPC field exchange

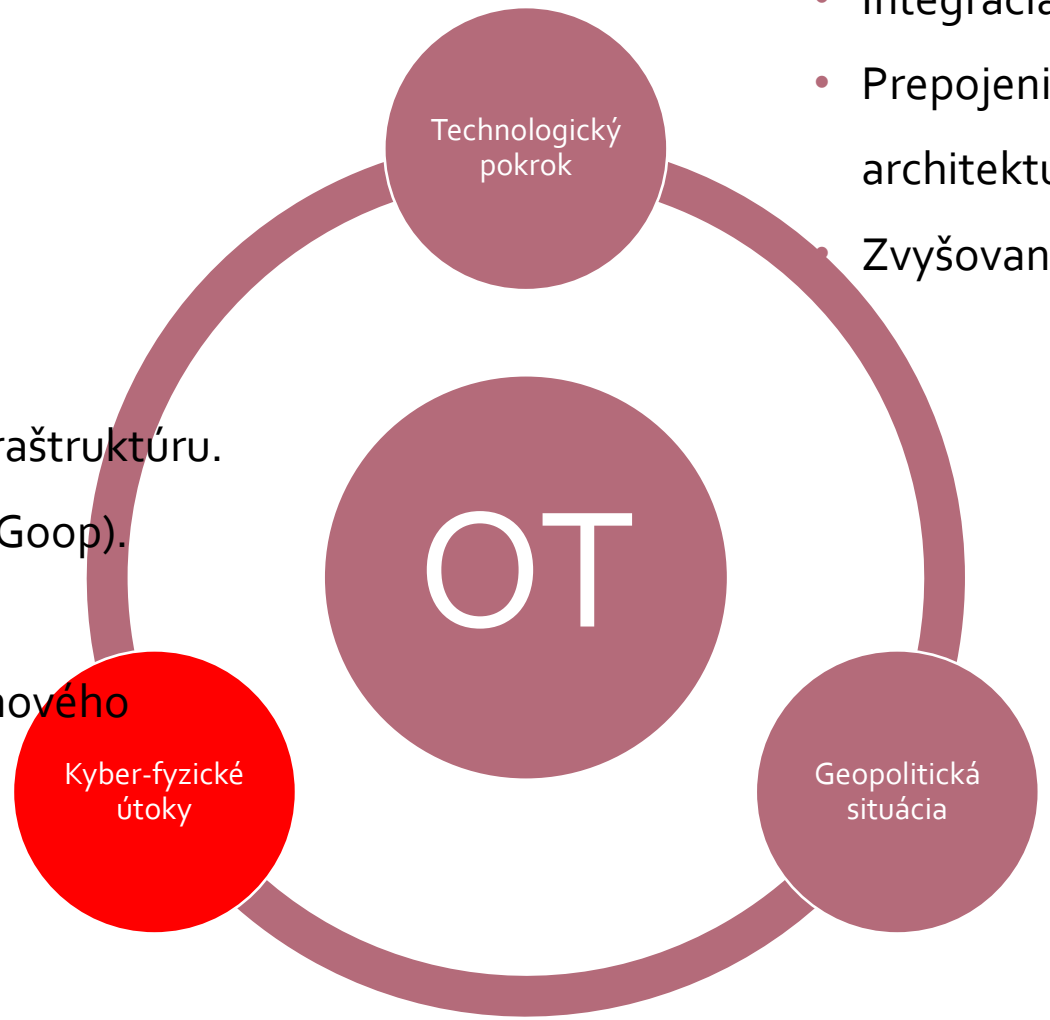


Zdroj: Extending OPC UA to the field: OPC UA for Field eXchange (FX) Version 2, 2021

- *Aplikácie IIoT s cloud backendom či ako SaaS*
- *Viditeľnosť do AIM a do oprávnení*
- *Best practices na implementáciu a overovanie/audity*
- *Integrácia existujúcich OT systémov a sietí s IIoT infraštruktúrami*

Hrozby a OT

- Integrácia IIoT do OT prostredí.
- Prepojenie OT s cloudovými (hyperscale) architektúrami a vendor lock-in
- Zvyšovanie zraniteľností



- Cielené útoky na kritickú infraštruktúru.
- Malvéry na ICS (napr. FrostyGoop).
- Nové vektory útokov.
- Nové formy hybridného vojnového konfliktu (Vulkan files)

Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity

TLP:CLEAR

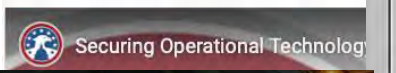
MS-ISAC® Multi-State Information Sharing & Analysis Center®

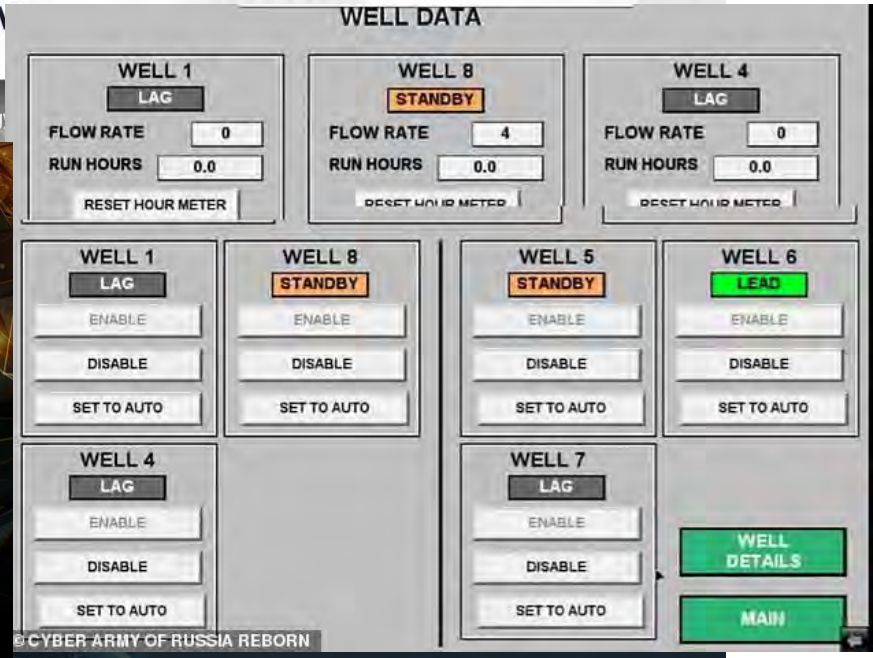
Communications Security Establishment / Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications / Centre canadien pour la cybersécurité

SECURING OPERATIONAL TECHNOLOGY: A DEEP DIVE INTO THE WATER SECTOR

FEBRUARY 6 – 10:00 AM





black hat ASIA 2024

APRIL 18-19, 2024

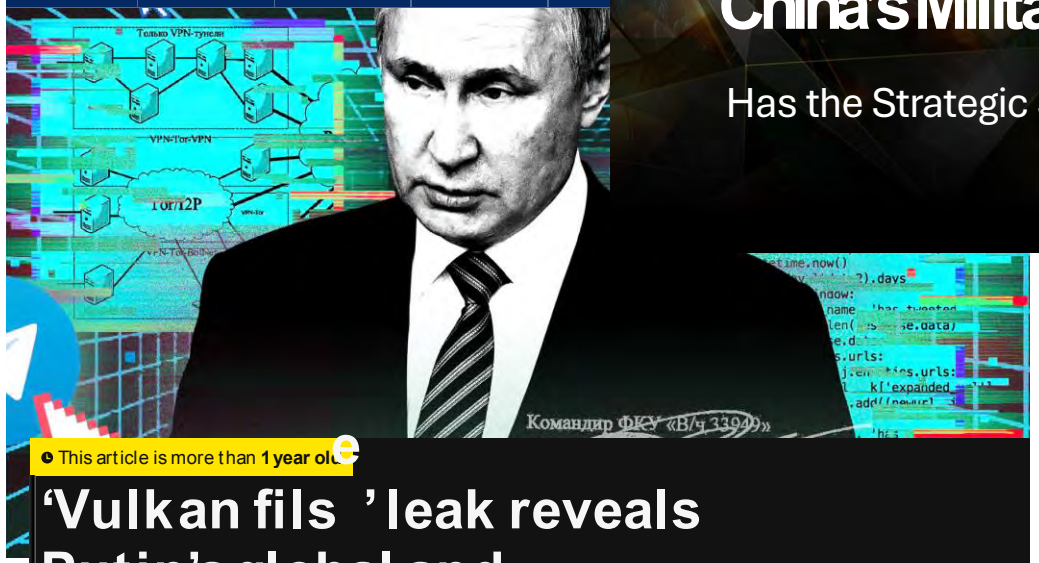
BRIEFINGS

China's Military Cyber Operations

Has the Strategic Support Force Come of Age?

Pukhraj Singh

Opinion | Sport | Culture | Lifestyle



This article is more than 1 year old

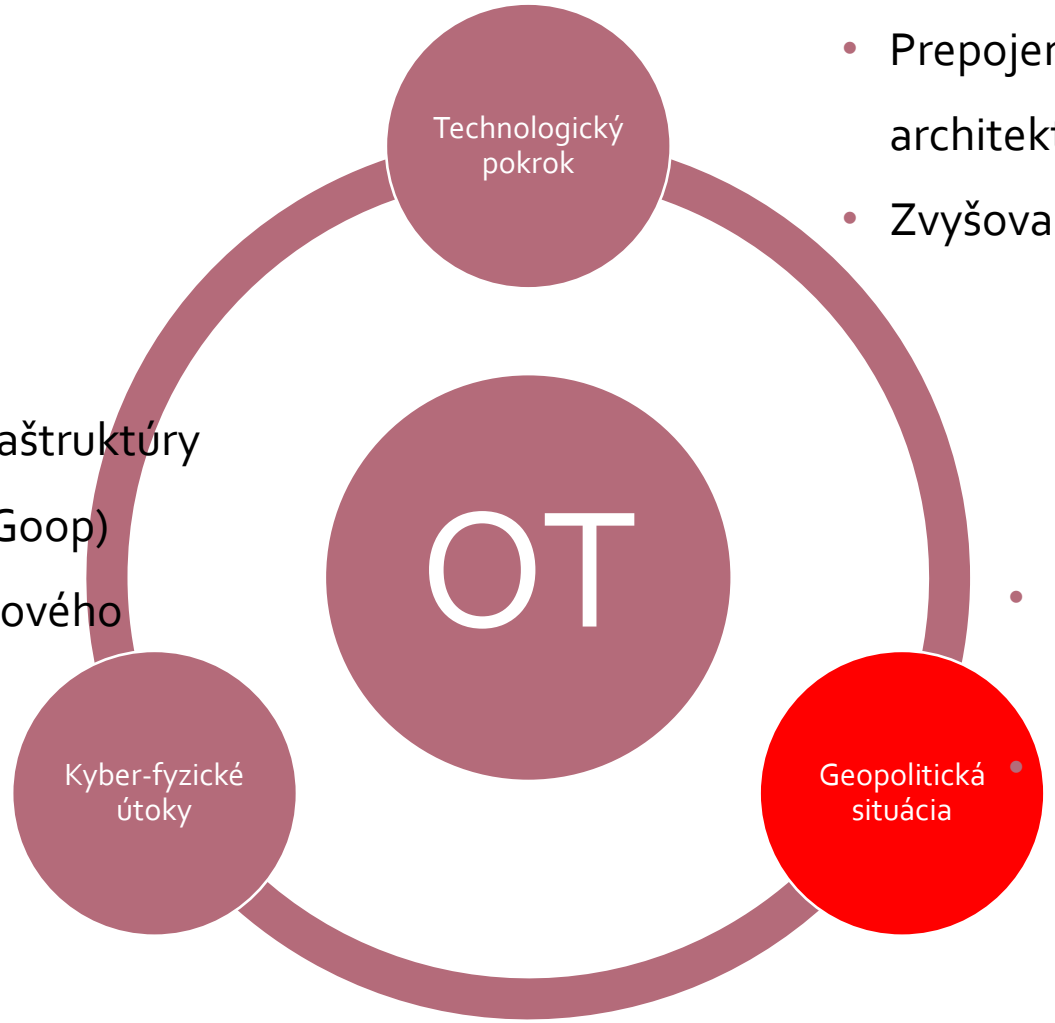
'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics

Intelligence Brief: Impact of FrostyGoop ICS Malware on Connected OT Systems

In April 2024, FrostyGoop, an ICS malware, was discovered in a publicly available malware scanning repository. FrostyGoop can target devices communicating over Modbus TCP to manipulate control, modify parameters, and send unauthorized command messages. Modbus TCP is a commonly used protocol across all industrial sectors.

Hrozby a OT

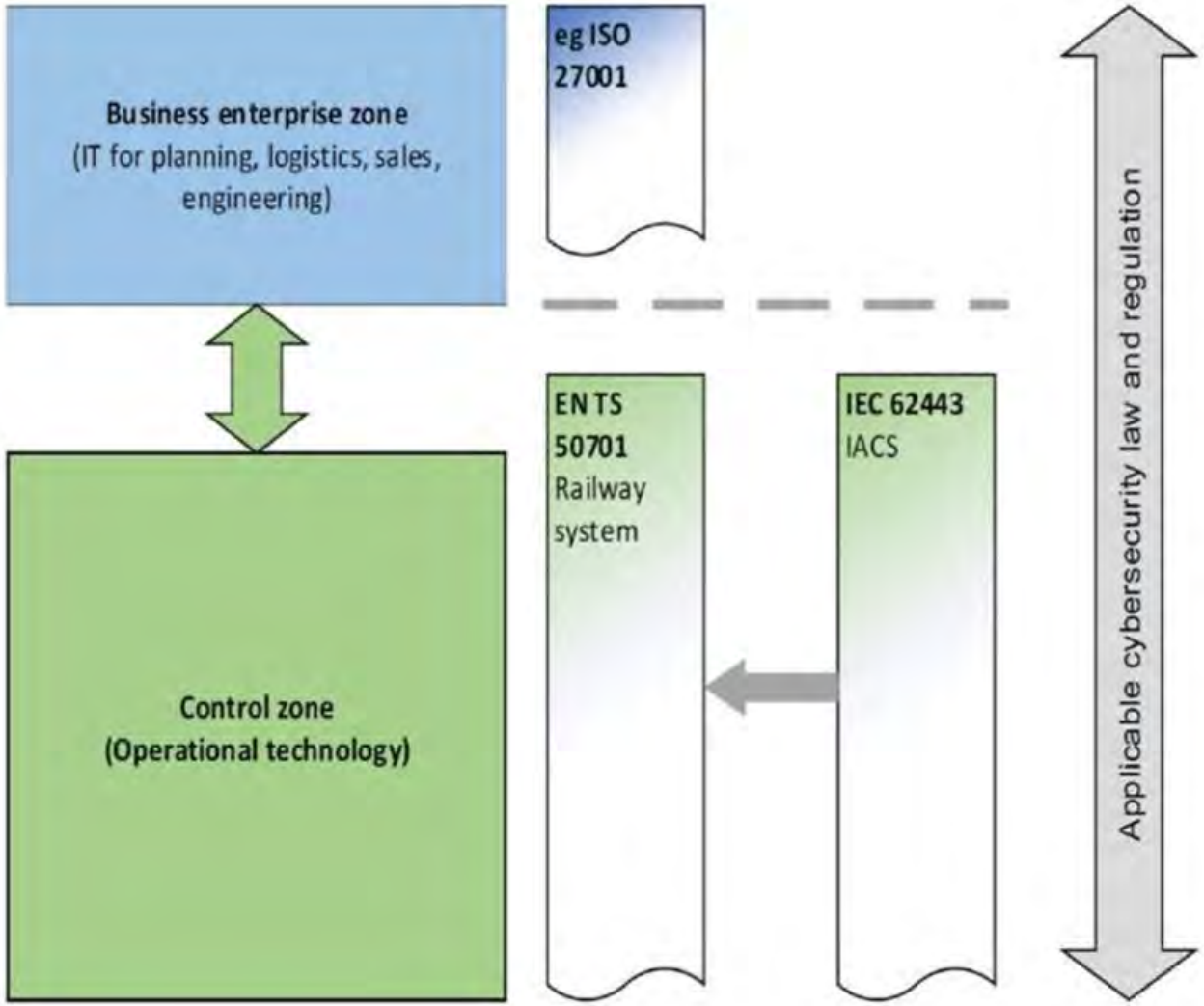
- Integrácia IIoT do OT prostredí
- Prepojenie OT s cloudovými (hyperscale) architektúrami a vendor lock-in
- Zvyšovanie zraniteľností



- Cielené útoky na kritické infraštruktúry
- Malvéry na ICS (napr. FrostyGoop)
- Nové formy hybridného vojnového konfliktu (Vulkan files)

- Vplyv regulácií a tech. noriem na kybernetickú bezpečnosť OT
- Smernice NIS2 a CER a (návrh) nariadenia CRA.

Technické normy a právna regulácia



NIS 2

CER, CRA, PLD, etc.

Nový regulačný rámec pre OT

- Prepojenie medzi smernicami NIS2, CER a nariadením CRA

NIS2 a CER

- OT
- Kritická infra.

PLD
(nová smernica EÚ o zodpovednosti za chybné výrobky)

CRA

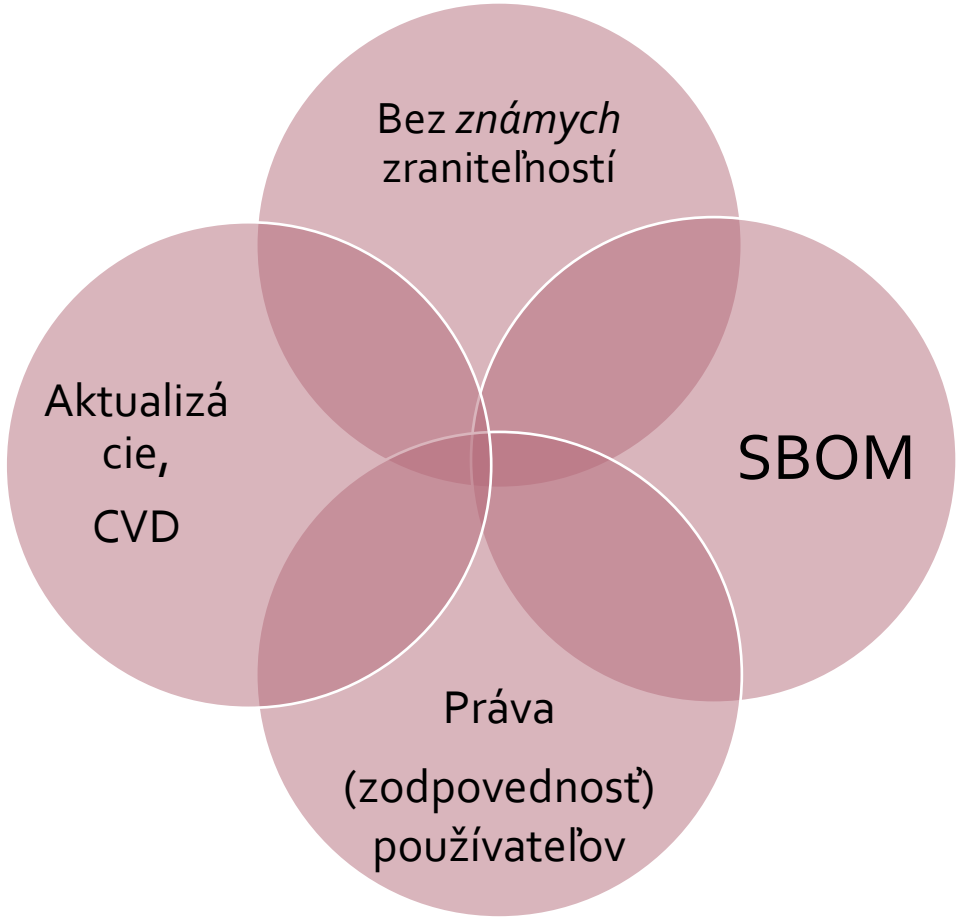
- Digitálne produkty (vrátane OT)

Význam nariadenia CRA

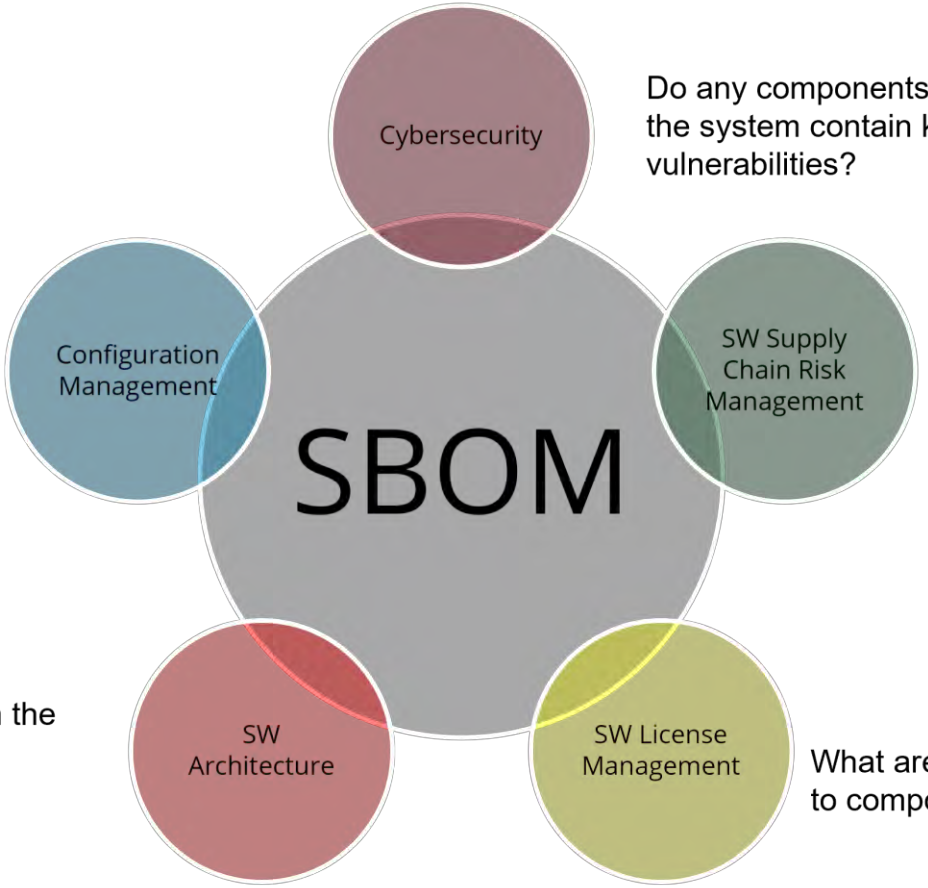
- Digitálny produkt = IoT, IIoT, SCADA, PLC, ..? a mnoho ďalšieho (FW, SIEM, IPS/IDS, atď.)
- A čo cloud? áno aj nie (CRA vs NIS2)
- (3) kategórie – „bežný“ (90%), dôležitý a kritický produkt
- Povinnosti výrobcu/distribútora/dodávateľa („kvázi“ výrobcu – pod vlastným menom/značkou alebo pri podstatnej úprave produktu)
- Základné požiadavky kybernetickej bezpečnosti produktu (Príloha I)

Príloha I nariadenia CRA

- Digitálne produkty „sa navrhujú, vyvíjajú a vyrábajú tak, aby sa zaistila *primeraná úroveň ich bezpečnosti* voči *kybernetickým rizikám* “



Softvérový kusovník (SBOM)



Do any components in or used by the system contain known vulnerabilities?

What components are included/needed in my system?

What are the third-party components in the system and the source of the component information?

Where are the components in the system architecture?

What are the licensing/data rights to components in my system?

Zdroj: Carnegie Mellon University, 2023

Softvérový kusovník (SBOM) a … aj hardverový kusovník (HBOM)

"We need visibility, we need incentives, and we need resiliency. An SBOM won't give us those, but they enable all of those. In other words, we can't move forward without SBOMs." Zdroj: The Linux Foundation, Software Bill of Materials (SBOM) and Cybersecurity Readiness, 2022

Požiadavka na HBOM nie je upravená v CRA ani inom právnom predpise

PRESS RELEASE

CISA Releases Hardware Bill of Materials Framework (HBOM) for Supply Chain Risk Management (SCRM)

Released: September 25, 2023

Výzvy pri implementácii

- Dôležitosť viditeľnosti a dokumentácie
- Definovanie perimetra v zmluvách (riadenie identít a prístupov, IAM)
- Integrácia SBOM a HBOM do zmlúv
- Zodpovednosť výrobcu vs. používateľa digitálneho produktu, osobitné dohody, custom produkty
- Zodpovednosť za softvér a vadný (chybný) digitálny produkt
- Riešenie problému vendor lock-in v OT
- Odporúčania pre zmluvné vzťahy a vyjednávanie s tretími stranami

Ďakujem za pozornosť

rampasek1@uniba.sk

AKTUÁLNE VÝZVY PRE RIEŠENIE ZRANITEĽNOSTÍ A RIADENIE BEZPEČNOSTI TRETÍCH STRÁN V ICS/OT PROSTREDÍ[1]

Michal Rampášek

ABSTRAKT

CURRENT CHALLENGES FOR ADDRESSING VULNERABILITIES AND MANAGING THIRD-PARTY SECURITY IN ICS/OT ENVIRONMENT

Rastúca závislosť prevádzkových technológií (OT) a predovšetkým priemyselných riadiacich systémov (ICS) na softvérových komponentoch tretích strán a open-source knižniciach prináša nové riziká tretích strán. V súlade s návrhom nariadenia o kybernetickej odolnosti (Cyber Resilience Act - CRA) by mal od roku 2027 každý nový digitálny produkt musieť spĺňať aspoň základné požiadavky kybernetickej bezpečnosti. Tento príspevok analyzuje prepojenie medzi požiadavkami smernice NIS2, smernice CER s návrhom nariadenia CRA, v prostredí OT/ICS pri riešení zraniteľností a riadení rizík tretích strán vrátane dopadu na zmluvné vzťahy s tretími stranami. Zameriava sa tiež na požiadavky na softvérový kusovník (SBOM) a zdieľanie informácií o zraniteľnostiach a aktualizáciách.

Cyber Resilience Act, NIS2 Directive, CER Directive, OT cybersecurity, Third-party Security, Software Bill of Materials, Vulnerability Management

1. Úvod

Vzhľadom na stále sa zvyšuje závislosť prevádzkových technológií (Operational technology – OT) na softvérových komponentoch tretích strán vrátane knižníc s otvoreným zdrojovým kódom sa zvyšujú riziká spojené s kybernetickou bezpečnosťou v OT prostrediach.

OT sú programovateľné systémy alebo zariadenia, ktoré interagujú s fyzickými prostrediami (alebo riadia zariadenia interagujúce s fyzickým prostredím). Zahŕňajú napríklad priemyselné riadiace systémy, systémy riadenia budov, požiarne riadiace systémy a mechanizmy riadenia fyzického prístupu [NIST, 2018].

OT systémy sa delia na štyri základné veľké skupiny, okrem priemyselných riadiacich systémov (Industrial Control Systems - ICS), sem patria aj riadiace systémy (Control Systems

[1] Táto práca bola podporená Agentúrou na podporu výskumu a vývoja na základe zmluvy č. APVV-23-0137.

– CS), kyber-fyzické systémy (Cyber-Physical System – CPS) a zariadenia rozšíreného internetu vecí (Extended Internet of Things – XIoT) [David, 2024].

ICS zahŕňa napríklad systémy pre dispečerské riadenie a zber dát (SCADA), distribuované riadiace systémy (DCS) a programovateľné logické riadiace jednotky (PLC) [Stouffer, 2023, s. 11].

V príspevku sa pokúsime zodpovedať kľúčové otázky: aký je vplyv nového regulačného rámca na riadenie tretích strán v OT/ICS, aké sú hlavné výzvy pri implementácii požiadaviek návrhu nariadenia CRA spoločne so smernicami NIS2 a CER v sektore OT, a ako môže softvérový kusovník (Software Bill of Materials – SBOM) prispieť k zlepšeniu bezpečnostných opatrení v OT.

Po tejto úvodnej časti je druhá časť venovaná priemyselnému internetu vecí (Industrial Internet of Things - IIoT) a OT. Tretia a štvrtá časť pokračuje skúmaním podstatných vlastností riadenia zraniteľnosti OT a riadenia tretích strán. Piata časť obsahuje analýzu prienikov medzi novými právnymi predpismi v oblasti kybernetickej bezpečnosti v oblasti riadenia zraniteľností OT a riadenia tretích strán. Šiesta časť sa sústreďuje na podstatu SBOM. Siedma časť obsahuje závery.

2. Priemyselný internet vecí (IIoT)

IIoT pozostáva zo snímačov, prístrojov, strojov a iných zariadení, ktoré sú navzájom prepojené a využívajú internetové pripojenie na zlepšenie priemyselných a výrobných podnikových procesov a aplikácií [Berge, 2002]. Implementácia IIoT do prostredí OT môže zvýšiť konektivitu, avšak znamená zmenu bezpečnostnej architektúry. Napríklad zavedenie zariadení IIoT do prostredí OT si môže vyžadovať zmenu perimetra alebo sprístupnenie väčšieho počtu rozhraní a služieb. Zariadenia IIoT môžu, ak nie sú chránené, získať prístup priamo do systémov OT bez autentifikácie a pracovných povolení, aby sa ušetril čas. To, samozrejme, zvyšuje riziko neoprávneného prístupu [Onhus, 2021]. IIoT je niečo, čo treba uznať a pochopiť, avšak zameriavame sa skôr na sieť ako na internet [Knapp, 2024]. Integrácia technológií IIoT do tradičného Purdue modelu [Williams, 1994] alebo modelu ISA-95 [IEC 62334] zároveň predstavuje významnú výzvu pre modernú priemyselnú kybernetickú bezpečnosť a je čoraz viac spochybňované [Mantravadi, 2020]. Integrácia cloudových riešení má veľký vplyv na posun smerom k architektúram veľkých hráčov (hyperscaler), ako sú Microsoft, Amazon, Google, najmä vďaka elasticite mať k dispozícii zdroje v prípade potreby, schopnosti rýchleho škálovania a schopnosti rýchlo nasadzovať a poskytovať zdroje [Perducat,

2023, s. 5]. To viedlo k tomu, že namiesto dodávateľov automatizovaných riešení alebo poskytovateľov siete je to teraz poskytovateľ hyperscaler cloudu v spolupráci s podnikovým IT, kto riadi zmeny v oblasti OT [Perducat, 2023, s. 10]. Cloudové architektúry pre OT však nemajú zavedené postupy najlepšej praxe pre implementáciu, bezpečnostné požiadavky a vykonávanie posúdení bezpečnosti alebo auditov [Stouffer, 2023, s. 82, Perducat, 2023 s. 4].

3. Riadenie zraniteľnosti

Jedným zo základných prvkov programu riadenia zraniteľností je komplexné pochopenie hardvérových, firmvérových a softvérových prostriedkov v organizácii [Riberio, 2024]. Okrem riadenia aktív zohráva konfigurácia týchto aktív kľúčovú úlohu [Kok, 2024, s. 8] pri udržiavaní bezpečného OT prostredia. Bez správneho riadenia konfigurácie organizácie často nemajú prehľad o stave riadenia záplat, bezpečnostných nastaveniach alebo verziách konfigurácie svojho hardvéru, firmvéru a softvéru. Ďalšou významnou výzvou v prostrediach OT je oneskorenie pri vývoji a nasadzovaní záplat bezpečnostných zraniteľností. Vzhľadom na úzke prepojenie softvéru OT a základného hardvéru musia všetky zmeny prejsť rozsiahlym a časovo náročným testovaním, čo s následnou distribúciou aktualizovaného softvéru vytvára otvorené okno zraniteľnosti [Stouffer, 2023, s. 175]. V niektorých priemyselných odvetviach [VCA, 2024], si záplaty môžu dokonca vyžadovať schválenie pre určité zariadenia. K rizikám OT patrí aj to, že dodávatelia môžu odmietnuť vyvinúť záplaty, najmä pre staršie OT systémy [Stouffer, 2023, s. 175].

4. Riadenie tretích strán

Riadenie tretích strán zahŕňa všetky externé subjekty (dodávateľov, poskytovateľov služieb, zmluvných partnerov a iných partnerov), ktoré majú prístup k IT alebo OT prostrediu organizácie alebo ho ovplyvňujú. Tretie strany môžu zaviesť zraniteľnosti buď priamym prístupom k systémom organizácie, alebo poskytovaním kompromitovaného softvéru alebo záplat či aktualizácií [Rebultan, 2023, HS, 2011]. Známym príkladom bol útok malvéru Havex [CISA, 2021], pri ktorom sa na nasadenie malvéru použila legitímna inštalačná služba pre aktualizáciu systému.

Dokumentovanie a sledovanie sériových čísel, kontrolných súčtov, elektronických certifikátov/podpisov alebo iných identifikačných znakov umožňuje overiť pravosť hardvéru, softvéru a firmvéru. Pravidelným posudzovaním dodávateľov sa zabezpečí, aby dodržiavali

postupy najlepšej praxe [Stouffer, 2023, s. 96]. Identifikácia závislostí od otvoreného zdrojového kódu a zavedenie monitorovania relevantných informácií, napríklad aktualizácií z webových stránok dodávateľov alebo spravodajských zdrojov, môže pomôcť uistiť sa, že neboli odhalené žiadne známe zraniteľnosti alebo falošné vydania [Stouffer, 2023, s. 96]. Riadenie identít a prístupov je ďalšou súčasťou riadenia tretích strán, ktorá zabezpečuje, aby každá osoba, proces alebo zariadenie boli riadne identifikované a autorizované pred získaním fyzického alebo logického prístupu ku kritickým zdrojom, ako sú systémy, informácie alebo lokality [Stouffer, 2023, s. 97].

5. Nová regulácia kybernetickej bezpečnosti

5.1 Smernica NIS2

Jedným z hlavných cieľov smernice NIS2 je zabezpečiť OT technológie [David, 2024] a kritickú infraštruktúru. NIS2 stanovuje rámec pre opatrenia kybernetickej bezpečnosti, ktoré budú jednotlivé členské štáty implementovať do svojich vnútroštátnych právnych predpisov.

Opatrenia kybernetickej bezpečnosti musia vychádzať z prístupu založeného na *všetkých rizikách* [článok 21 ods. 2 NIS2], ktorý zahŕňa digitálne aj fyzické hrozby pre sieťové a informačné systémy. Opatrenia musia okrem iného zahŕňať zásady kontroly prístupu [článok 21 ods. 2 písm. i) NIS2], aby subjekty zabezpečili, že prístupové práva budú primerane riešiť prístup tretích strán, najmä obmedzením rozsahu a trvania prístupových práv.

Ďalej sa opatrenia musia priamo týkať bezpečnosti dodávateľského reťazca [článok 21 ods. 2 písm. d) NIS2], zraniteľností špecifických pre každého priameho dodávateľa a poskytovateľa služieb a celkovej kvality produktov a postupov kybernetickej bezpečnosti ich dodávateľov a poskytovateľov služieb vrátane ich bezpečných vývojových postupov [článok 21 ods. 3 NIS2]. To podľa nášho názoru zahŕňa vykonávanie náležitej starostlivosti voči tretím stranám, zohľadnenie požiadaviek na kybernetickú bezpečnosť do procesov obstarávania a priebežné monitorovanie a hodnotenie výkonnosti dodávateľov [rovnako, Stouffer, 2023, s. 96].

5.2 Smernica CER

Cieľom CER je posilniť kritickú infraštruktúru proti fyzickým hrozbám. Kľúčovou požiadavkou je zaistenie fyzickej bezpečnosti kritickej infraštruktúry, ktorá sa vzťahuje aj na zariadenia tretích strán, ktoré podporujú kritické funkcie [článok 13 ods. 1 písm. b) CER]. Ak sa kritický subjekt spolieha na dátové centrum tretej strany, musí posúdiť bezpečnostné

opatrenia zariadenia, ako je monitorovanie perimetra, kontrola prístupu a možnosti reakcie na núdzové situácie, pretože nezabezpečenie fyzickej infraštruktúry tretej strany môže viesť k zneužiteľným zraniteľnostiam. Prípady, ako napríklad použitie sociálneho inžinierstva na narušenie bezpečnosti letísk, systémov energetických sietí alebo jadrových elektrární [Pollack, 2018], zdôrazňujú riziká, ktoré predstavuje nedostatočné zabezpečenie tretích strán. Okrem toho musia kritické subjekty zaviesť postupy riadenia rizík a krízového riadenia, ktoré zahŕňajú postupy reakcie na incidenty týkajúce sa v tretích strán [článok 13 ods. 1 písm. c) CER]. CER vyžaduje, aby kritické subjekty zabezpečili kontinuitu činnosti určením alternatívnych dodávateľských reťazcov a stratégií obnovy, najmä v súvislosti s rizikami tretích strán [článok 13 ods. 1 písm. d) CER]. Tento prístup je kľúčový v odvetviach ako je výroba a distribúcia potravín [Orengo Serra, 2022, s. 14-34]. CER tiež zdôrazňuje dôležitosť riadenia bezpečnosti zamestnancov vrátane preverovania ich minulosti, kontroly prístupu a odbornej prípravy zamestnancov zapojených do kritických funkcií [článok 13 ods. 1 písm. e) CER]. Riziká tretích strán v tejto oblasti môžu zahŕňať externých dodávateľov alebo poskytovateľov služieb s prístupom do citlivých lokalít.

5.3 Nariadenie CRA

CRA bolo v marci 2024 formálne schválené Európskym parlamentom [24]. Po schválení Radou a zverejnení bude platiť prechodné obdobie 36 mesiacov, čo znamená, že výrobcovia budú musieť spĺňať požiadavky od roku 2027 [článok 71, CRA].

Cieľom CRA je v podstate uložiť výrobcom, dovozcom a distribútorom digitálnych produktov určité povinnosti, aby sa zvýšila kybernetická bezpečnosť a zabránilo sa zneužívaniu zraniteľností takýchto produktov. Produktom s digitálnymi prvkami (digitálnym produktom) sa rozumie akýkoľvek softvérový alebo hardvérový produkt a jeho riešenia na diaľkové spracovanie údajov vrátane softvérových alebo hardvérových komponentov, ktoré sa uvádzajú na trh samostatne [článok 3 ods. 1 CRA].

Digitálne produkty sú v CRA rozdelené do troch hlavných kategórií na základe úrovne ich rizika. Prvou sú všeobecné (nekritické) produkty ktoré predstavujú 90 % digitálnych produktov uvedených na trh [Európska komisia, 2023], t. j. hardvér a softvér s nízkou úrovňou kritickosti (napr. hry, pevné disky alebo inteligentní asistenti). Druhým sú dôležité produkty (uvedené v prílohe III, trieda I a trieda II), napr. prehliadače, správcovia hesiel, virtuálne privátne siete (VPN), systémy riadenia bezpečnostných informácií a udalostí (SIEM),

bezpečnostné kamery, alarmy, ďalej firewally, systémy na detekciu a prevenciu vniknutia (IDS/IPS) atď. Treťou a najmenšou kategóriou, sú kritické produkty (príloha IV), napr. hardvérové zariadenia s bezpečnostnými schránkami, čipové karty atď. Aj keď pojmy IIoT ani ICS (SCADA, PLC atď.) nie sú výslovne uvedené, tieto druhy zariadení spadajú do rozsahu pôsobnosti CRA. CRA sa však nevzťahuje na softvér ako službu (SaaS), pokiaľ nie je súčasťou integrálnych riešení diaľkového spracovávania údajov pre digitálny produkt [Recitál č. 12, CRA]; na služby cloud computingu vrátane SaaS, sa totiž vzťahuje NIS2. Základné požiadavky na kybernetickú bezpečnosť sú vymedzené v prílohe I CRA, a mali by byť podrobne rozpracované v harmonizovaných normách a/alebo v spoločných špecifikáciách prijatých Komisiou [článok 27 CRA].

5.3.1 Dodávanie digitálnych produktov bez zraniteľností

CRA v prvom rade vyžaduje, aby digitálne produkty mali *primeranú úroveň kybernetickej bezpečnosti* zodpovedajúcu *rizikám* [bod 1 príloha I CRA]. Po druhé, budú musieť výrobcovia zabezpečiť, aby ich produkty vstupovali na trh *bez známych zneužiteľných zraniteľností* [časť I, bod 2 písm. a) príloha I CRA]. Presný rozsah známych zneužiteľných zraniteľností ostáva bližšie nedefinovaný, bez odkazu napríklad na niektorú z databáz zraniteľností. Okrem toho sa produkty musia poskytovať s konfiguráciou *secure-by-default*, čo znamená, že pri nasadení sú bezpečné na úrovni štandardného nastavenia, pokiaľ nie sú prispôsobené inak na základe osobitných dohôd s komerčnými používateľmi [časť I bod 2 písm. b) príloha I CRA]. Požiadavka secure-by-default je doplnená požiadavkou na obmedzenie plôch útoku vrátane externých rozhraní, ktoré by mohli zneužiť škodlivé subjekty [časť I bod 2 písm. j) príloha I CRA]. Okrem toho by produkty mali byť vybavené mechanizmami na zmiernenie zneužitia, aby sa minimalizoval vplyv akýchkoľvek potenciálnych incidentov [časť I bod 2 písm. k) príloha I CRA]. Tieto požiadavky sa majú spoločne vykonávať i) v závislosti od posúdenia rizík v oblasti kybernetickej bezpečnosti [článok 13 ods. 2 CRA] a ii) podľa potreby.

5.3.2 Poskytovanie bezpečnostných aktualizácií

Medzi požiadavky CRA patrí, aby zraniteľnosti boli riešiteľné prostredníctvom aktualizácií, ktoré môžu zahŕňať automatické aktualizácie nastavené ako predvolené, pričom používatelia majú možnosť v prípade potreby tento proces odmietnuť alebo odložiť [časť I bod

2 písm. c) príloha I CRA]. Od výrobcov sa vyžaduje, aby bezodkladne reagovali na zistené zraniteľnosti a ponúkali bezpečnostné aktualizácie oddelene od aktualizácií funkcií, ak je to technicky možné [časť II bod 2 príloha I CRA]. Týmto oddelením sa zabezpečí, že kritické bezpečnostné záplaty nebudú zdržiavané inými zmenami softvéru, čím sa zníži časový priestor vystavenia sa riziku. Okrem toho musia výrobcovia zaviesť bezpečné mechanizmy na distribúciu týchto aktualizácií, čím sa zabezpečí, že zraniteľnosti budú okamžite odstránené [časť II, bod 7 príloha I CRA]. Dôležité je, že tieto bezpečnostné aktualizácie sa musia poskytovať bezplatne a mali by byť sprevádzané jasnými informačnými správami, ktoré informujú používateľov o opatreniach, ktoré musia prijať, pokiaľ sa výrobca a komerčný používateľ nedohodnú inak pri individualizovanom produkte [časť II bod 8 príloha I CRA].

5.3.3 Práva používateľov

CRA kladie dôraz na práva používateľov pri riadení bezpečnosti produktov. Používatelia majú možnosť kontrolovať spôsob uplatňovania bezpečnostných aktualizácií, pričom majú možnosť odmietnuť automatické aktualizácie a možnosť ich dočasného odloženia [Časť I bod 2 písm. c) Prílohy I CRA]. Túto úroveň kontroly ďalej podporujú požiadavky, aby produkty ponúkali informácie týkajúce sa bezpečnosti prostredníctvom monitorovania a zaznamenávania interných činností, pričom používatelia majú možnosť sa z takéhoto monitorovania v prípade potreby odhlásiť [Časť I bod 2 písm. l) Prílohy I CRA]. Okrem toho musia mať používatelia možnosť trvalo bezpečne odstrániť všetky údaje a nastavenia zo svojich zariadení a pri prenose údajov do iných produktov alebo systémov sa tento proces musí uskutočniť bezpečným spôsobom [Časť I bod 2 písm. m) Prílohy I CRA]. Od výrobcov sa vyžaduje zverejňovanie informácie o odstránených zraniteľnostiach. Výnimkou je, ak výrobcovia usúdia, že bezpečnostné riziká zverejnenia prevažujú nad bezpečnostnými výhodami, takže môžu odložiť zverejnenie informácií o opravenej zraniteľnosti až do doby, keď používatelia budú mať možnosť aplikovať príslušnú záplatu [Časť II, bod 4 príloha I CRA]. Okrem toho sa od výrobcov vyžaduje, aby zaviedli a presadzovali koordinované politiky oznamovania zraniteľností a zabezpečili, aby boli používatelia okamžite informovaní o potenciálnych rizikách [Časť II bod 5 príloha I CRA]. Tieto opatrenia posilňujú postavenie používateľov, ich aktívnu úlohu a tiež zodpovednosť za riadenie bezpečnosti používaných produktov.

7. Softvérový kusovník (SBOM)

Výrobcovia sú povinní identifikovať a zdokumentovať zraniteľnosti a komponenty v rámci svojich produktov do SBOM [Časť II bod (1) príloha I CRA]. SBOM nie je len záznam informácií o podrobnostiach a vzťahoch v rámci dodávateľského reťazca komponentov použitých v digitálnom produkte [článok 3 ods. 39 CRA], môže obsahovať ďalšie informácie o svojom obsahu vrátane autorských práv a údajov o licenciách a verziách [Linux Foundation, 2022, s. 44].

Požiadavka SBOM nie je žiadnou novinkou v oblasti kybernetickej bezpečnosti. V Spojených štátoch od roku 2021, musia federálnu agentúru použiť od dodávateľov predloženie SBOM [Executive Order, 2021], a to v súlade s minimálnymi prvkami [NTIA, 2021].

Keďže SBOM bude patriť ku kľúčovým požiadavkám podľa CRA, dôraz by mal byť na definovaní obsahu a formátu SBOM. Rovnako je dôležité, aby organizácie dostali návod ako plánovať, vyvíjať, nasadzovať a používať SBOM [Alberts, 2023]. Bude teda kľúčové, ako Európska komisia využije oprávnenie vydať implementačné nariadenie pre CRA na spresnenie formátu a prvkov softvérového kusovníka [článok 13 ods. 24 CRA].

Samotná smernica NIS2 výslovne neuvádza povinnosti regulovaných subjektov ohľadom SBOM, ale využitie SBOM možno podľa nášho názoru určite zaradiť pod opatrenia na riadenie kybernetických rizík. V kontexte riadenia tretích strán [článok 21 ods. 2 písm. d) NIS2], SBOM umožňuje subjektu podrobne sledovať a overovať softvér, ktorý im poskytuje priamy dodávateľ alebo poskytovateľ služieb, čím sa znižuje riziko zavlečenia zraniteľností cez tretie strany. Ďalej, pri získavaní, vývoji a údržbe sietí a informačných systémov [článok 21 ods. 2 písm. e) NIS2], SBOM poskytuje prehľad o všetkých softvérových komponentoch, čo je potrebné pre riešenie zraniteľnosti a správne zverejňovanie informácií o týchto zraniteľnostiach. SBOM sú aj ukazovateľom uplatňovania postupov bezpečného vývoja softvéru. SBOM je tiež dôležitým nástrojom na zabezpečenie kybernetickej bezpečnosti zariadení IIoT a IoT [Danagana, 2022, s. 3].

Okrem softvéru sa venuje značná pozornosť aj významu transparentnosti a bezpečnosti hardvérových komponentov, čo viedlo k vytvoreniu rámca pre hardvérový kusovník (Hardware Bill of Materials - HBOM). HBOM poskytuje podrobný súpis hardvérových komponentov v systéme, podobne ako SBOM pre softvér [CISA, 2023]. CRA však neobsahuje výslovnú požiadavku na HBOM pre digitálne produkty.

6. Záver

Pre OT prostredie osobitne, je charakteristické nerovné postavenie zmluvných strán, kde rokovania o zmluvách často zvýhodňujú dodávateľov, čo vedie k situáciám, keď sa zákazník stáva príliš závislým od technológie alebo služieb jedného dodávateľa (vendor lock-in). Táto závislosť obmedzuje schopnosť zákazníka rokovať o bezpečnostných aktualizáciách, procesoch riadenia záplat, formáte a detaile SBOM či celkovej kontrole nad stavom bezpečnosti systému.

Z našej analýzy vyplýva, že mnohé prostredia OT, ktoré využívajú predovšetkým cloudovú architektúru, trpia miznúcim perimetrom. Podľa nášho názoru, sa riadenie identity a prístupov sa čoraz viac stáva novým perimetrom, čo si vyžaduje, aby zmluvy s tretími stranami jasne riešili zodpovednosti súvisiace s riadením identít a prístupov.

Hoci sa SBOM čoraz viac uznáva ako dôležitý nástroj na zaistenie bezpečnosti a integrity softvérových komponentov, jeho prijatie zostáva zatiaľ viac víziou než plnohodnotným uplatnením v praxi. Vývoj a implementácia ďalších nástrojov, ako sú napríklad hardvérové kusovníky (HBOM), sú kľúčové pre dosiahnutie viditeľnosti v systémoch OT. Riešenie problému vendor lock-in, dôsledná správa identít a prístupov, a presadzovanie zahrnutia nástrojov ako je SBOM a HBOM do zmlúv aj do požiadaviek právnej regulácie, bude mať podľa nás zásadný význam pre posilnenie odolnosti prostredí OT voči rizikám tretích strán a pri riadení zraniteľností. V tomto smere považujeme za kľúčový posun presadenie základných požiadaviek na kybernetickú bezpečnosť digitálnych produktov.

Zoznam odkazov:

1. NIST SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations

A System Life Cycle Approach for Security and Privacy (2018) [online]. [cit. 26.8.2024]. Dostupné z: https://doi.org/10.6028/NIST.SP.800-37r2

2. DAVID, I. Průmyslová kybernetická bezpečnost dle NIS2 a nového českého Zákona o kybernetické bezpečnosti. Data Security Management (DSM). 2024, 11.8.2024, 10. ISSN 2336-6745
3. STOUFFER K, PEASE M, et al. (2023) *Guide to Operational Technology (OT) Security*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-82r3. [online]. [cit. 26.8.2024]. Dostupné z: https://doi.org/10.6028/NIST.SP.800-82r3
4. Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)
5. Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES (smernica CER)
6. návrh nariadenia Európskeho parlamentu a Rady o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadenia (EÚ) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)) prijatý 12. Marca 2024 Európskym parlamentom (nariadenie CRA)
7. BERGE, J. (2002) Fieldbuses for Process Control: Engineering, Operation, and Maintenance. (International Society of Automation, Research Triangle Park, North Carolina).
8. KNAPP, Eric D. Industrial Network Security (Third Edition), Syngress, 2024, Pages 1-9, ISBN 9780443137372, [online]. [cit. 26.8.2024]. Dostupné z: https://doi.org/10.1016/B978-0-443-13737-2.00016-6.
9. ONSHUS, T. et al. ICT Security and Independence, Report, 2021:01387 – Open. Version 2, 17 December 2021, [online]. [cit. 26.8.2024]. Dostupné z: https://www.havtil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/sintef---report---ict-security-and-independence.pdf
10. WILLIAMS, Theodore J. The Purdue enterprise reference architecture, Computers in Industry, Volume 24, Issues 2–3, 1994, Pages 141-158, ISSN 0166-3615, [online]. [cit. 26.8.2024]. Dostupné z: https://doi.org/10.1016/0166-3615(94)90017-5.
11. ISO/IEC 62334 Enterprise-control system integration
12. MANTRAVADI, S. R. et al, "Securing IT/OT Links for Low Power IIoT Devices: Design Considerations for Industry 4.0," in *IEEE Access*, vol. 8, pp. 200305-200321, 2020, [online]. [cit. 26.8.2024]. Dostupné z: doi: 10.1109/ACCESS.2020.3035963.
13. PERDUCAT, C. Et al., "Evolution and Trends of Cloud on Industrial OT Networks," in IEEE Open Journal of Industry Applications, vol. 4, pp. 291-303, 2023, [online]. [cit. 26.8.2024]. Dostupné z: doi: 10.1109/OJIA.2023.3309669
14. RIBERIO, A. Dealing with OT asset monitoring and discovery to enhance cybersecurity across industrial, OT systems (9 March 2024) [online]. [cit. 26.8.2024]. Dostupné z: https://industrialcyber.co/features/dealing-with-ot-asset-monitoring-and-discovery-to-enhance-cybersecurity-across-industrial-ot-systems/

15. KOK, A. et al. (2024). The Impact of Integrating Information Technology With Operational Technology in Physical Assets: A Literature Review. IEEE Access. PP. 1-1. [online]. [cit. 26.8.2024]. Dostupné z: 10.1109/ACCESS.2024.3442443.
16. Vehicle Certification Agency. Cyber Security and Software Updating (14 May 2024) [online]. [cit. 26.8.2024]. Dostupné z: https://www.vehicle-certification-agency.gov.uk/connected-and-automated-vehicles/cyber-security-and-software-updating
17. REBULTAN, M. A.G. Common Cybersecurity Risks to ICS/OT Systems, 12 June 2023 [online]. [cit. 26.8.2024]. Dostupné z: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/common-cybersecurity-risks-to-ics-ot-systems
18. Hommeland Secuirty, Common Cybersecurity Vulnerabilities Identified in DHS Industrial Control Systems Products (2011) [online]. [cit. 26.8.2024]. Dostupné z: https://www.cisa.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf
19. CISA ICS Advisory. ICS Focused Malware (2021) [online]. [cit. 26.8.2024]. Dostupné z: https://www.cisa.gov/news-events/ics-advisories/icsa-14-178-01
20. POLLACK, J., & RANGANATHAN, P. (2018). Social engineering and its impacts on critical infrastructure: A comprehensive survey. Athens: The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). [online]. [cit. 26.8.2024]. Dostupné z: https://www.proquest.com/conference-papers-proceedings/social-engineering-impacts-on-critical/docview/2153616034/se-2
21. ORENGO SERRA, K.L. and SANCHEZ-JAUREGUI, M. (2022), "Food supply chain resilience model for critical infrastructure collapses due to natural disasters", British Food Journal, Vol. 124 No. 13, pp. 14-34. [online]. [cit. 26.8.2024]. Dostupné z: https://doi.org/10.1108/BFJ-11-2020-1066
22. Európska komisia. EU Cyber Resilience Act [online]. [cit. 26.8.2024]. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
23. Európska komisia, 'Cyber Resilience Act – Factsheet' (1 December 2023) [online]. [cit. 26.8.2024]. Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet
24. The Linux Foundation, Software Bill of Materials (SBOM) and Cybersecurity Readiness (2022), [online]. [cit. 26.8.2024]. Dostupné z: https://www.linuxfoundation.org/research/the-state-of-software-bill-of-materials-sbom-and-cybersecurity-readiness
25. President's Executive Order (EO) 14028, 86 Fed. Reg. 26,633 on Improving the Nation's Cybersecurity issued on May 12, 2021
26. National Telecommunications and Information Administration (NTIA), The Minimum Elements For a Software Bill of Materials (2021) [online]. [cit. 26.8.2024]. Dostupné z: https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
27. ALBERTS, C., et al, 2023: The SEI SBOM Framework: Informing Third-Party Software Management in Your Supply Chain. Carnegie Mellon University, Software Engineering Institute's Insights (blog), [online]. [cit. 26.8.2024]. Dostupné z: https://doi.org/10.58012/kste-p278.

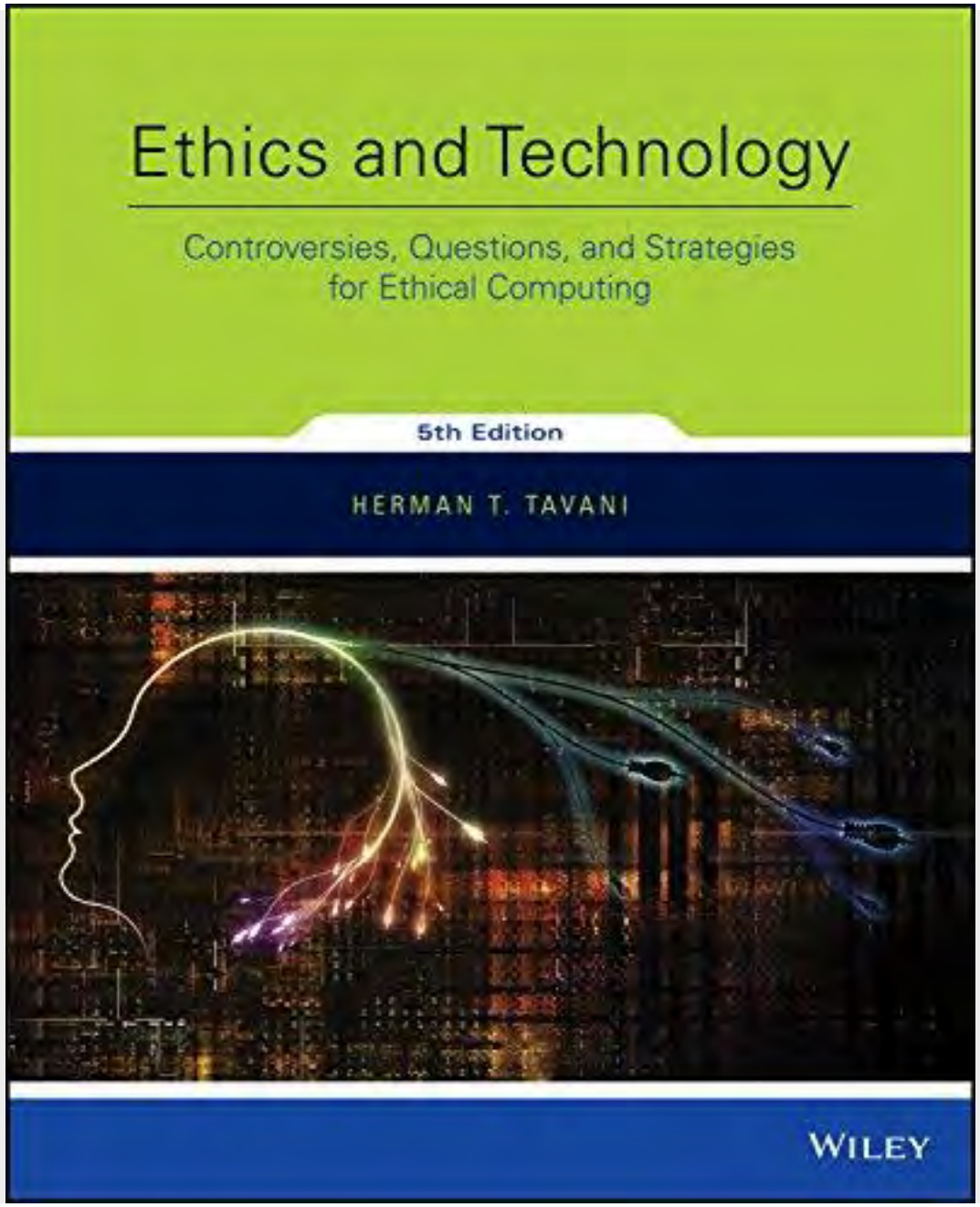
28. DANGANA I, ALRICH T, Using SBOMs to Secure Industrial IoT Devices (2022) the Journal of Innovation, [online]. [cit. 26.8.2024]. Dostupné z: https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/07/6-JOI_20220727_Using_SBOMs_to_Secure_Industrial_IoT_Devices_Standalone.pdf
29. CISA Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management (2023) [online]. [cit. 26.8.2024]. Dostupné z: https://www.cisa.gov/resources-tools/resources/hardware-bill-materials-hbom-framework-supply-chain-risk-management

etické dosahy algoritmov umelej inteligencie a posudzovanie vplyvu digitálnych technológií

miroslav.pikus@e-tika.sk

“všetko čo potrebujete aby bolo vaše mesto smart, je všetko so všetkým prepojiť”

Herman T. Tavani



prínosy vs. neduhy

sú technológie hodnotovo neutrálne?

Stanovisko Telegramu k zatknutiu ich CEO:

”Technológia predsa nemôže za to, ako ju kto použije”

algoritmy ovplyvňujú naše životy

- prijatie na štúdium / do zamestnania
- úvery
- liečba
- sociálne benefity
- kritická infraštruktúra
- …

sú algoritmy (a-)politické?

- sú technológie apolitické (kávovar)
- ..a sú technológie politické (jadrové zbrane)
- prípadne sú spolitizované (ručné zbrane)
- kam patria algoritmy?

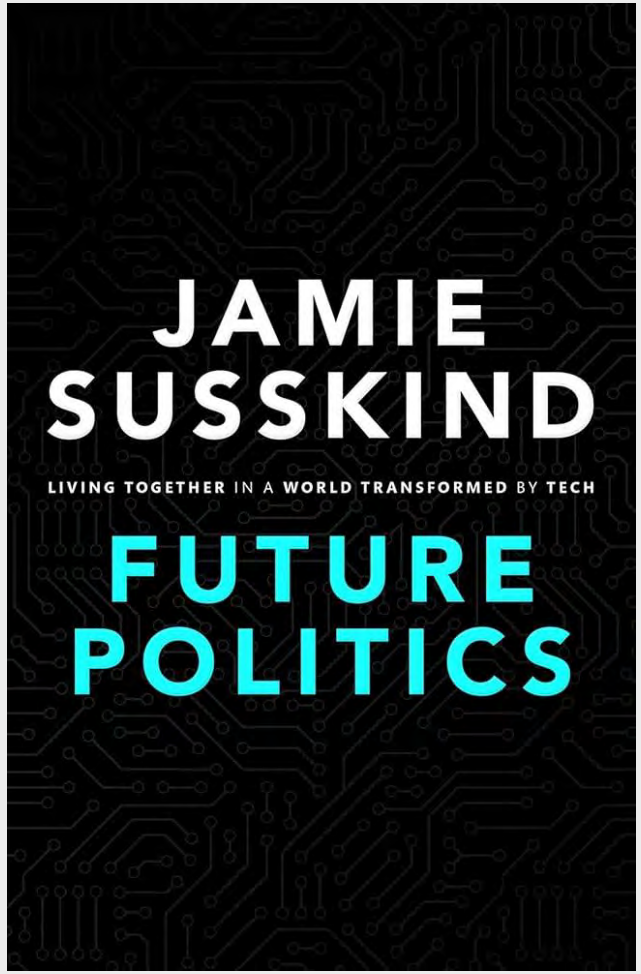
(politická) moc digitálnych technológií

- stanovujú pravidlá, ktoré je nutné dodržiavať
- podrobne skúmajú ľudí
- vytvárajú náš pohľad na svet
- ovplyvňujú spoločenský dialóg

IT špecialisti majú podobne silný vplyv na spoločnosť ako napr. zdravotníci či právnici

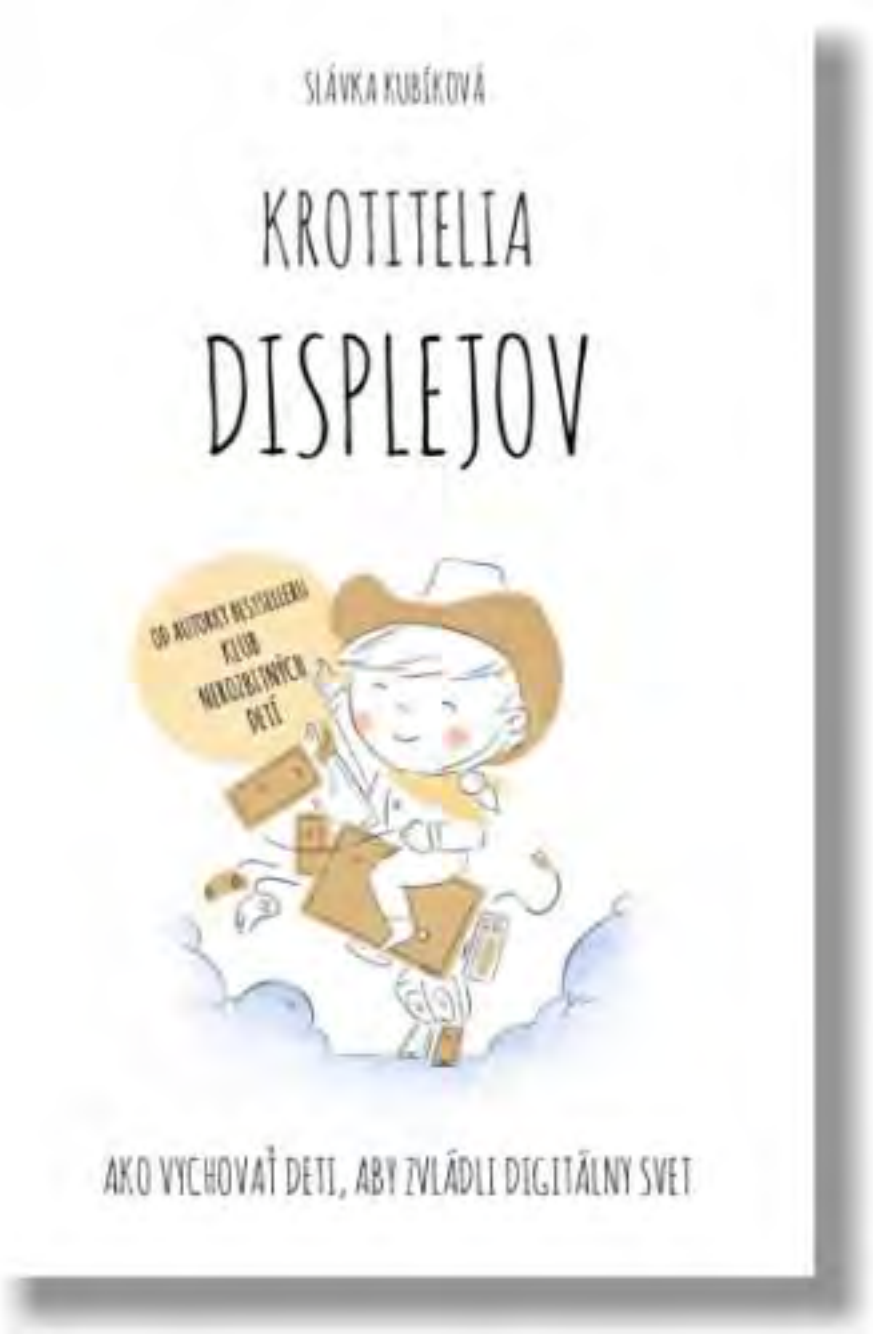
- …ale (takmer) nie sú regulovaní
- skúšky, certifikáty, atestácie
- kurzy lekárskej etiky vs kurzy počítačovej etiky

jamie susskind

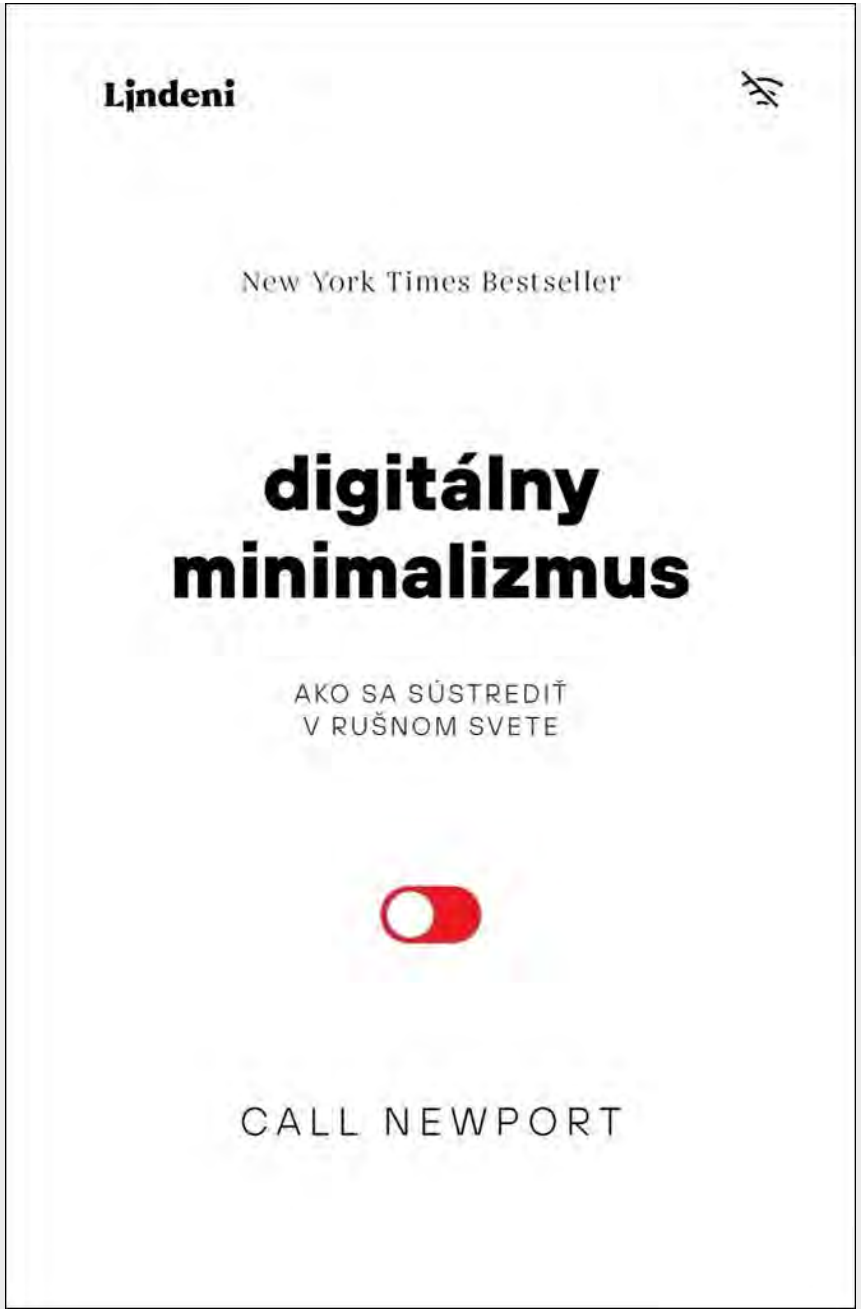


adam greenfield

slávka kubíková



cal newport


Lindeni
New York Times Bestseller
digitálny minimalizmus
AKO SA SÚSTREDIŤ V RUŠNOM SVETE
CALL NEWPORT

regulácia a sloboda

- nestačí “neviditeľná ruka trhu?”
- zákony obmedzujú slobodu
- zlebo: zákony podporujú slobodu?

iniciatívy na budovanie zodpovedného prístupu k AI

- Singapur – Model AI Governance Framework
- Responsible Research and Innovation
- Ethical Aligned Design
- Canada – Artificial Intelligence and Data Act
- EU – Ethics Guidelines for Trustworthy AI
- EU – AI Act

zodpovedné AI

- transparentnosť
- nediskriminácia a férovosť
- spoľahlivosť, technická odolnosť a bezpečnosť
- správa súkromia a údajov
- ľudský faktor a dohľad

Zodpovedné AI

systematické a odborné posúdenie etických rizík AI

- ”Príručka o etických rizikách algoritmov”
- E-tika.sk
- Dohľad nad AI Act

ako identifikovať etické riziká

1. Vplyv. Skúma sa, ako algoritmus ovplyvní ľuďi a majetok.

2. Vhodné používanie. Kontroluje sa vzťah medzi údajmi používanými v algoritme a účelom, na ktorý sa zbierali, ako aj vnímaním ich očakávaného použitia.

3. Zodpovednosť. Zisťuje sa, do akej miery sú ľudia zapojení do prebiehajúceho používania algoritmu, ako aj to, či sa dajú automatizované rozhodnutia každému jasne vysvetliť.

4. Skreslenie a predpojatosť. Skúma sa skrytý vplyv dát a ľuďi, ktorí sa podieľali na vytvorení algoritmu.

EÚ AI act

- účinnosť od 1.augusta 2024
- široká definícia ai zahrňuje aj “klasický” sw
- úzke zameranie na použitie algoritmov
- zakazuje manipulatívne či klamlivé ovplyvňovanie
- zakazuje hodnotenie občanov na základe správania, prediktívnu políciu
- obmedzenie použitia biometrie
- automatizované spracovanie úverov, poistných udalostí, sociálnych benefitov
- agenda ľudských zdrojov
- pridaná oblast četbotov
- pokuty až do výšky 7% z obratu
- AI a autorské práva

kto je kto v SK AI etike

Juraj Podroužek (KINIT)

Matúš Mesarčík (KINIT)

Juraj Čorba (MIRRI)

ďakujem za pozornosť

- miroslav.pikus@e-tika.sk

bonus?

mestá nasadzujú smart lampy.
tie vedia (okrem iného) svietiť viac či menej.
navrhnite algoritmus, akým by sa pri tom mali riadiť

kde svietiť viac? tam, kde je...

- ....viac ľudí,
- viac dopravy,
- voličov,
- prosperity (daní z nehnuteľnosti),
- kriminality (bolo vs. bude),
- dopravných nehôd,
- bezdomovcov,
- podujatie ako futbalový zápas

kto určí kde svietiť viac a kde menej?

- primátor, starosta
- poslanci
- občianske združenia, aktivisti
- výrobca lámp
- dodávateľ lámp
- programátor lámp
- all of the above
- ai of the above
- občania prostredníctvom stáleho hlasovania (aplikáciou?)
- senzor (podľa jasu, zvuku a pod.)

uzávery

- kľúčový prínos smart osvetlenia by mal byť efektivita, ale..
- svietiť menej alebo vôbec je rizikové – môže spraviť zle.
- zmysel má skôr jednoduchý algoritmus založený na senzoroch..
- ..než komplikované AI algoritmy

Prověříme kybernetickou odolnost vaší firmy

Důsledně. Komplexně.
Postupy, které používají hackeři

www.cyber-rangers.com

TANEC S VLKY V KYBERPROSTORU

Daniel Hejda | Cyber Rangers s.r.o.

CEH | C|OSINT | CompTIA Pentest+ | CompTIA CySA+ | eWPT | Microsoft MVP | PECB IEC/ISO 27001 Lead Auditor

Ethical Hacker & Founder of Cyber Rangers

@daniel_hejda | daniel@cyber-rangers.com | www.cyber-rangers.com

CYBER RANGERS
ARMORING YOUR BUSINESS

Daniel Hejda

Spoluzakladatel | Etický hacker

Daniel Hejda je red teamer, výzkumník, sociální inženýr a bezpečnostní konzultant s více jak 15 lety praxe v oblasti IT technologií a 5 let v oblasti technologií OT. V rámci své činnosti se zabývá nejen audity, poradenstvím a testováním, ale také přednášením na předních českých konferencích. Mezi hlavní činnosti v oblasti bezpečnosti patří penetrační testování, sociální inženýrství, zpravodajská činnost a výzkum kybernetických útoků nejen státem sponzorovaných skupin (APT).

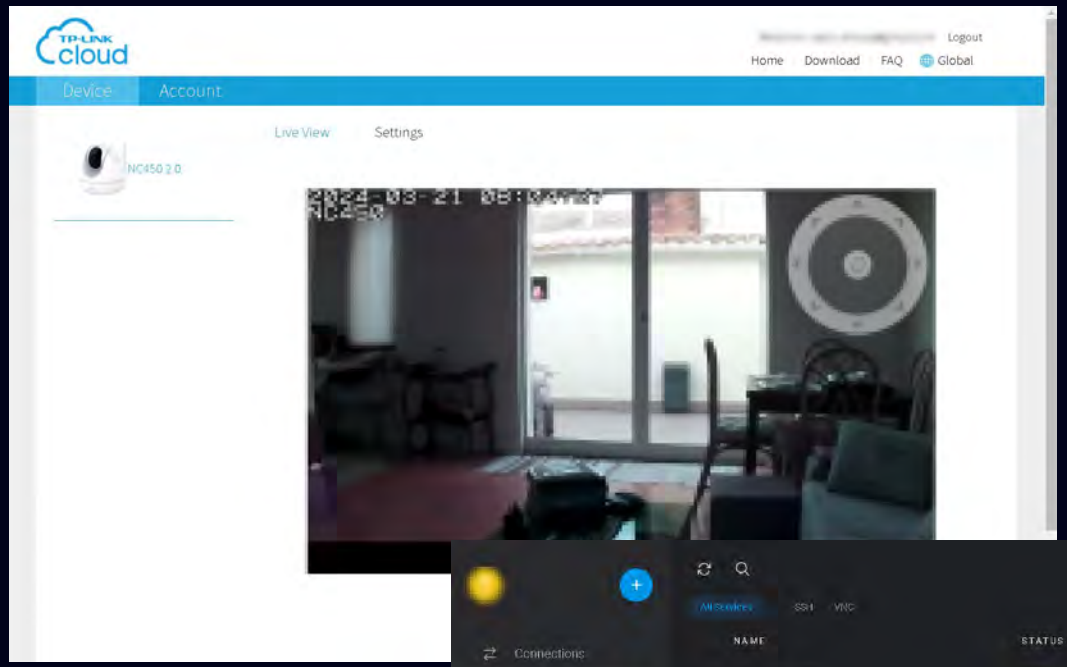
Nejsilnější je v disciplínách

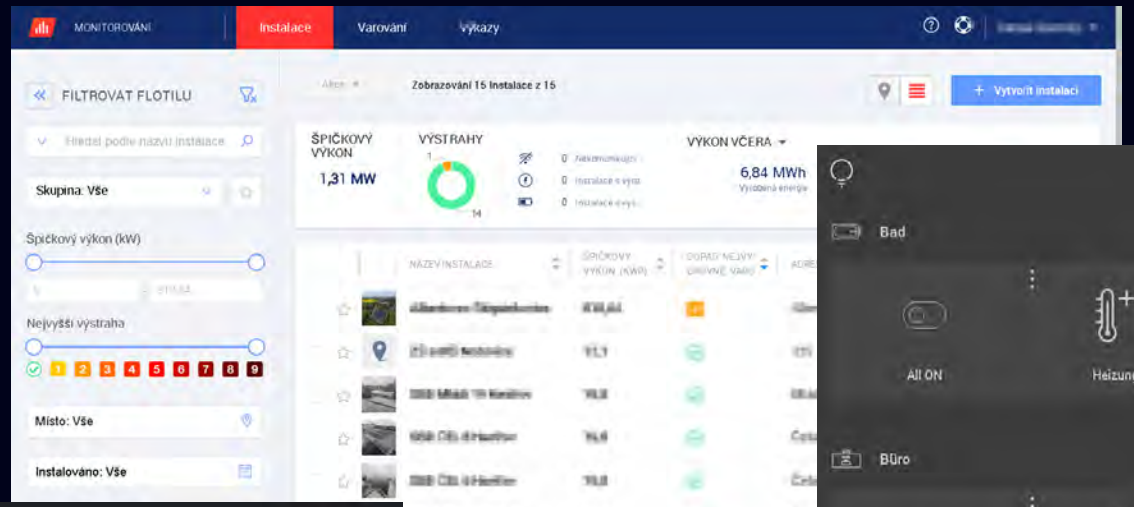
- Red Teaming se zaměřením na fyzický a lidský aspekt
- Penetrační testování IT/OT prostředí
- Sociální inženýrství
- Zpravodajská činnost (OSINT, HUMINT, SOCINT, atd.)

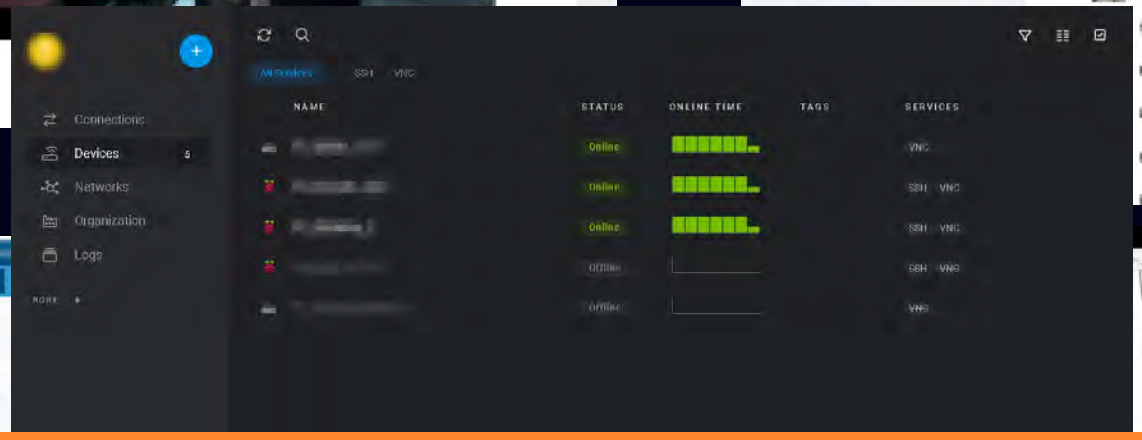
MÁTE NA POČÍTAČI UŽIVATELSKÁ OPRÁVNĚNÍ PŘI PŘÍSTUPU DO INTERNETU A SKORO VŠUDE MFA?

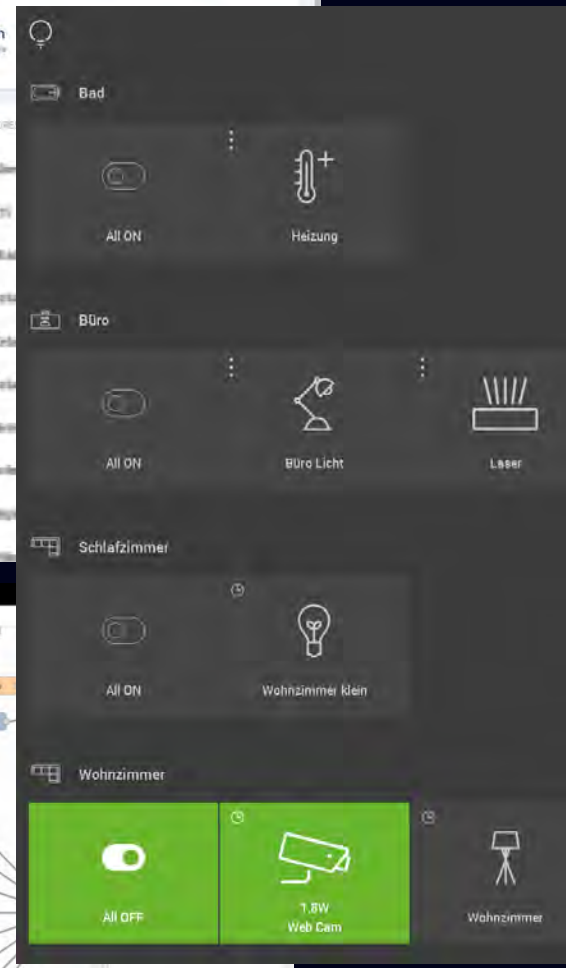
A CO KDYŽ MŮŽETE PŘIJÍT O SVÉ PŘÍSTUPY NEVĚDOMKY?

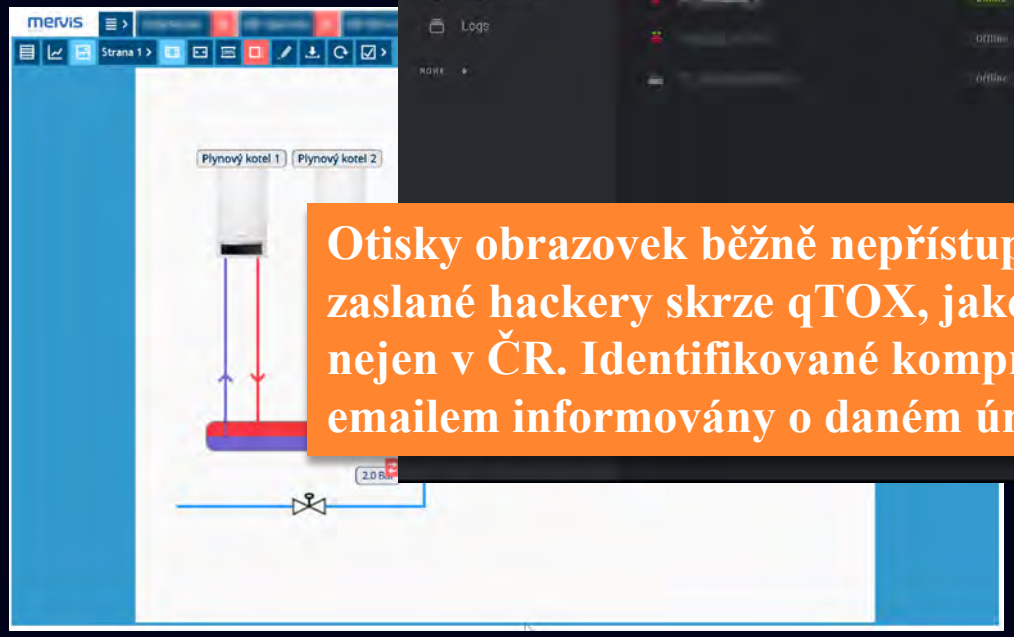
CHTĚLI BYSTE ABY STATISÍCE LIDÍ MĚLI VAŠE PŘÍSTUPY K DISPOZICI?











Otisky obrazovek běžně nepřístupnýh zařízení, které byly zaslané hackery skrze qTOX, jako PoC přístupů do zařízení nejen v ČR. Identifikované kompromitované osoby byly emailem informovány o daném úniku informací

SITUACE

- Sdílíte s rodinnou (dětmi) jeden počítač?
- Připojujete se ze stejného počítače do
  - Banky?
  - Práce?
  - E-shopů?
  - Chytré domácnosti?
  - Kamerám?
  - Atd.
- Co když si dítě chce doinstalovat doplněk do legální hry? Co když si může nainstalovat doplněk do prohlížeče? Napadlo vás někdy, že by mohl být malware i tam?

O CO SE JEDNÁ?

Infostealer malware

- Malware, který pravidelně vykrádá váš PC/Mobil
- Krade obrovské množství informací
- Některé obsahují keyloggery
- Některé postavené jako Remote Access Tooly (HVNC)
- Některé přesně cílené na konkrétní státy (identifikace přes ipinfo.io uvnitř malware)
- Kompletní customizace a vždy nový payload

Infostealer browser extensions

- Kontroluje celý prohlížeč (může ovládat cokoliv děláte i v jiných záložkách)
- Může zasahovat do obsahu stránky (mění obsah)
- Může zasahovat do požadavku i odpovědi serveru (proxy)
- Může kontrolovat kameru a mikrofon na vašem PC

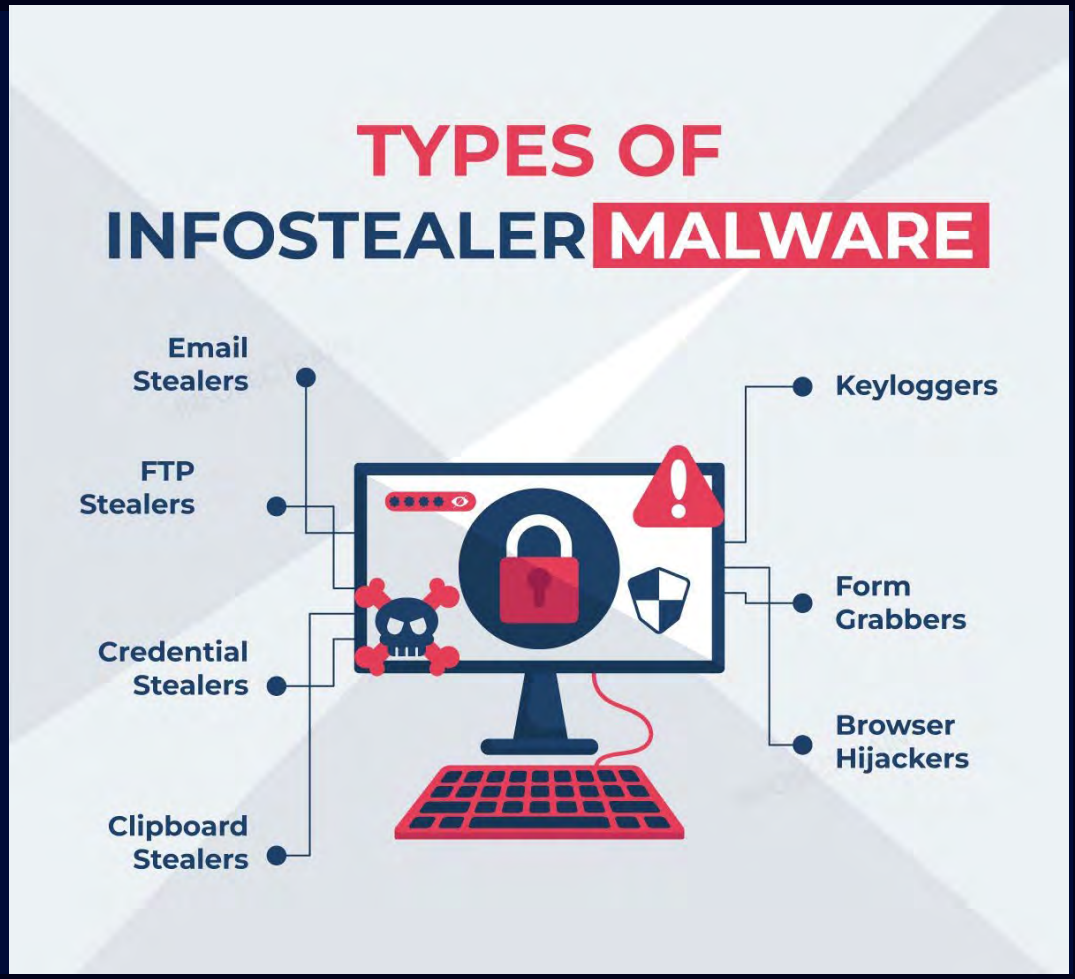
Malware, který se zaměřuje na odcizení dat z VAŠEHO počítače

ZBRAŇ VŠECH KYBERNETICKÝCH ŠPIÓNŮ

- **Malware, který se zaměřuje na odcizení dat z počítače**
- Aktéři využívají logy (digitální entity s ukradenými přístupy) k dalším operacím (např. iniciální vstup)
- Denně se ve volném prostředí Dark/DeepWebu pohybuje několik desítek tisíc nových přístupů od stále nových inzerentů
- Infostealery jsou často distribuovány jako Malware-as-a-Service (kdokoliv si může pronajmout licenci tohoto software)
- Některé infostelaery jsou postaveny na bázi keyloggeru a jiné fungují více jako Remote Access Trojan / Remote Access Tool / Hidden Virtual Network Computing (skryté VNC)

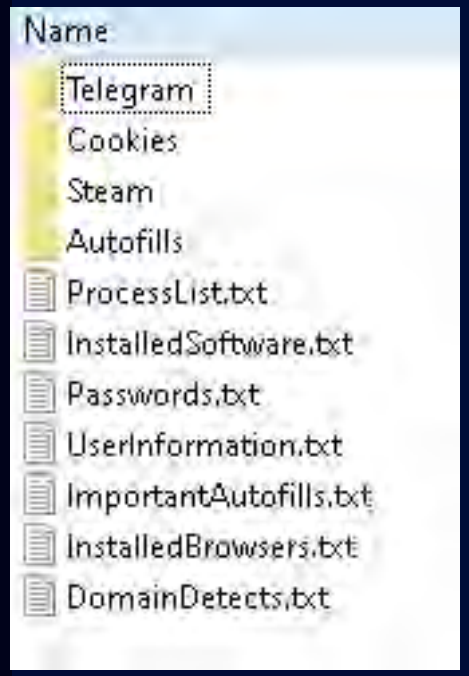
NA JAKÁ DATA SE INFOSTELAER ZAMĚŘUJE

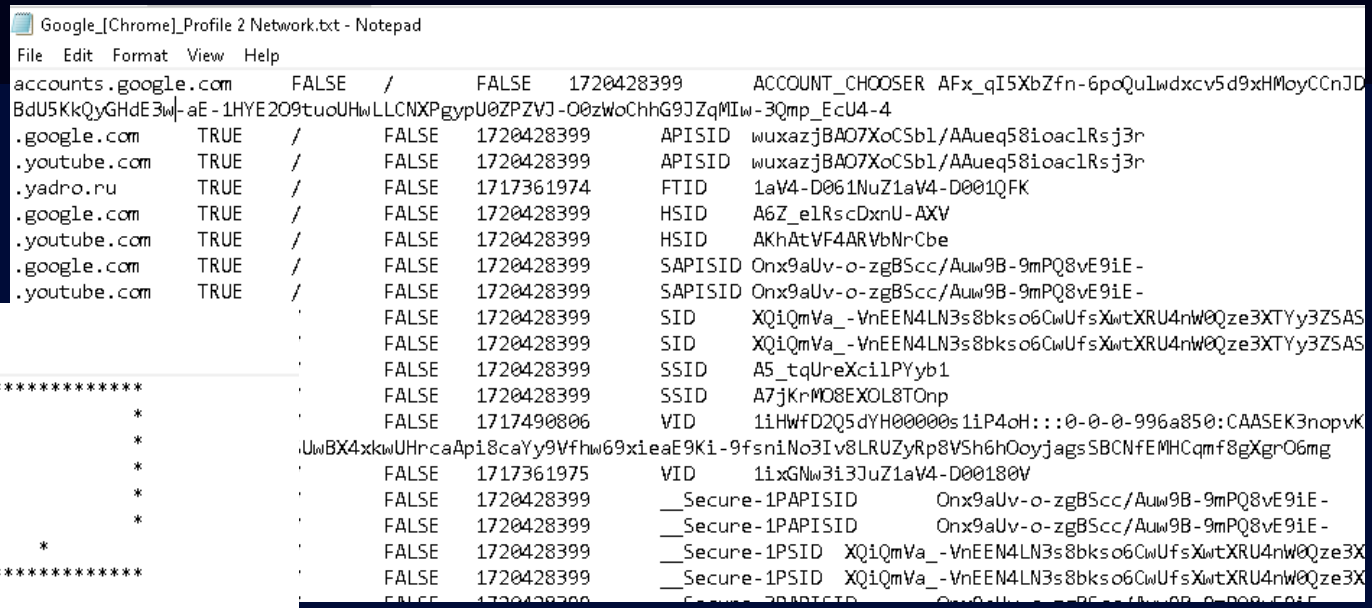
- **Uživatelská jména, hesla a URL adresy** (mnohem zákeřnější než přípravy combolistů)
- **Autentizační cookies a Access / Refresh tokeny do aplikací** (bankovní aplikace, platební portály, e-shopy a další aplikace chráněné MFA)
- **Přístupy do krypto peněženek** (tokeny do krypto peněženek, informace o zůstatcích, atd.)
- **Dokumenty** (dokumenty ze speciálních umístění – chaty, soubory z plochy / dokumentů, atd.)
- **Informace z vyplňovaných formulářů** (autocomplete informace, kreditní karty)
- **Informace z paměti počítače** a některých procesů v počítači (lsass proces například)
- **Informace o počítači** (aplikace, služby, hostname, ip adresy (lokální/veřejné), jméno profilu, atd.)
- Otisky obrazovky nebo z kamery zařízení, případně nahrávky zvuků

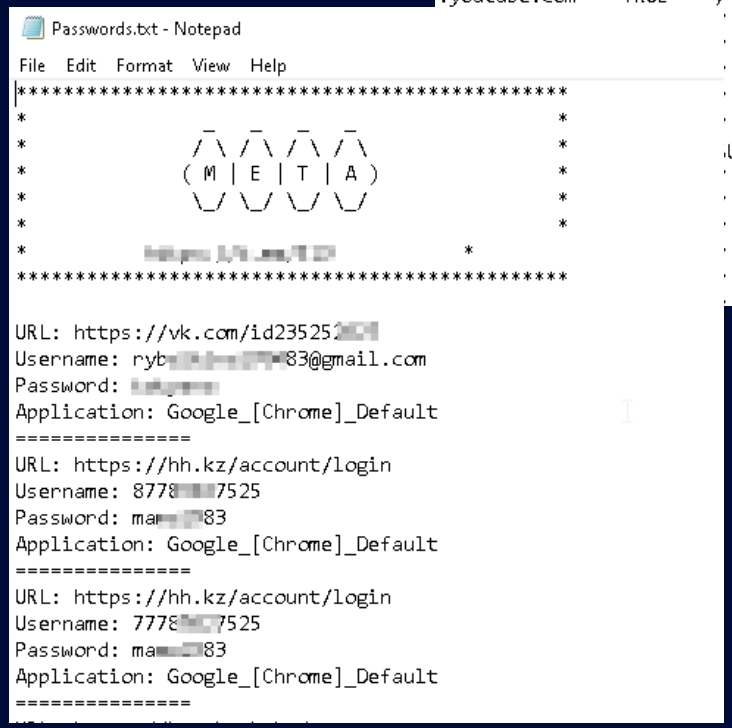


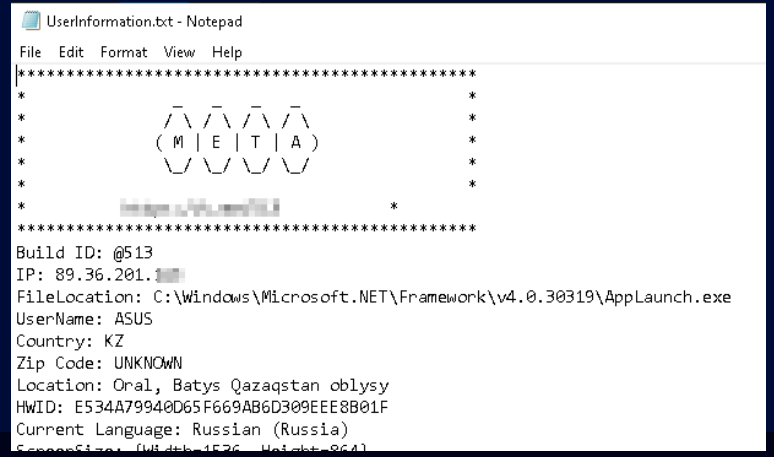
https://www.linkedin.com/pulse/what-infostealer-malware-infosec-train/

JAK VYPADÁ OBSAH INFOSTELAER LOGU



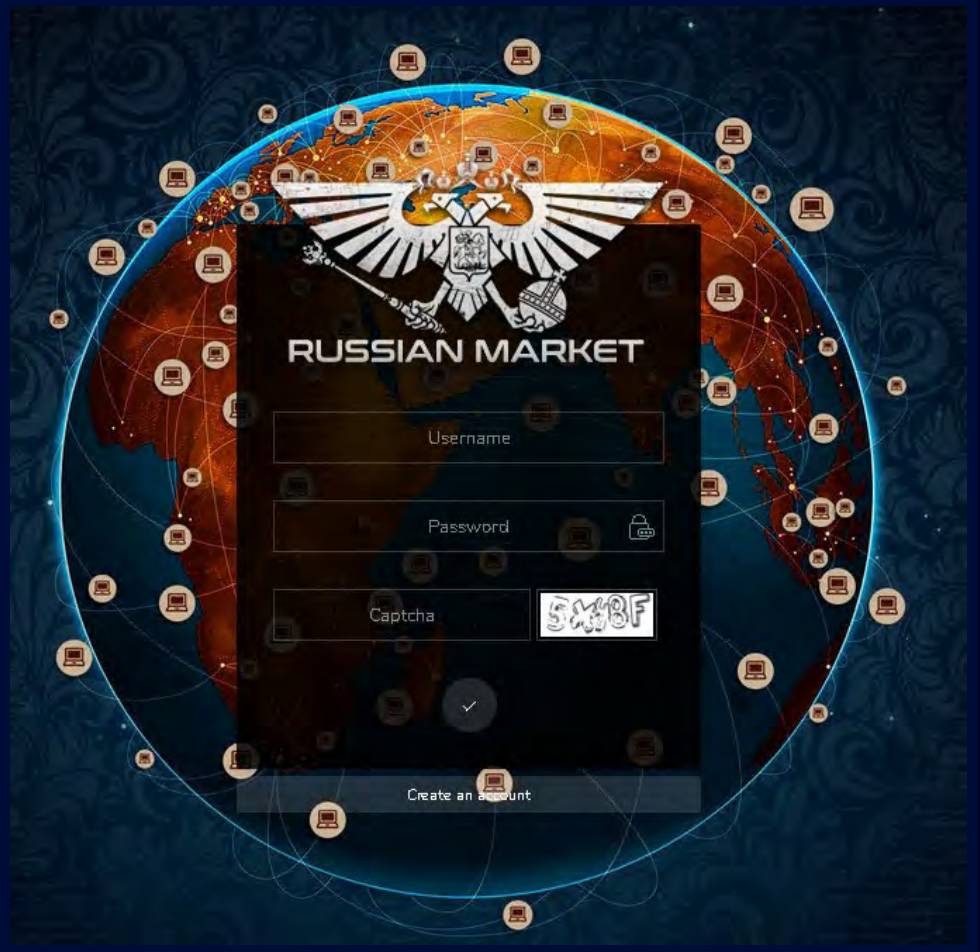




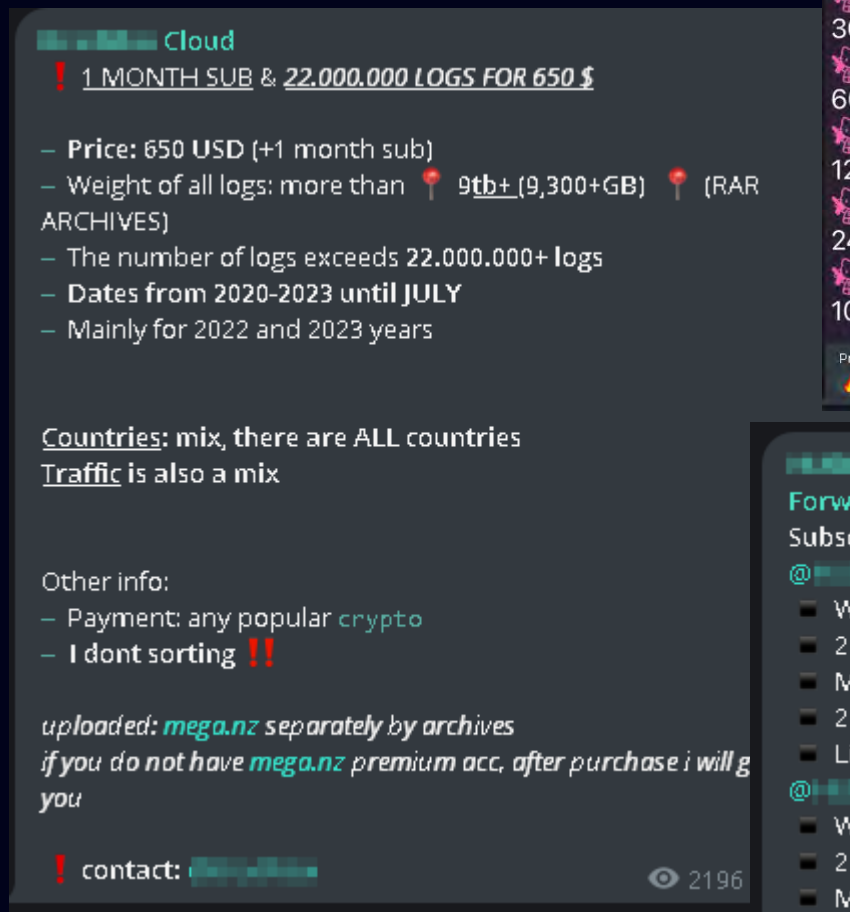


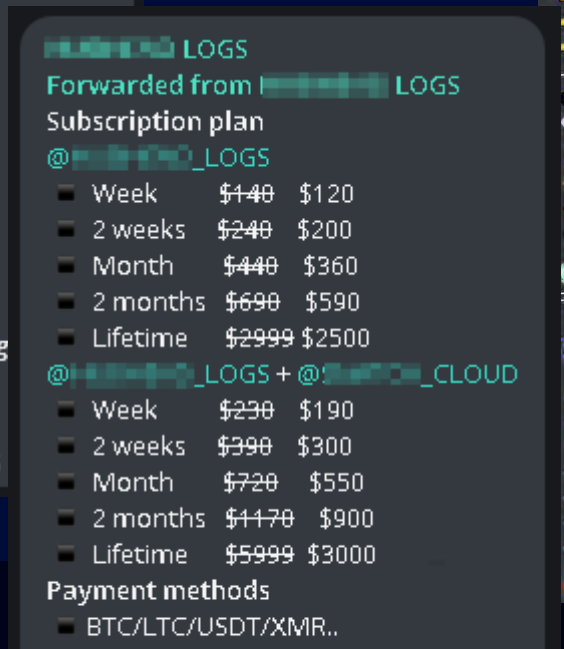
DISTRIBUČNÍ KANÁLY LOGŮ INFOSTEALERU

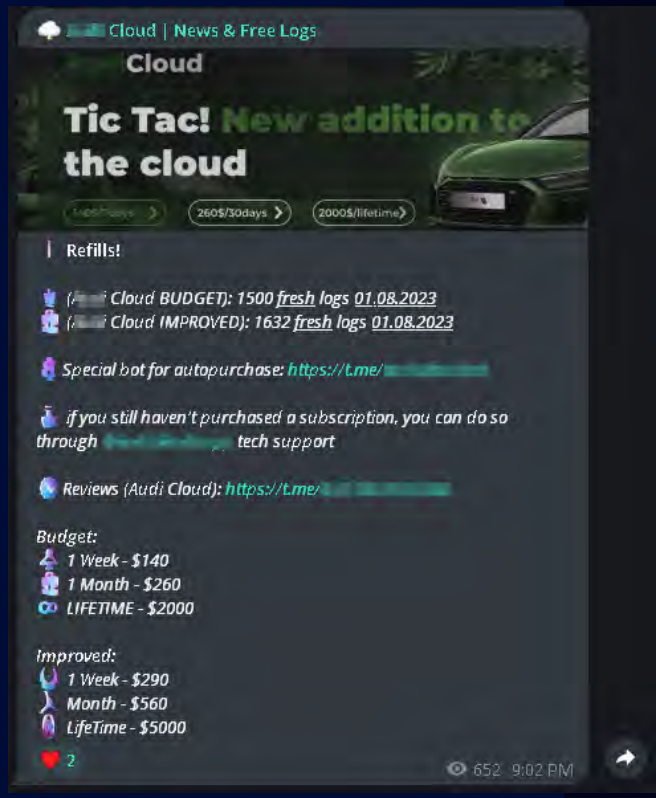
- Primárním kanálem je Telegram a
- Dalším velkým kanálem jsou Dark/Deep/SurfaceWeb diskuzní fóra (většina na dostupná na SurfaceWebu)
  - Hydra Market (public a VIP za poplatek)
  - Russian Market (za poplatek)
  - Raidforums (zavřeno)
  - Genesis Market (pouze pro zvané, zavřeno v surface webu / dark web stále funguje)
  - ...
- Obsah je v zásadě duplicitním, protože se každý snaží monetizovat obsah někoho jiného
- Kvalitní obsah není veřejně přístupný a je pouze pro zvané

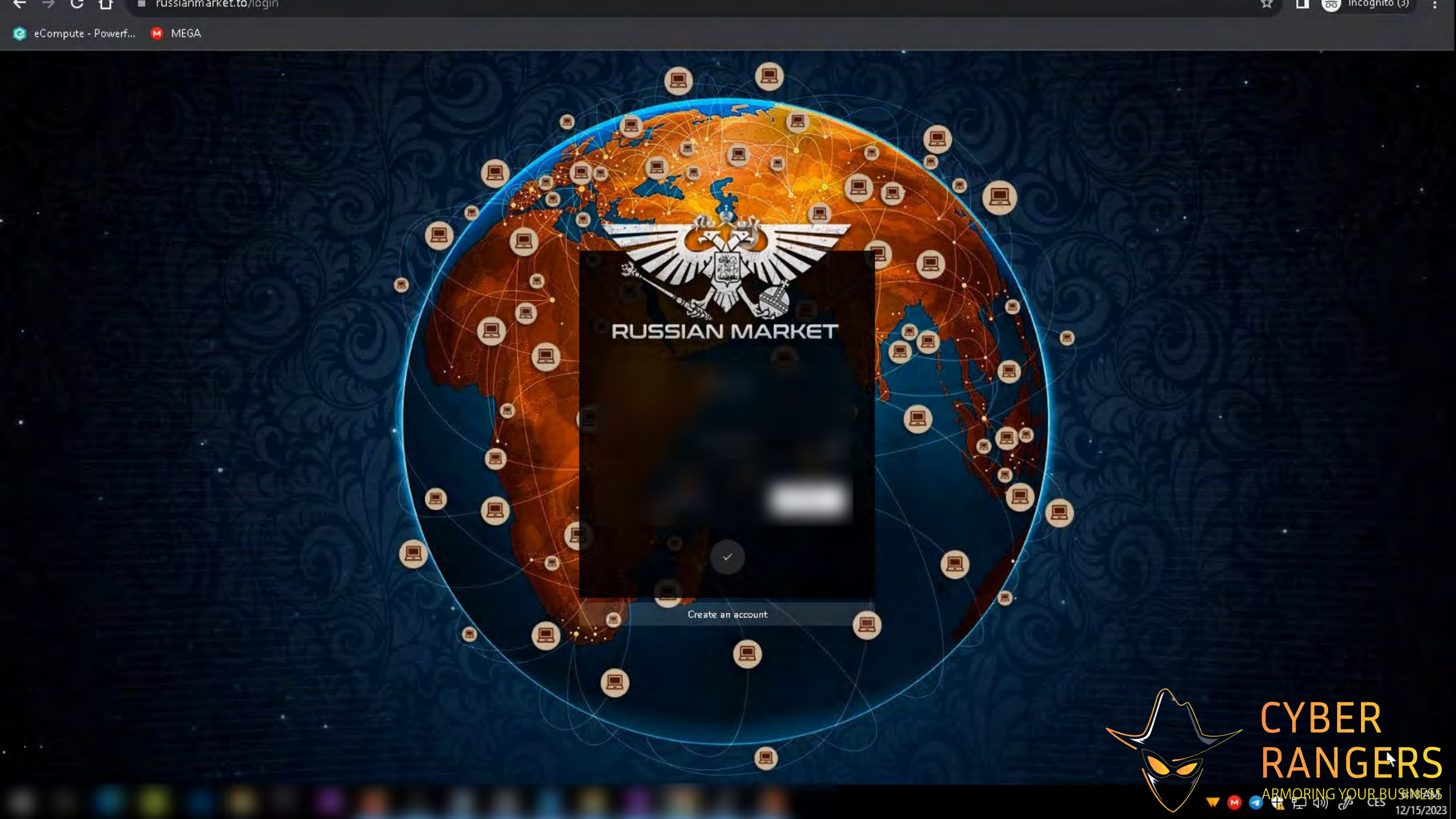


VÍCE JAK 1 000 000 SUBSCRIBERS V TELEGRAMU



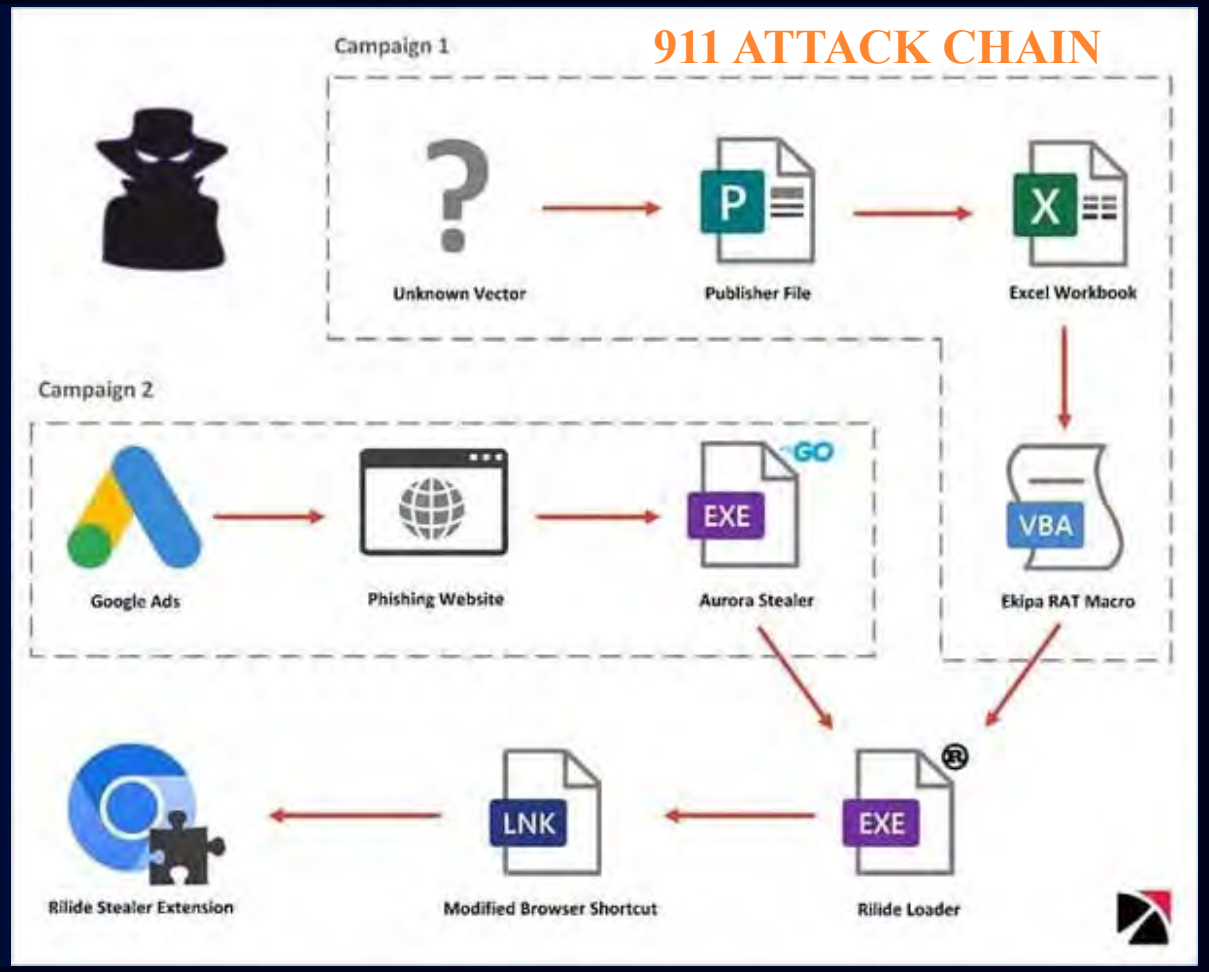





russianmarket.to/login
Incognito (3)
eCompute - Powerf...
MEGA
RUSSIAN MARKET
Create an account
CYBER
RANGERS
ARMORING YOUR BUSINESS
CES
12/15/2023

JAK SE DOSTÁVÁ INFOSTEALER K OBĚTEM

- **Cracky programů a her (file inject)**
  - dll, exe, bat, atd.
- **Ads (Facebook, Google, atd.)**
  - Směrování na podvodný web s malware
- **Phishing**
  - Odkazy na webové stránky s možností stažení obsahu (programu)
  - Odkaz na užitečné doplňky programů (vysoká oprávnění přístupu k prohlížeči nebo možnost stažení dalšího obsahu (programu))
    - ChromeLoader
    - Mystic Stealer 1.2
    - Vlastní doplněk Cyber Rangers



https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/rilide-a-new-malicious-browser-extension-for-stealing-cryptocurrencies/

Extensions

Chrome | chrome://extensions

Relaunch to update

Extensions

Search extensions

Developer mode

Load unpacked | Pack extension | Update

My extensions

Keyboard shortcuts

Discover more extensions and themes on the Chrome Web Store

All Extensions

Passafe 1.0
Checks the strength of the entered password.
ID: eohlmndlhnkboegailkhabokhhjgnblh
This extension cannot read and change site information or run in the background

1Password – Password Manager 2.17.1
The best way to experience 1Password in your browser. Easily sign in to sites, generate passwords, and store secure information.
ID: aeblfdkhhhdcdjpifhhbdiojplfjncoa
Inspect views service worker
Details | Remove

Absolute Enable Right Click & Copy 1.3.8
Force Enable Right Click & Copy
ID: jdocbkpgdakpekjlhemmfcncgdjeiika
Inspect views background.html
Details | Remove

Adblock Plus - free ad blocker 3.21.1
Block YouTube™ ads, pop-ups & fight malware!
ID: cfhdojbkjhnklbpkdaibdccddilifddb
Inspect views background page
Details | Remove

Adobe Acrobat: PDF edit, convert, sig... 23.11.1.0
Do more in Google Chrome with Adobe Acrobat PDF tools. View, fill, comment, sign, and try convert and compress tools.
ID: efaidnbmnnnibpcajpcglclefindmkaj
Details | Remove

Awesome Screen Recorder & Screenshot 4.4.4
The best screen recorder and screen capture & screenshot tool to record screen.
ID: nlipoenfbbikpbjkfpfillcgkoblgpmj
Inspect views service worker (Inactive)
Details | Remove

Beanote - Note Taking on Web Pages 1.5.5
This extension helps you to highlight, take notes and annotate on web pages.
ID: nikccehomlnjkmgmhnieecolhgdafajb
Inspect views background page
Details | Remove

ClickOnce for Google Chrome 2.1
Adds basic support for launching ClickOnce applications (by Menarva Ltd).
ID: kekahkplibinaibelipdcikofmedafmb
Details | Remove

Cookie Manager 0.1.1
Cookie Manager
ID: bjdaiadcbbcomhnlhpnbmnnfcnhkiibj
Details | Remove

Crypto Web Extension 24.1.8725
The extension is intended only for TESCO SW a.s. web applications and provides communication

Cyber Rangers: Ransomware Alert System 1.0.4
Ransomware tracker based on DeepDarkCTI, Ransomwatch and RansomLook.

EditThisCookie 1.6.3
EditThisCookie is a cookie manager. You can add, delete, edit, search, protect and block cookies!

Prověříme kybernetickou odolnost vaší firmy

Důsledně. Komplexně.
Postupy, které používají hackeři

www.cyber-rangers.com

Q & A

TANEC S VLKY V KYBERPROSTORU

Daniel Hejda | Cyber Rangers s.r.o.

CEH | C|OSINT | CompTIA Pentest+ | CompTIA CySA+ | eWPT | Microsoft MVP | PECB IEC/ISO 27001 Lead Auditor

Ethical Hacker & Founder of Cyber Rangers

@daniel_hejda | daniel@cyber-rangers.com | www.cyber-rangers.com

CYBER RANGERS
ARMORING YOUR BUSINESS

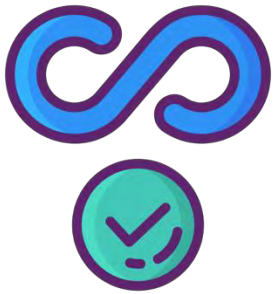
www.cyber-rangers.com

NOVELA ZÁKONA č. 69/2018 Z. z. o KYBERNETICKEJ BEZPEČNOSTI prichádza

EPI Konferencia
Kybernetická bezpečnosť 2024
30. 9. – 1. 10. 2024
Liptovský Mikuláš, Hotel Grand Jasná****

Transpozícia NIS2 – povinná jazda ale nie len...

Transpozícia smernice (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (**smernica NIS 2**)



Úprava zákona na základe skúseností z praxe

- Spresnenie niektorých definícií
- Flexibilnejšia aplikácia opatrení
- Zjednodušenie hlásení incidentov
- Podrobnejšia úprava oprávnení úradu v rámci dohľadu

Základná zmena koncepcie NIS2

Predmetom regulácie nie je kybernetická bezpečnosť vo vzťahu k základným službám ale **kybernetická bezpečnosť a odolnosť kľúčových subjektov** a celých sektorov voči aktuálnym kybernetickým hrozbám.

Kľúčové zmeny

- **Rozšírenie** pôsobnosti zákona **na nové subjekty**
- **Identifikácia regulovaného subjektu** na základe jeho zaradenia do sektora
- **Aplikácia bezpečnostných opatrení** na základe rizikovej analýzy
- **Úprava bezpečnosti dodávateľského reťazca**
- **Úprava hlásenia incidentov**
- Koordinované zverejňovanie zraniteľností
- Audit a samohodnotenie
- **Certifikácia** bezpečnosti IKT produktov a služieb

Rozšírenie pôsobnosti zákona a identifikácia subjektov (PZS)

Prevádzkovateľom základnej služby (PZS) je (bez ohľadu na sektor):

- **ústredný orgán štátnej správy a iný štátny orgán s celoštátnou pôsobnosťou,**
- **kritický subjekt,**
- **štátny orgán vykonávajúci pôsobnosť v najmenej dvoch okresoch a vyšší územný celok,** ak by narušenie ich činnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,
- **mesto,** ak by narušenie výkonu jeho pôsobnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,
- **správca ITVS** po predchádzajúcej konzultácii s príslušným ústredným orgánom,
- **osoba, ktorá poskytuje službu registrácie názvu domény** bez ohľadu na splnenie podmienok veľkosti pre stredný podnik alebo
- **tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti,** má uzatvorenú zmluvu s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu

Rozšírenie pôsobnosti zákona a identifikácia subjektov (PZS)

PZS sú ďalej subjekty zaradené do sektorov podľa prílohy 1 a 2:

- ak sú **minimálne stredným podnikom** (min. 50 zamestnancov a obrat alebo súvaha 10mil. Eur a viac)

- **bez ohľadu na veľkosť:**
  - je podnikom poskytujúcim verejnú EK sieť alebo verejnú EK službu,
  - je poskytovateľom dôveryhodnej služby,
  - je správcom TLD,
  - poskytuje službu DNS,
  - je v Slovenskej republike jediným poskytovateľom služby, ktorá je kľúčovou službou,
  - poskytuje službu, ktorej narušenie by mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,
  - poskytuje službu alebo má také postavenie, že narušenie poskytovania služby alebo zásah do postavenia by mohli vyvolať významné systémové riziko pre celý sektor vykonávanej činnosti, najmä ak by takéto riziko mohlo mať cezhraničný vplyv,
  - je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritická pre konkrétny sektor, alebo
  - je subjektom hospodárskej mobilizácie, ktorému bolo uložené opatrenie podľa osobitného predpisu,

SEKTORY S VYSOKOU ÚROVŇOU KRITICKOSTI (príloha 1)	INÉ KRITICKÉ SEKTORY (príloha 2)
Energetika (vykurovanie, chladenie, vodík)	Poštové a kuriérske služby
Doprava	Odpadové hospodárstvo
Financie	Výroba a distribúcia chemických látok
Zdravotníctvo	Výroba a distribúcia spracovanie potravín
Voda a atmosféra (odpadová voda)	Výroba (zdrav. pomôcky, elektro, výpočtová technika, optika, stroje a zariadenia, motorové vozidla, iné dopr. prostriedky)
Digitálna infraštruktúra	Poskytovatelia digitálnych služieb
Riadenie služieb IKT	Výskum
Verejná správa	
Vesmír	

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Rozšírenie pôsobnosti zákona a identifikácia subjektov (PKZS)

Kritickou základnou službou je:

- výkon pôsobnosti **ústredného orgánu štátnej správy alebo iného štátneho orgánu s celoštátnou pôsobnosťou,**
- **činnosť v sektore podľa prílohy č. 1,** okrem sektoru verejná správa, ak ju vykonáva osoba, ktorá **presahuje podmienky veľkosti pre stredný podnik** (min. 250 zamestnancov a obrat 50 mil. EUR alebo súvaha 43mil. EUR a viac),
- **kvalifikovaná dôveryhodná služba,**
- **správa TLD,**
- **služba DNS,**
- **poskytovanie verejnej EK siete alebo verejnej EK služby osobou, ktorá dosahuje najmenej podmienky veľkosti pre stredný podnik,**
- vykonávanie činnosti alebo existencia postavenia podľa § 17 ods. 1 písm. c) piateho až deviateho bodu,
- poskytovanie základnej služby **kritickým subjektom,**
- informačná činnosť a elektronické služby, vykonávané s použitím **ITVS** určených úradom**.**

Aplikácia bezpečnostných opatrení

- Nová štruktúra všeobecných bezpečnostných opatrení (§20 ods. 1 a 2)
- Podrobnejší popis bezpečnostných opatrení bude obsahovať vyhláška
- **Rozsah a spôsob implementácie bezpečnostných opatrení na základe rizikovej analýzy**
- Ak existuje **sektorový bezpečnostný štandard,** opatrenia sa aplikujú na jeho základe pri zachovaní základných spôsobilostí riadiť informačnú bezpečnosť, hlásiť a riešiť incidenty a pod. (§20 ods. 6)
- **Povinnosť zaviesť bezpečnostné opatrenia do 12 mesiacov odo dňa zápisu do registra PZS**

Úprava bezpečnosti dodávateľského reťazca

Tretia strana - dodávateľ na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre PZS.

- **PZS je povinný uzatvoriť s treťou stranou zmluvu** o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
- Tretia strana je povinná zaviesť a vykonávať bezpečnostné opatrenia podľa zmluvy a zákona
- Tretia strana je povinná podrobiť sa kontrole plnenia požiadaviek zmluvy a zákona zo strany PZS
- Tretia strana, ktorá nemá sídlo alebo miesto podnikania na území EÚ je povinná ustanoviť zástupcu na území EÚ (v krajine kde vykonáva svoju činnosť)

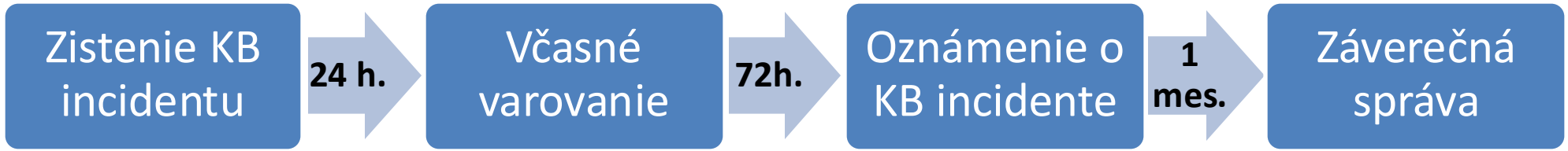
Tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, má uzatvorenú zmluvu s PZS, ktorý prevádzkuje kritickú základnú službu **má postavenie PZS**

- PKZS je povinný úradu hlásiť uzatvorenie zmluvy s takouto treťou stranou a aj jej ukončenie
- tretia strana sa **zapisuje do registra PZS**
- tretia strana povinná plniť bezpečnostné opatrenia podľa zákona a **podlieha dohľadu zo strany NBÚ**
- tretej strane je možné uložiť **povinnosť riešiť KB incident** alebo vykonať reaktívne opatrenie v čase krízy

Úprava hlásenia kybernetických bezpečnostných (KB) incidentov

PZS je povinný:

- **hlásiť závažný KB incident NBÚ** prostredníctvom jednotného informačného systému kybernetickej bezpečnosti



- **hlásiť ďalšie dôležité udalosti:**
  - významnú kybernetickú hrozbu, o ktorej sa dozvie,
  - udalosť odvrátenú v poslednej chvíli, ktorá mohla spôsobiť závažný kybernetický bezpečnostný incident,
  - zraniteľnosť, ktorá môže byť zneužitá na spôsobenie závažného KB incidentu a PZS ju nevie efektívne odstrániť alebo minimalizovať riziko jej zneužitia

Ostatné udalosti môže PZS hlásiť dobrovoľne. Rovnako tak aj akákoľvek iná osoba.

Zraniteľnosti a ich koordinované zverejňovanie

Aktívne vyhľadávanie zraniteľností

- oprávnenie národnej jednotky CSIRT vykonávať automatizovanú detekciu zraniteľností v rámci kybernetického priestoru SR
- aj sektorové jednotky CSIRT v rámci svojej konštituencie
- pomoc PZS pri ich mitigácii

Koordinované zverejňovanie zraniteľností

- mediácia a koordinácia pri zistení zraniteľnosti, jej analýze a zverejňovaní
- účelom je ochrana výskumníka/ nahlasovateľa a PZS resp. výrobcu alebo poskytovateľa IKT produktu alebo služby
- cieľom je analýza zraniteľnosti, jej katalogizácia (CVE) a koordinované zverejnenie s minimalizáciou negatívnych dopadov na zúčastnené strany

Audit a samohodnotenie

Povinnosť vykonať audit:

- PZS prvý audit do 2 rokov od zapísania do registra PZS a následne v periodicite podľa vyhlášky
- Audit vykonáva certifikovaný audítor kybernetickej bezpečnosti podľa príslušnej schémy
- **PZS, ktorý neposkytuje kritickú službu,** môže audit vykonať aj tzv. **samohodnotením**.
- Samohodnotenie vykonáva manažér kybernetickej bezpečnosti
- PZS, ktorý si zvolil vykonanie audit samohodnotením musí vykonať prvý **audit prostredníctvom certifikovaného audítora do 5 rokov** a následne v periodicite podľa vyhlášky
- Podrobnosti o audite upravuje vyhláška

Certifikácia kybernetickej bezpečnosti

- Systémom certifikácie kybernetickej bezpečnosti je súbor pravidiel a postupov na riadenie jednotlivých schém certifikácie kybernetickej bezpečnosti.

- Schéma certifikácie kybernetickej bezpečnosti je súbor pravidiel, technických požiadaviek, technických noriem a postupov, ktoré sa uplatňujú na certifikáciu alebo posudzovanie zhody konkrétnych produktov IKT, služieb IKT alebo procesov IKT.

- Certifikáciu kybernetickej bezpečnosti pre úrovne záruky základná, významná a vysoká podľa osobitého predpisu vykonáva len akreditovaná osoba.

- Akreditovanou osobou pre certifikáciu kybernetickej bezpečnosti pre úroveň záruky vysoká môže byť len Národný bezpečnostný úrad

Jaroslav Ďurovka, CISM
Riaditeľ Národného centra kybernetickej bezpečnosti

Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti

Road 2 Cyber

EPI Kybernetická bezpečnosť 2024

Tomáš Hettych, CISA, CISM, CGEIT, CRISC, CDPSE, ITIL4 Master

Člen predstavenstva KCCKB, COO

KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Skrátene „Kompetenčné centrum", alebo „KCCKB" je štátna príspevková organizácia zriadená Národným bezpečnostným úradom podľa § 21 zákona č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy

Hlavné úlohy:

- Pôsobnosť **Národného koordinačného centra** v zmysle Nariadenia EÚ č. 2021/887 o Európskej sieti centier odvetvových, technologických a výskumných kompetencií
- Certifikácia:
  - audítorov a manažérov kybernetickej bezpečnosti
  - produktov v kybernetickej bezpečnosti podľa Nariadenia EÚ č. 2019/881
- Vzdelávanie v kybernetickej bezpečnosti
- Organizácia kampaní na zvyšovanie povedomia v kybernetickej bezpečnosti
- Publikačná činnosť , organizácia podujatí
- Audit kybernetickej bezpečnosti podľa zákona č. 69/2018 Z.z.
- Konzultačné služby v oblasti kybernetickej bezpečnosti, utajovaných skutočností a dôveryhodných služieb
- Znalecká a expertízna činnosť podľa zákona č. 382/2004 Z. z.. o znalcoch

ĽUDSKÉ ZDROJE PRE KYBERNETICKÚ BEZPEČNOSŤ

ZÁKONNÉ ROLY V KYBERNETICKEJ BEZPEČNOSTI

Manažér kybernetickej bezpečnosti

Podľa §20 ods. 4 písm. a) Zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti:

- bezpečnostné opatrenia musia zahŕňať najmenej **určenie manažéra kybernetickej bezpečnosti,** ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti

Audítor kybernetickej bezpečnosti

Podľa §29 ods. 3 Zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti:

- Audit kybernetickej bezpečnosti vykonáva **certifikovaný audítor kybernetickej bezpečnosti,** ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby
- Certifikáciu audítora kybernetickej bezpečnosti vykonáva **osoba akreditovaná podľa osobitného predpisu** ako orgán certifikujúci osoby (v oblasti kybernetickej bezpečnosti)

KTO JE CERTIFIKOVANÝ AUDÍTOR?

- Koľko máme certifikovaných audítorov kybernetickej bezpečnosti?
  - 70+
- Aké predpoklady musí certifikovaný audítor splniť?
  - Disponuje medzinárodným IT alebo security auditným certifikátom (CISA, ISO27001 Auditor, ISO20000 Auditor)
  - Mať auditné skúsenosti
  - Absolvovať certifikačnú skúšku
- Akú metodológiu auditor využíva?
  - Auditnú vyhlášku
  - Metodiku auditu KB
  - Automatizovaný auditný checklist/dotazník a auditnú správu

KTO JE MANAŽÉR KYBERNETICKEJ BEZPEČNOSTI?

- MKB/CISO je pracovná rola, nie len pozícia
  - nemusí byť jedinou rolou zamestnanca
  - rolu môže plniť viacero osôb (zastupiteľnosť)
  - a naopak – rola môže byť zdieľaná medzi viacerými zákazníkmi (outsourcing)
- SR je prvým ČŠ EÚ, ktorý má požiadavky na znalosti a zručnosti v KB stanovené právnym predpisom:
  - Vyhláška Národného bezpečnostného úradu č. 492/2022 Z. z. ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti

Zdroj: Vyhláška NBÚ č. 492/2022 o znalostných štandardoch v KB


I CAME HERE TO DRINK MILK AND KICK ASS
AND I'VE JUST FINISHED MY MILK.

EURÓPSKY VS. SLOVENSKÝ RÁMEC ROLÍ V KB

1. Manažér kybernetickej bezpečnosti
2. Špecialista pre vyšetrovanie kybernetických bezpečnostných incidentov
3. Špecialista pre riadenie súladu
4. Špecialista pre riešenie kybernetických bezpečnostných incidentov
5. Architekt kybernetickej bezpečnosti
6. Audítor kybernetickej bezpečnosti
7. Lektor kybernetickej bezpečnosti
8. Špecialista kybernetickej bezpečnosti
9. Výskumník kybernetickej bezpečnosti
10. Špecialista pre riadenie rizík
11. Špecialista pre analýzu digitálnych stôp
12. Tester kybernetickej bezpečnosti

ODHAD POŽIADAVIEK PRACOVNÉHO TRHU

Rola / Kategória subjektu	PZS	Stredné podniky	Verejná správa	OVM	OČTK	Vysoké školy
1.Manažér kybernetickej bezpečnosti	1	1	1	1	1	
2.Špecialista pre vyšetrovanie KBI	1		1	10	200	
3.Špecialista pre riadenie súladu	1		1	1	1	
4.Špecialista pre riešenie KBI	1			10	10	
5.Architekt kybernetickej bezpečnosti	1		1	2		
6.Audítor kybernetickej bezpečnosti				100		
7.Lektor kybernetickej bezpečnosti				50		
8.Špecialista kybernetickej bezpečnosti	2			10		
9.Výskumník kybernetickej bezpečnosti				10		20
10.Špecialista pre riadenie rizík	1		1	1	1	
11.Špecialista pre analýzu digitálnych stôp			2	10	200	
12.Tester kybernetickej bezpečnosti			1	5		
TYPOVÝ POČET RÔL V KB	8	1	8	210	413	20
POČET SUBJEKTOV	1 600	2 688	300	2	2	5
Odhadovaná potreba FTE podľa subjektov	**12 800**	**2 688**	**2 400**	**420**	**826**	**100**

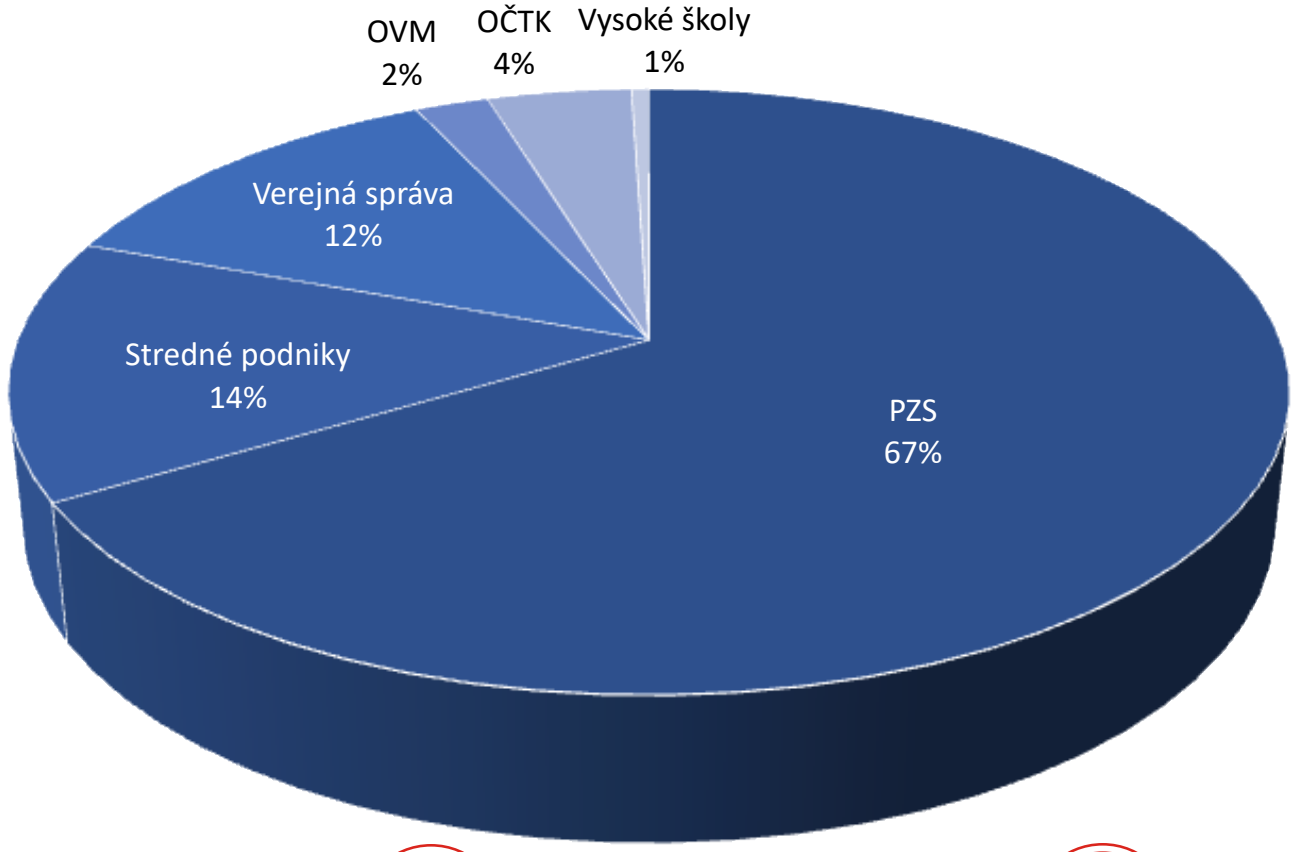
Analyzované subjekty:

- Prevádzkovatelia základných služieb (vrátane veľkých podnikov)
- Stredné podniky
- Verejná správa (ústredné orgány a samospráva)
- Orgány verejnej moci (regulátori: NBÚ / MIRRI)
- Orgány činné v trestnom konaní
- Relevantné vysoké školy

ODHAD POŽIADAVIEK PRACOVNÉHO TRHU

Rola / Kategória subjektu	PZS	Stredné podniky	Verejná správa	OVM	OČTK	Vysoké školy
1.Manažér kybernetickej bezpečnosti	1	1	1	1	1	
2.Špecialista pre vyšetrovanie KBI	1		1	10	200	
3.Špecialista pre riadenie súladu	1		1	1	1	
4.Špecialista pre riešenie KBI	1			10	10	
5.Architekt kybernetickej bezpečnosti	1		1	2		
6.Audítor kybernetickej bezpečnosti				100		
7.Lektor kybernetickej bezpečnosti				50		
8.Špecialista kybernetickej bezpečnosti	2			10		
9.Výskumník kybernetickej bezpečnosti				10		20
10.Špecialista pre riadenie rizík	1		1	1	1	
11.Špecialista pre analýzu digitálnych stôp			2	10	200	
12.Tester kybernetickej bezpečnosti			1	5		
TYPOVÝ POČET RÔL V KB	8	1	8	210	413	20
POČET SUBJEKTOV	1600	2 688	300	2	2	5
Odhadovaná potreba FTE podľa subjektov	**12 800**	**2 688**	**2 400**	**420**	**826**	**100**

19 234 FTE!



Manažér KB (ako zákonná povinnosť) – 1600

Manažér KB (nepovinne) – 2992

Počet zamestnancov KB u PZS – 12 800


HOUSTON
WE HAVE A PROBLEM...

MOŽNÉ RIEŠENIA NEDOSTATKU ODBORNÍKOV NA KB

(IT) ARMÁDA „ANTE PORTAS“ ?

UPSKILLING

Zvyšovanie zručností (upskilling):

- Trend, ktorý uľahčuje ďalšie vzdelávanie poskytovaním školiacich programov a príležitostí na rozvoj, ktoré rozširujú schopnosti zamestnancov a minimalizujú nedostatky v zručnostiach
- Zvyšovanie zručností sa zameriava na **zlepšovanie zručností súčasných profesionálov**
- **Zvyčajné metódy**: školenia a tréningy
- **Cieľ**:
  - napredovanie v práci
  - nájdenie nových príležitostí v rámci organizácie
  - zvýšenie disponibilnej kapacity ľudských zdrojov v konkrétnych profesiách a roliach

„BASED ON TRUE STORY" - 1

Skutočný príbeh (upskilling):

- Rok 2000 – mladý človek nastupuje na pozíciu IT Managera (alebo Správcu siete, alebo Systémového administrátora) do strednej firmy
  - Potrebné znalosti a skúsenosti – support, inštalácie, konfigurácie, IT školenia
- Rok 2004 – firma prechádza na centralizované riadenie IT a projektov
  - Doplnenie znalostí a nové skúsenosti – IT služby, projektové riadenie, time management
  - Potrebné školenia a vzdelávanie – ITIL V2/V3, Prince2, soft-skills
- Rok 2008 – prichádza fúzia 2 firiem, sťahovanie, hodnotenie, spájanie kultúr a formalizácia
  - Doplnenie znalostí a nové skúsenosti – Informačná bezpečnosť, procesy
  - Možné školenia a vzdelávanie – CISA, BPM, TQM, ISO20000, soft-skills

„BASED ON TRUE STORY" - 2

Skutočný príbeh (upskilling):

- Rok 2012 – ďalšia fúzia, prvý security audit, prvé incidenty, centralizácia IT
  - Doplnenie znalostí a nové skúsenosti – riadenie bezpečnosti, riadená dokumentácia, KPI, KRI, due dilligence, compliance
  - Možné školenia a vzdelávanie – CISM, CGEIT, ISO27001, ISO22301
- Rok 2018 – ošiaľ s GDPR a ZoKB, príchod cloudu
  - Doplnenie znalostí a nové skúsenosti – ochrana osobných údajov, riadenie rizík, kybernetická bezpečnosť
  - Možné školenia a vzdelávanie – CRISC, CDPSE, Cobit5, ISO27001 Lead auditor
- Rok 2021 – ZoKB – prvé audity KB, implementácie
  - Doplnenie znalostí a nové skúsenosti – audit, zákonné predpoklady
  - Možné školenia a vzdelávanie – Manažér KB, Audítor KB, ITIL4

KTO JE IDEÁLNYM KANDIDÁTOM NA BEZPEČÁKA?

KTO JE IDEÁLNY „KANDIDÁT“ NA BEZPEČÁKA?

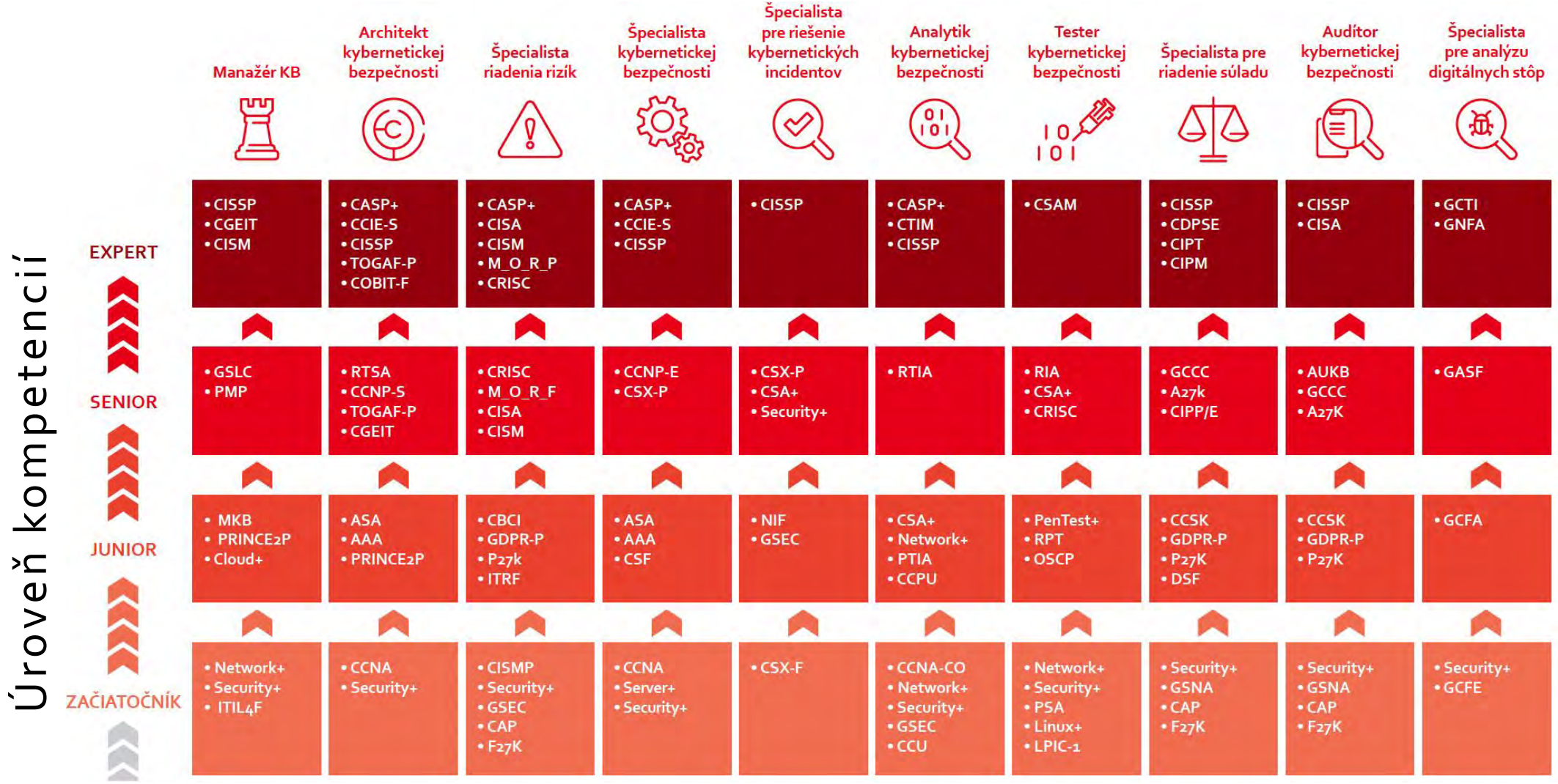
- IT špecialisti
- Administrátori systémov a aplikácií
- Interní audítori
- Dátoví analytici
- Helpdesk špecialisti
- IT/IS manažéri
- Špecialisti ochrany osobných údajov
- Compliance špecialisti
- Manažéri pre riadenie procesov

CERTIFIKÁCIA OSÔB

- Tak ako vysokoškolské vzdelávanie je po absolvovaní štúdia formálne ukončené štátnou skúškou a potvrdené vysokoškolským diplomom, je možné formálne ukončiť aj ďalšie vzdelávanie skúškou a potvrdením získaných vedomostí a zručností certifikáciou
- Certifikácia je zásadne dobrovoľná. Existujú dve kategórie certifikátov:
  - Komerčné certifikáty vydávané v neakreditovanom režime
  - Certifikáty od akreditovaných vzdelávacích inštitúcií
- Druhé typy certifikátov môžu poskytovať výhradne tie vzdelávacie inštitúcie, ktoré prešli atestáciou spôsobilosti vykonávať posudzovanie kompetencií osôb
- To neznamená, že neakreditované komerčné certifikácie sú automaticky nepravé, alebo nedôveryhodné
  - Mnohé, najmä tie, ktoré sú poskytované medzinárodnými organizáciami, patria medzi uznávané v oblasti kybernetickej bezpečnosti (Typicky napríklad certifikáty od ISACA, ISC2, CompTIA, GIAC, SANS a ďalšie)

Spolufinancovaný Európskou úniou

UZNANÉ KOMERČNÉ (NEAKREDITOVANÉ) CERTIFIKÁTY



Spolufinancovaný Európskou úniou

ZÁVER

ZÁVER

Problém spoločnosti:

- Nedostatok disponibilných profesionálov v KB

Cieľ:

- V najkratšom možnom čase získať potrebný počet kvalifikovaného personálu pre obsadenie aspoň povinných zákonných rôl (Manažér kybernetickej bezpečnosti)

Ako?

- Najefektívnejšie formou upskillingu, predovšetkým formou ďalšieho kontinuálneho vzdelávania vo vzdelávacích inštitúciách
- Certifikáciou osôb, ktoré spĺňajú znalostné a kompetenčné predpoklady
- V dlhodobom horizonte formou vysokoškolského vzdelávania

Spolufinancovaný Európskou úniou

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autorov a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za nich nepreberajú žiadnu zodpovednosť.

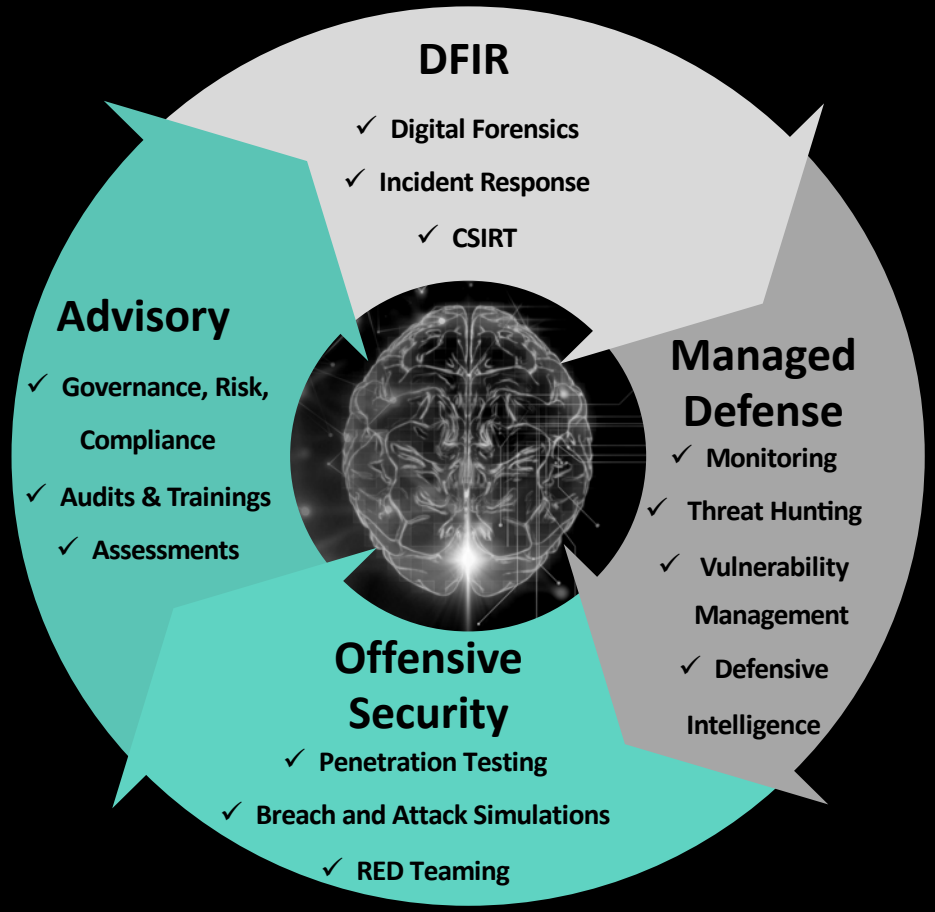
IstroSec

Incident Response & Preparedness with no Compromise!

Roman Cupka, Chief Sales & Strategy Officer
Lukas Hlavicka, Chief Technology Officer & Head of DFIR

EPI Conference
Sept. 30th, 2024
Jasna, SK, EU

IstroSec



Our Experiences

We are an innovative, multidisciplinary team of 30+ world-class subject matter experts. Comprised of highly-skilled ethical hackers, incident responders, and consultants with a decades of experience, our team's expertise covers a wide range of cybersecurity scope.

CCFH CCFR CCFA FORTUNE 500 NATO OTAN

IstroSec

Weeks

Hours

Days

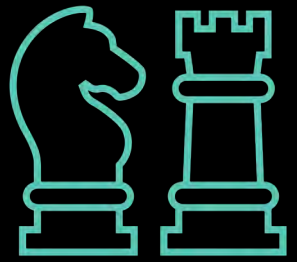
Weeks

Risk

76%

€ ROI of IR Retainer

1st 12hrs of IR



Prepraration

Detection & Analysis

Containment, Eradication & Recovery

Post-Incident Activity

!! Cyber Resilience & Quality of implemented Security Measures testing !!

Continuous

IstroSec

Risk

93.7%

ACPT

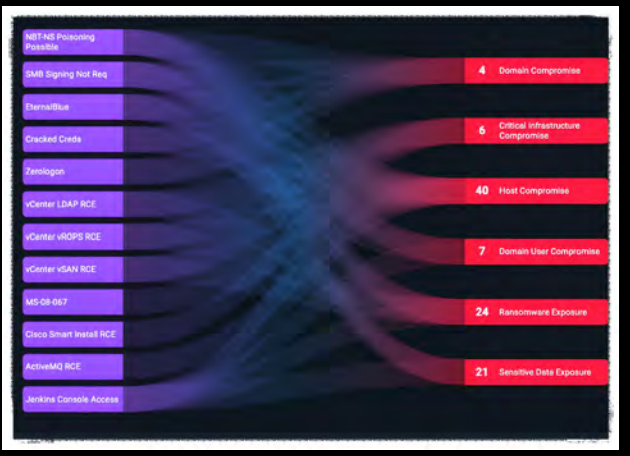
BAS

CART

MPT

CIR

Cyber
Resilience
Continuous
Testing



€ ROI

Single Incident

IstroSec

Thank you for your attention

For more information visit us at:

www.istrosec.com

Ako audítovať odolnosť informačných systémov a sietí

Dušan Peško

Čo je to resilience?

Schopnosť systému alebo siete **zotaviť sa** z porúch **a pokračovať** v poskytovaní služieb bez výrazného narušenia.

Byť pripravený na akýkoľvek typ narušenia, či už plánovaného, alebo neplánovaného tak, aby sa minimalizovalo riziko výpadku prevádzky IT systémov alebo sietí.

Základné prvky odolnosti systémov a sietí

Analýza rizík

Pravidelné hodnotenie rizík a zraniteľností, ktoré môžu ovplyvniť systémy, a prijímanie opatrení na ich minimalizáciu.

Redundancia

Implementácia záložných prvkov, ktoré môžu prevziať funkciu v prípade zlyhania primárnych systémov. To zahŕňa záložné servery, sieťové prvky, dátové úložiská, aj konektivitu.

Zálohovanie

Pravidelné zálohovanie kritických dát a ich ukladanie na bezpečné miesta, ideálne mimo hlavného pracoviska. To zabezpečí, že v prípade výpadku alebo straty dát je možné obnoviť prevádzku.

Monitoring a detekcia

Neustále sledovanie systémov a sietí na identifikáciu potenciálnych problémov a rýchlu reakciu na incidenty. To zahŕňa použitie nástrojov na detekciu narušení a anomálií.

Údržba a aktualizácie

Zabezpečenie, že všetky systémy a softvér sú pravidelne aktualizované a udržiavané, aby sa minimalizovalo riziko zraniteľností a zlyhaní. Vrátane ochrany proti škodlivému kódu.

Vzdelávanie a tréningy

Pravidelné školenia zamestnancov na postupy pri výpadkoch a poruchách, aby vedeli, ako správne reagovať a minimalizovať dopady na prevádzku.

Ako interne overiť, či sú naše systémy dostatočne odolné?

Ak spoločnosť má interných audítorov tak interným auditom, ktorý:

- Určí rozsah (systémov a sietí) ktorý budeme posudzovať.
- Určí riziká (scenáre) ktorým sa chceme vyhnúť
- Určí pracovný program auditu (jednotlivé kroky)
- Získa informácie a vyhodnotí ich
- Navrhne riešenia (opatrenia)

Ak spoločnosť nemá interných audítorov tak, externe (alebo svoj-pomocne).

Postup

1) **Určiť ktoré systémy a siete potrebujeme mať odolné voči výpadkom.**
2) Identifikovať riziká (hrozby) ktoré môžu spôsobiť narušenie
3) Identifikovať základné prístupy/opatrenia pre zabezpečenie odolnosti
4) Preštudovať dostupnú vnútropodnikovú dokumentáciu
5) Overiť ako sú vnútropodnikové požiadavky aplikované v praxi
6) Vyhodnotiť zistenia a navrhnúť opatrenia
7) Sledovať plnenie auditných opatrení

V ideálnym zdrojom informácií je Business Impact Analýza, ale v menších a stredných organizáciách pomôže aj zdravý rozum...

Postup

1) Určiť ktoré systémy a siete potrebujeme mať odolné voči výpadkom.
2) **Identifikovať riziká (hrozby) ktoré môžu spôsobiť narušenie**
3) Identifikovať základné prístupy/opatrenia pre zabezpečenie odolnosti
4) Preštudovať dostupnú vnútropodnikovú dokumentáciu
5) Overiť ako sú vnútropodnikové požiadavky aplikované v praxi
6) Vyhodnotiť zistenia a navrhnúť opatrenia
7) Sledovať plnenie auditných opatrení

Ak je zavedený proces riadenia rizík využiť katalóg hrozieb, ak nie stačí sa zamyslieť aké úmyselné, neúmyselné hrozby a vplyvy prostredia môžu ohroziť prevádzku systémov.

Postup

1) Určiť ktoré systémy a siete potrebujeme mať odolné voči výpadkom.
2) Identifikovať riziká (hrozby) ktoré môžu spôsobiť narušenie
3) **Identifikovať základné prístupy/opatrenia pre zabezpečenie odolnosti**
4) Preštudovať dostupnú vnútropodnikovú dokumentáciu
5) Overiť ako sú vnútropodnikové požiadavky aplikované v praxi
6) Vyhodnotiť zistenia a navrhnúť opatrenia
7) Sledovať plnenie auditných opatrení

Zistiť, či existujú zadokumentované „inštrukcie“ na to, ako zabezpečiť odolnosť systémov (redundancia, monitoring, zálohovanie, plány obnovy..)

Postup

1) Určiť ktoré systémy a siete potrebujeme mať odolné voči výpadkom.
2) Identifikovať riziká (hrozby) ktoré môžu spôsobiť narušenie
3) Identifikovať základné prístupy/opatrenia pre zabezpečenie odolnosti
4) **Preštudovať dostupnú vnútropodnikovú dokumentáciu**
5) Overiť ako sú vnútropodnikové požiadavky aplikované v praxi
6) Vyhodnotiť zistenia a navrhnúť opatrenia
7) Sledovať plnenie auditných opatrení

Zistiť, či sú požiadavky na zabezpečenie odolnosti systémov obsiahnuté v smerniciach, podľa ktorých postupujú zamestnanci pri návrh a prevádzke systémov.

Postup

1) Určiť ktoré systémy a siete potrebujeme mať odolné voči výpadkom.
2) Identifikovať riziká (hrozby) ktoré môžu spôsobiť narušenie
3) Identifikovať základné prístupy/opatrenia pre zabezpečenie odolnosti
4) Preštudovať dostupnú vnútropodnikovú dokumentáciu
5) **Overiť ako sú vnútropodnikové požiadavky aplikované v praxi**
6) Vyhodnotiť zistenia a navrhnúť opatrenia
7) Sledovať plnenie auditných opatrení

Zistiť, či požiadavky uvedené v smerniciach sú aj reálne v praxi dodržiavané, či sú zodpoveným pracovníkom známe, či ich vykonávajú tak ako majú. To sa týka aj dodávateľov.

Postup

1) Určiť ktoré systémy a siete potrebujeme mať odolné voči výpadkom.
2) Identifikovať riziká (hrozby) ktoré môžu spôsobiť narušenie
3) Identifikovať základné prístupy/opatrenia pre zabezpečenie odolnosti
4) Preštudovať dostupnú vnútropodnikovú dokumentáciu
5) Overiť ako sú vnútropodnikové požiadavky aplikované v praxi
6) **Vyhodnotiť zistenia a navrhnúť opatrenia**
7) Sledovať plnenie auditných opatrení

Všetky zistené nedostatky/odchýlky od požiadaviek na zabezpečenie odolnosti kategorizovať podľa závažnosti a navrhnúť opatrenia na ich odstránenie.

Postup

1) Určiť ktoré systémy a siete potrebujeme mať odolné voči výpadkom.
2) Identifikovať riziká (hrozby) ktoré môžu spôsobiť narušenie
3) Identifikovať základné prístupy/opatrenia pre zabezpečenie odolnosti
4) Preštudovať dostupnú vnútropodnikovú dokumentáciu
5) Overiť ako sú vnútropodnikové požiadavky aplikované v praxi
6) Vyhodnotiť zistenia a navrhnúť opatrenia
7) **Sledovať plnenie auditných opatrení**

Vytvoriť časový plán pre realizáciu opatrení a sledovať, či sú realizované včas a podľa odsúhlasených kritérií, tak aby znižovali riziko.

Čím sa interný audit líši od auditu podľa ZoKB?

Zameraný na potreby vašej organizácie

Adresný

Jasné adresovanie zistení/opatrení do vnútra organizácie

Dôraz na sledovanie a plnenie navrhnutých opatrení

Orientovaný do hĺbky

Prináša viac zistení s väčším detailom (nie len súlad/nesúlad)

Ako interný audit prebieha v praxi

I. **Workprogram**

Pracovný program, ktorý, obsahuje jednotlivé kroky z ktorých pozostáva audit

II. **Announcement**

Oznam zainteresovaným osobám a stranám o rozsahu a cieľoch auditu.

III. **Kick-off**

Úvodný meeting pre lepšie zabezpečenie poskytovania súčinnosti

IV. **Fieldwork**

Hlavná fáza auditu, posudzovanie, získavanie informácií, dôkazov, zistení...

V. **Reporting**

Formulácia, kategorizácia zistení a opatrení. Záverečná práva

VI. **Follow-up**

Sledovanie plnenia nápravných opatrení a ich uzatváranie

Ďakujem za pozornosť

dusan.pesko@telekom.sk

Ako na DDoS útoky v roku 2024 s pomocou F5

Ondrej Ciz
F5, Solution Engineer III

Agenda

DDoS Overview

AI-Based DDoS Attack Architecture

AI-Based DDoS Attack Mitigation

Q&A

DDoS attacks are on the rise significantly YoY 2022/2023

DDoS impacts include:

- Loss of revenue
- Loss of productivity (IT Ops / Security)
- Hiring specialized consultants
- Credits to consumers
- Legal and compliance fees
- Public relations

Indirect costs often include:

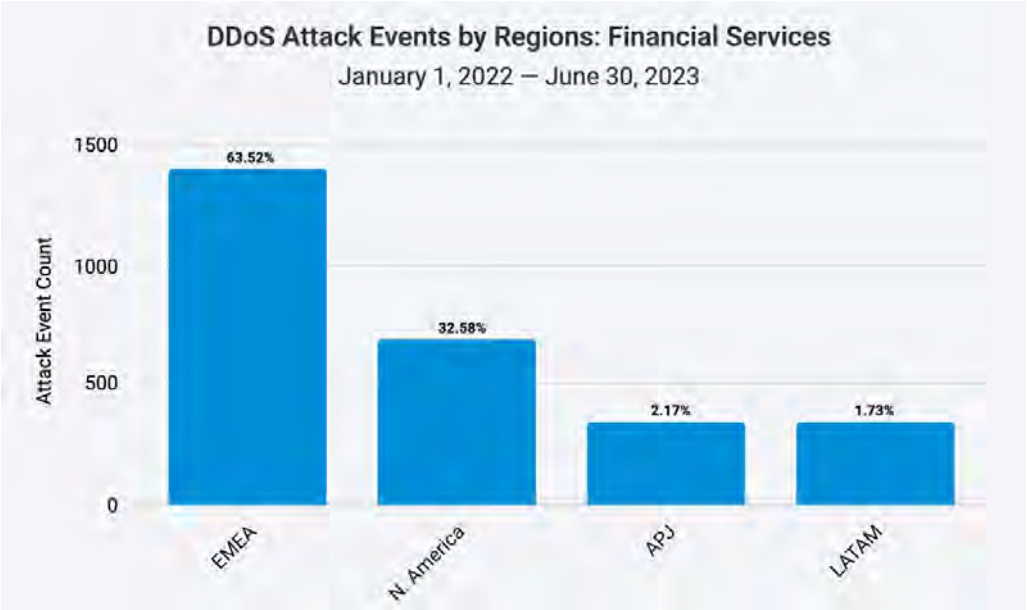
- Damage to the brand
- Theft of vital data
- Loss of valuable customers and
- Opportunity loss

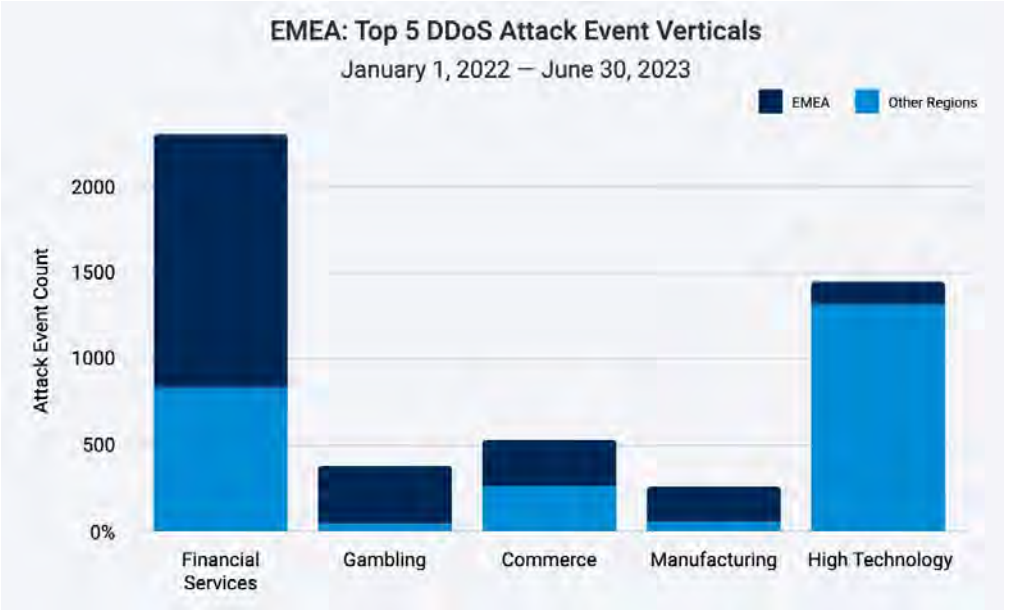
55 seconds between attacks in 2022
14 seconds between attacks in 2023

*https://www.link11.com/en/download/european-cyber-report-2023/

EMEA DDoS Statistics

- EMEA experienced the most DDoS attack events, nearly double the amount in the next top region.
- UK tops the list at 29.2% of DDoS events, followed by Germany at 15.1%
- As of January 2025, the EU financial sectors should be prepared to comply with DORA.
- NIS2 will go into effect on October 17, 2024.
- PCI DSS v4.0 requires organizations to meet new requirements by March 2025.



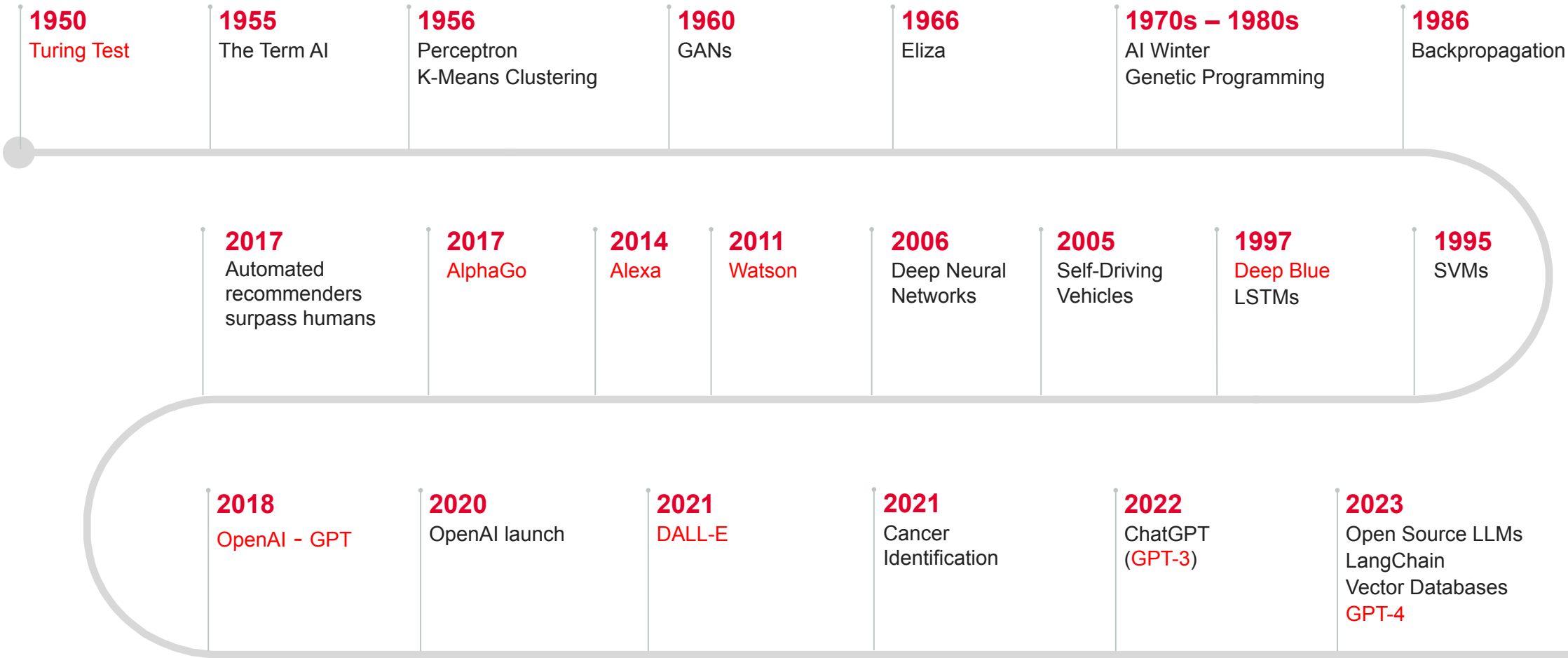


Source: Akamai Attack Trends in Financial Services

AI Evolution and adoption

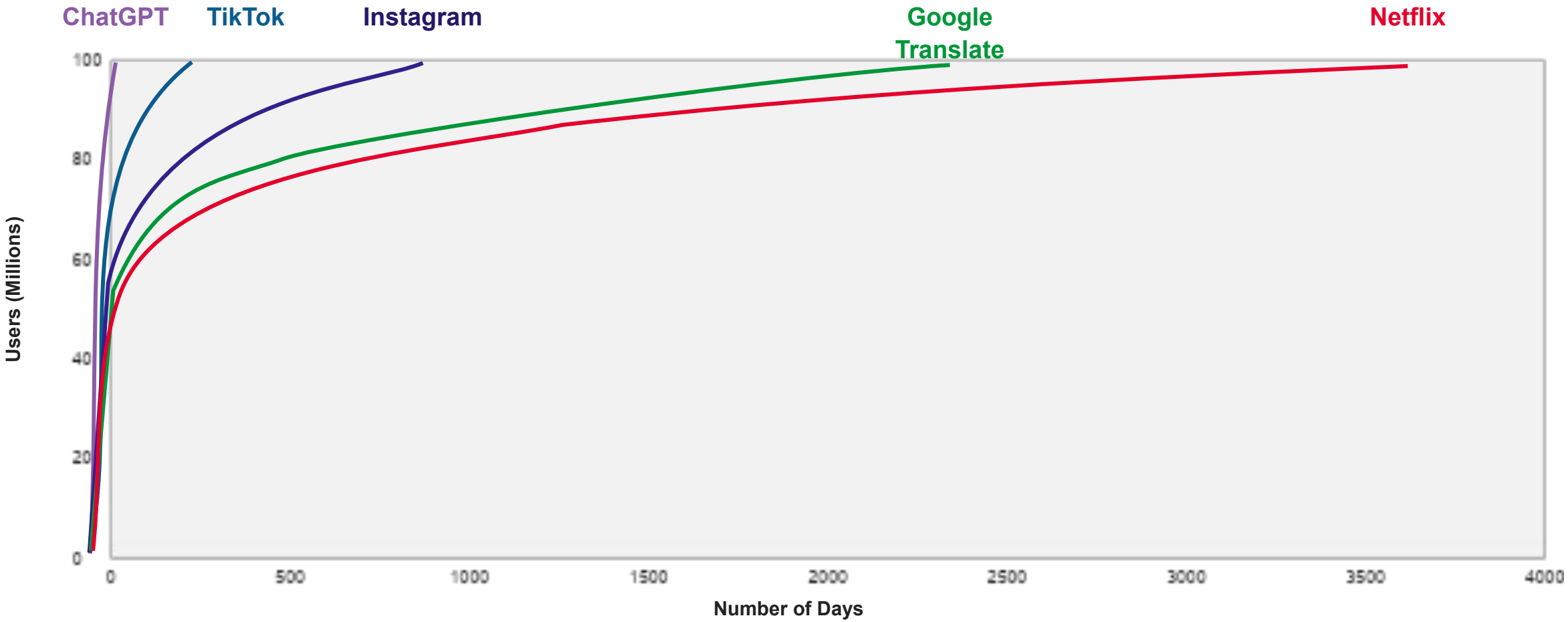
AI is not new

History of AI



The Pace of Adoption of Generative AI Has Been Astounding

Time it took companies to reach 100 million users:



Sources: Global X ETFs with info derived from: BBC News. (2018, Jan 23). Netflix's history: From DVD rentals to streaming success; Cerullo, M. (2023, Feb 1). ChatGPT user base is growing faster than TikTok. CBS News.

For Cyber Security AI Is a Double-Edged Sword

Creates new attack surfaces and new attack capabilities

Moving at alarming speed, no reservations

Enhances cyber security

Exercising caution with deferment to human expertise

F5 has been an AI pioneer for decades – and continues to evolve to meet market needs

2006
Policy Builder to automatically create WAF security policy

2011
Machine Learning (ML) to optimize BIG-IP network stack

2012
ML-based learning mode to improve WAF efficacy

2014
Behavioral anomaly analysis to improve WAF efficacy

2015
ML in iHealth to identity customer BIG-IP issues and misconfigurations

2016
Behavioral DoS to mitigate attacks using dynamic signatures

2019
Stage 2 retrospective analysis to deter bots and automated attacks

2020
Shape acquisition AI powered Anti- Bot & Fraud

2021
Dynamic API Discovery to mitigate risk from rogue APIs

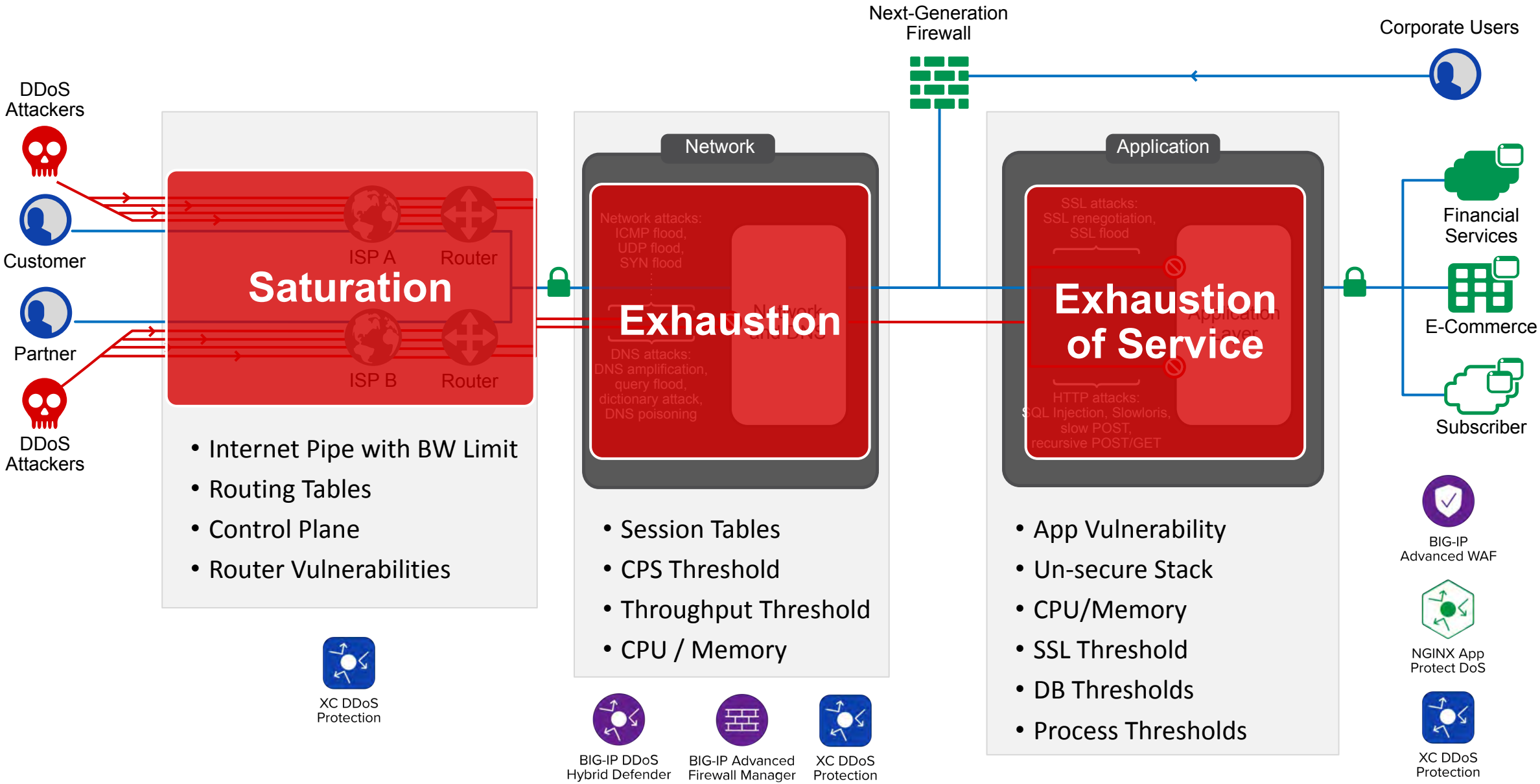
2021
False Positive Suppression to reduce burden on SecOps teams

2022
Malicious User Detection to automatically mitigate bad actors

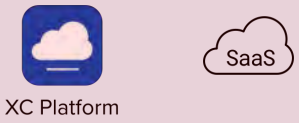
2023
API Endpoints Risk Score to measure risk of discovered APIs

DDoS attack mitigation

F5 DDoS Attack Mitigation



F5 DDoS Hybrid solution

	BIG-IP DDoS Defender **BIG-IP Advanced Firewall Manager** **BIG-IP Advanced WAF**	
	NGINX APP Protect DoS	
	XC DDoS Protection	

F5 XC Distributed Cloud DDoS Mitigation Network

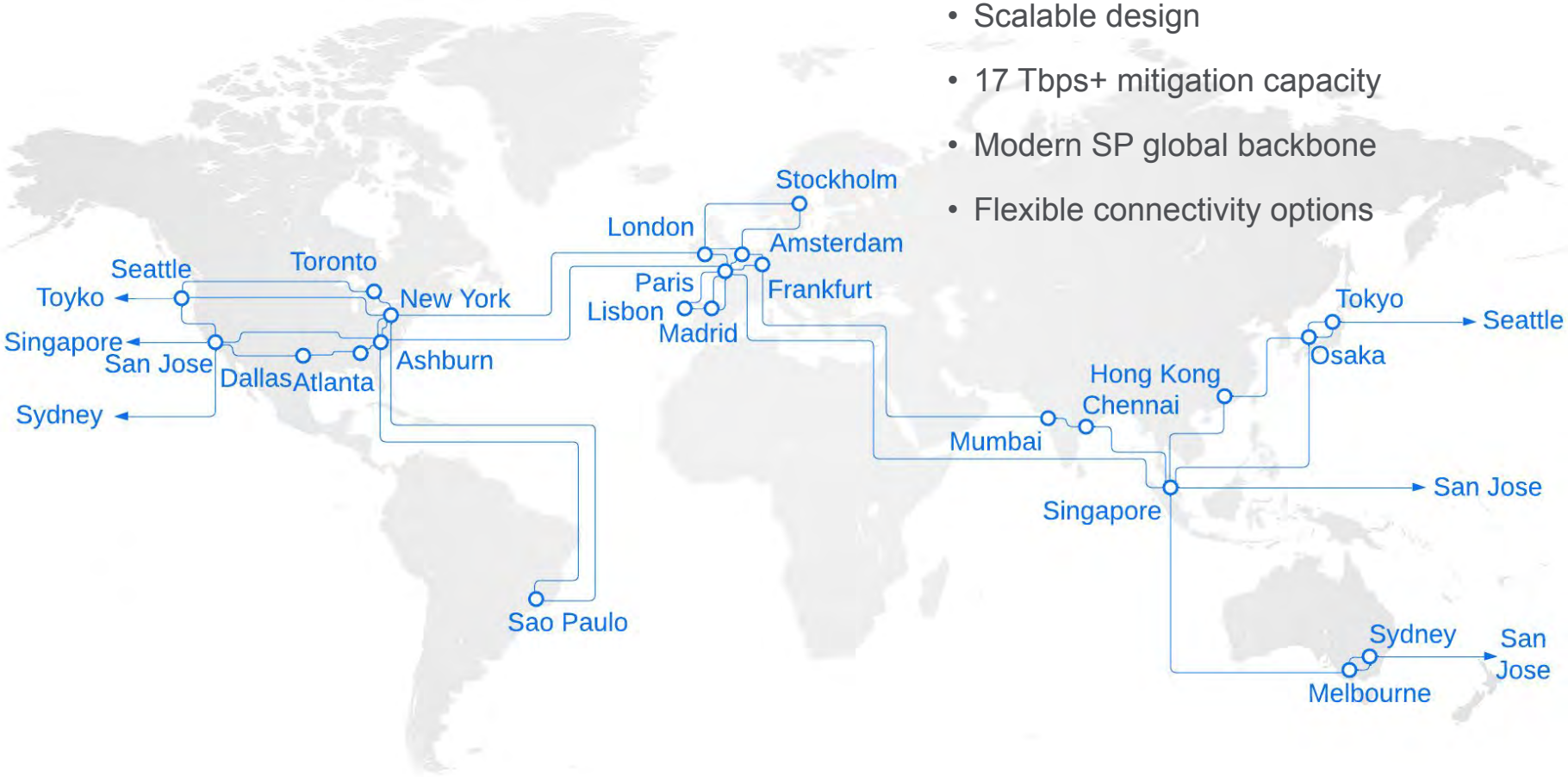
- 26 Points of Presence
- Scalable design
- 17 Tbps+ mitigation capacity
- Modern SP global backbone
- Flexible connectivity options

Responds to DDoS attacks in < 2 minutes on average.*
Top BGP peering

Modern Service Provider Global Backbone

Flexible Service Options including Always Available or Always On deployments

Connect how and where you need with BGP or Proxy-based traffic redirection and direct connections, peering or GRE tunnels for clean traffic return.



Standard DDoS Service offering MSA specifies a 15 Minute Response SLA.

DDoS Mitigation Options

Choose from two DDoS Mitigation configurations

F5 XC ALWAYS AVAILABLE:

Protection available
on-demand

Pre-configured for your systems, runs on standby, and can be initiated when under attack.

- **On-Demand Service Activation by BGP** or Proxy (DNS redirection)
- Actions required by customer and/or SOC to initiate mitigation when under attack
- No limit to the number of mitigation events or service activations
- Can be combined with Router Monitoring to provide accelerated attack detection and notification

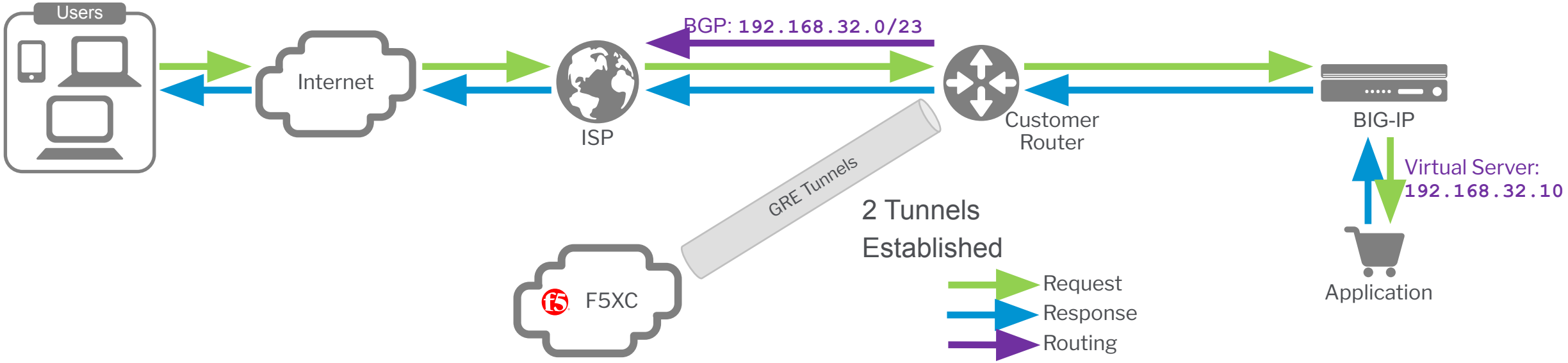
F5 XC ALWAYS ON:

Primary protection
as the first line of defense

Configured to continuously route and process your traffic through the F5 network, allowing only legitimate traffic to reach your apps.

- **Lowest "Time to Mitigate"**
- Maximum visibility for attack trends and detected threats
- Consistent, reliable service delivery metrics and awareness
- Zero activation tasks when under attack
- Ideal for complex, dispersed customer application infrastructure

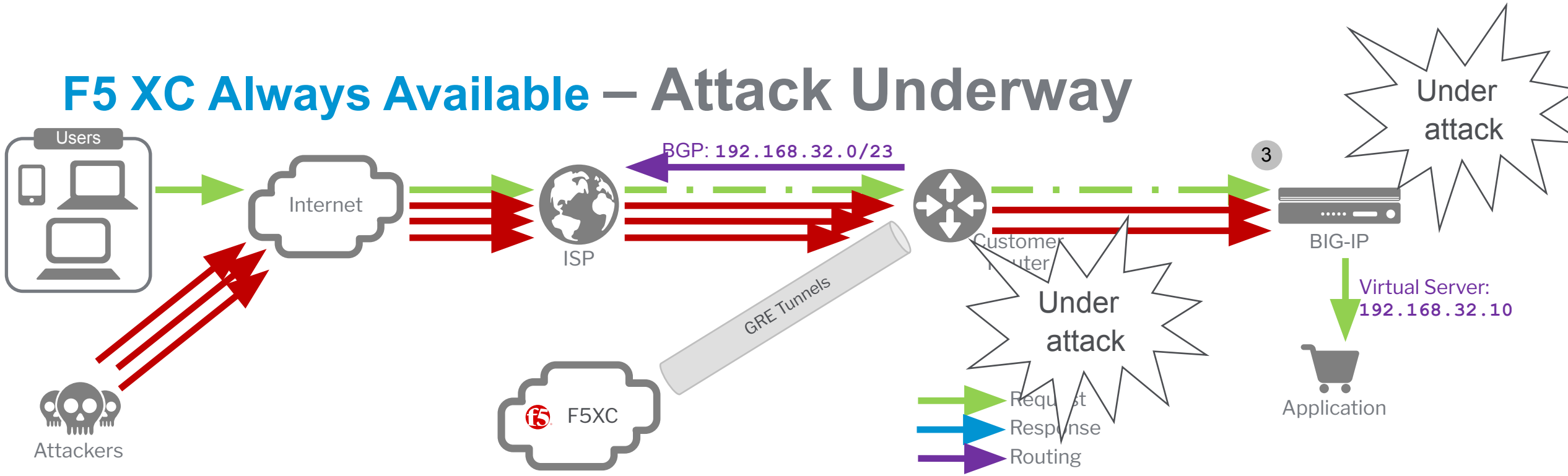
F5 XC Always Available – Basic Configuration



High Level Configuration

1. Customer Router is advertising the public summary route (192.168.32.0/23) to peacetime ISP
2. Router Monitoring service is configured to monitor customer router traffic
3. Customer Router is configured with the necessary GRE Tunnels to F5 Distributed Cloud

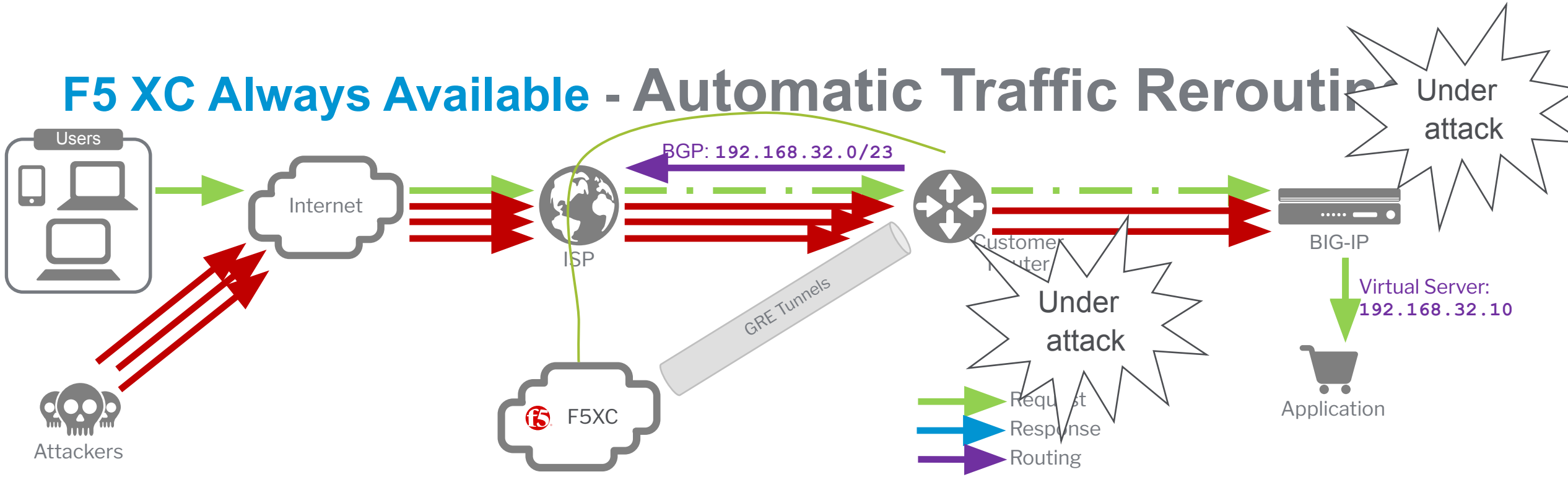
F5 XC Always Available – Attack Underway



Attack Overview

1. Volumetric attack traffic originates from various locations across the internet with a traffic volume designed to overwhelm the customer's connectivity to the Internet.
2. Legitimate traffic bound for the customer's application is congested by the attack traffic at the link between the ISP and the customer.
3. The BIG-IP blocks the attack traffic that made it through. Requests are served to the Application as normal but they are greatly impacted by the upstream congestion.

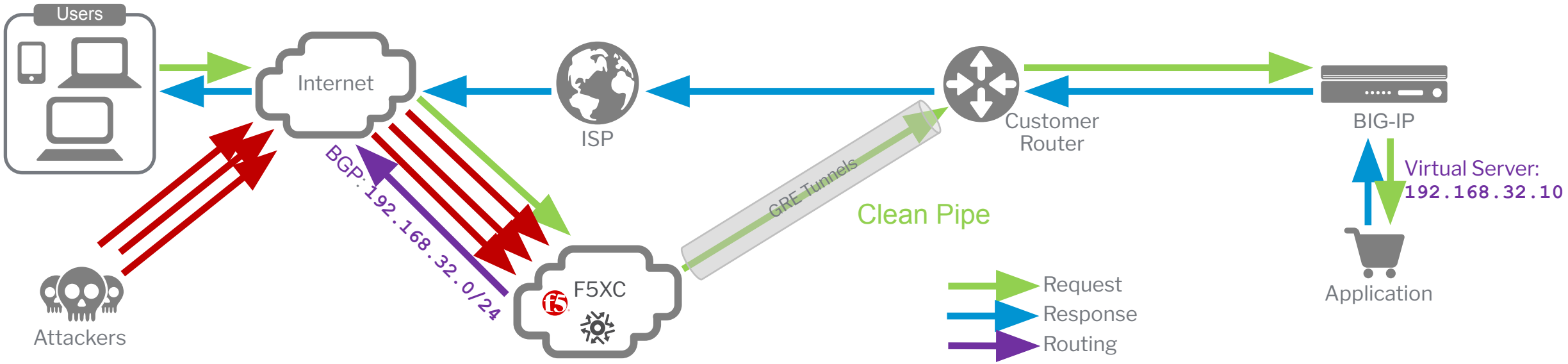
F5 XC Always Available - Automatic Traffic Routin



Traffic Diversion Process

1. Router monitoring service detect bandwidth threshold is exceeded by the attack
2. Alert is generated informing SOC to start advertising the affected prefix (192.168.32.0/24)
3. SOC engineers execute a router change to advertise the prefix (192.168.32.0/24) on behalf of the customer through Real Time Incident Procedures (RTIP)
4. Customer CPE router's summary route advertisement is unchanged (192.168.32.0/23)

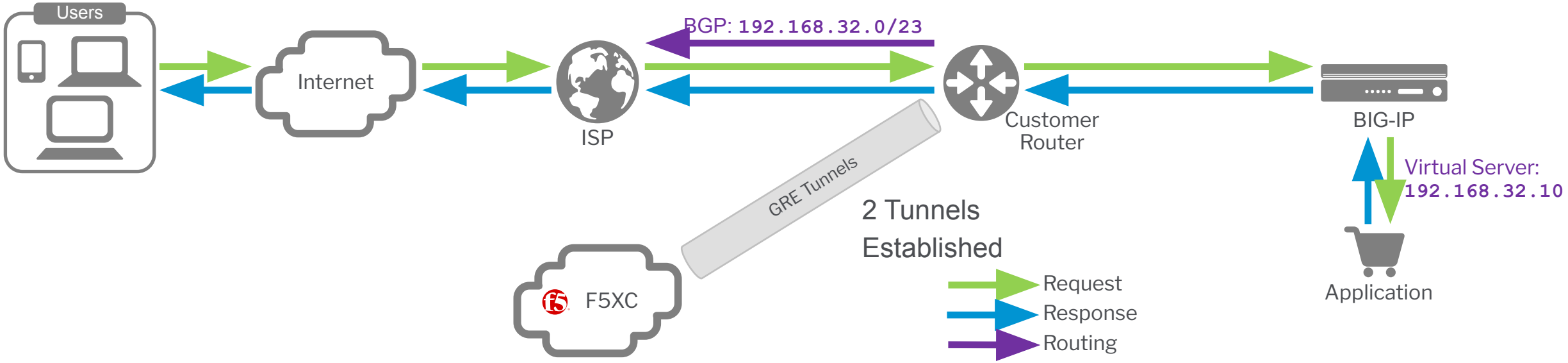
F5 XC Always Available – Attack Mitigation



Attack Mitigation Overview

1. F5 Distributed Cloud is the source for the customer's public subnet
   - F5 Distributed Cloud receives all traffic destined for the customer's public subnet (192.168.32.0/24)
   - F5 Distributed Cloud SOC analysts review the attack and apply the appropriate mitigations
2. F5 Distributed Cloud returns the clean traffic to the customer via GRE tunnel
3. User Response traffic is processed by the application and flows back to the User via the ISP
   - While the customer's public subnet is advertised to Distributed Cloud, the customer still has a default route directed to their ISP for outbound traffic.

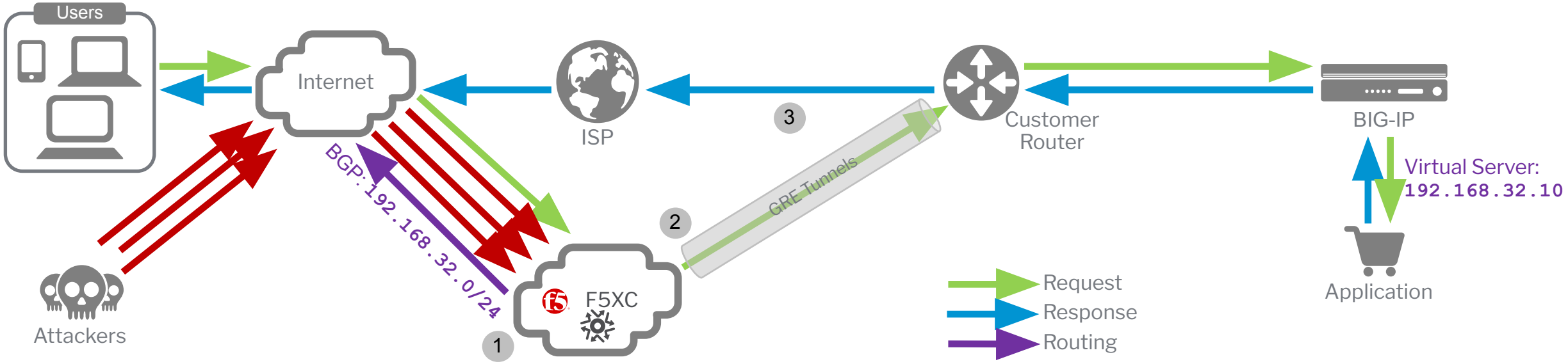
F5 XC Always Available – Attack Mitigated



High Level Configuration

1. Customer Router is advertising the public summary route (192.168.32.0/23) to peacetime ISP
2. Router Monitoring service is configured to monitor customer router traffic
3. Customer Router is configured with the necessary GRE Tunnels to F5 Distributed Cloud

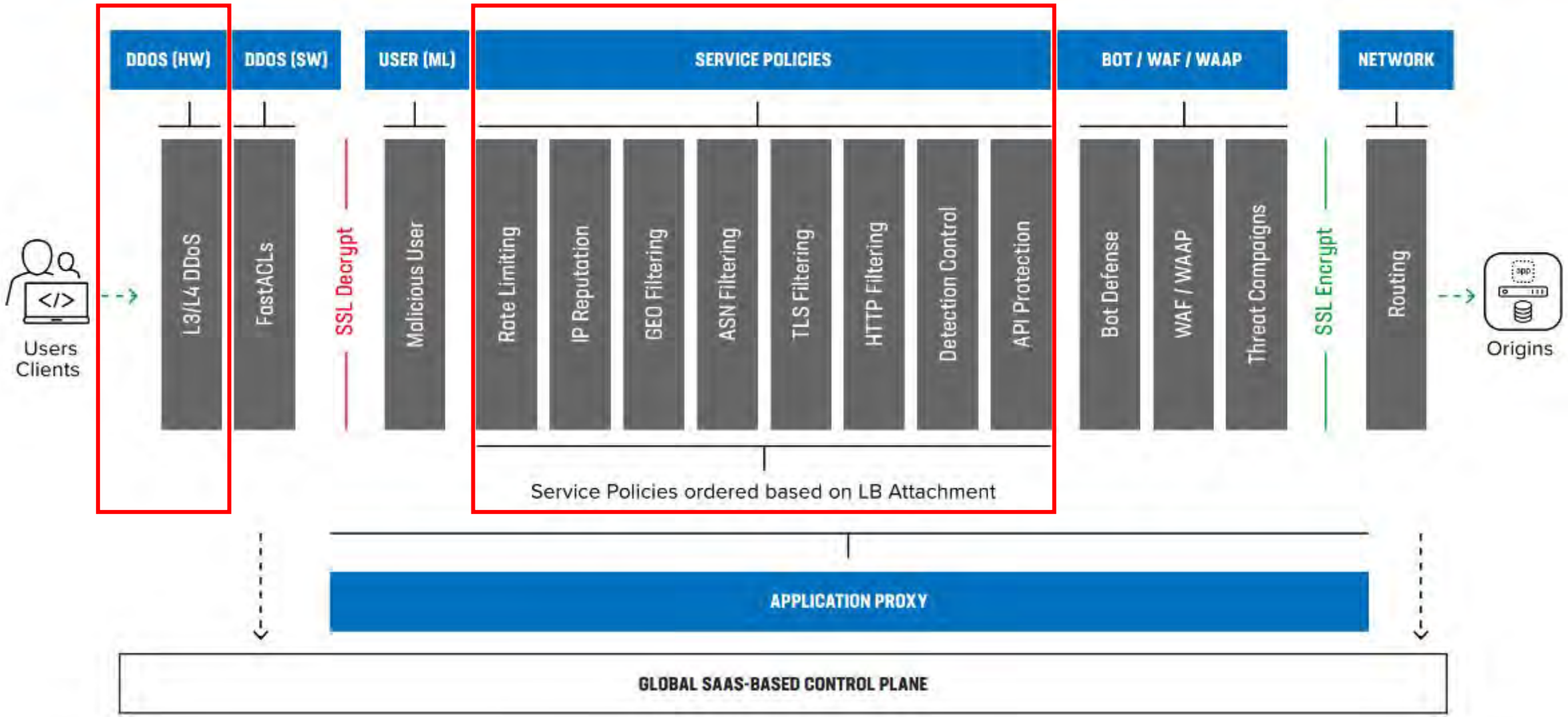
F5 XC Always ON – Attack Mitigated All The Time



Attack Mitigation Overview

1. F5 Distributed Cloud is the source for the customer's public subnet
   - F5 Distributed Cloud receives all traffic destined for the customer's public subnet (192.168.32.0/24)
   - F5 Distributed Cloud SOC analysts review the attack and apply the appropriate mitigations
2. F5 Distributed Cloud returns the clean traffic to the customer via GRE tunnel
3. User Response traffic is processed by the application and flows back to the User via the ISP
   - While the customer's public subnet is advertised to Distributed Cloud, the customer still has a default route directed to their ISP for outbound traffic.

The FLOW of Security [Logical Flow]

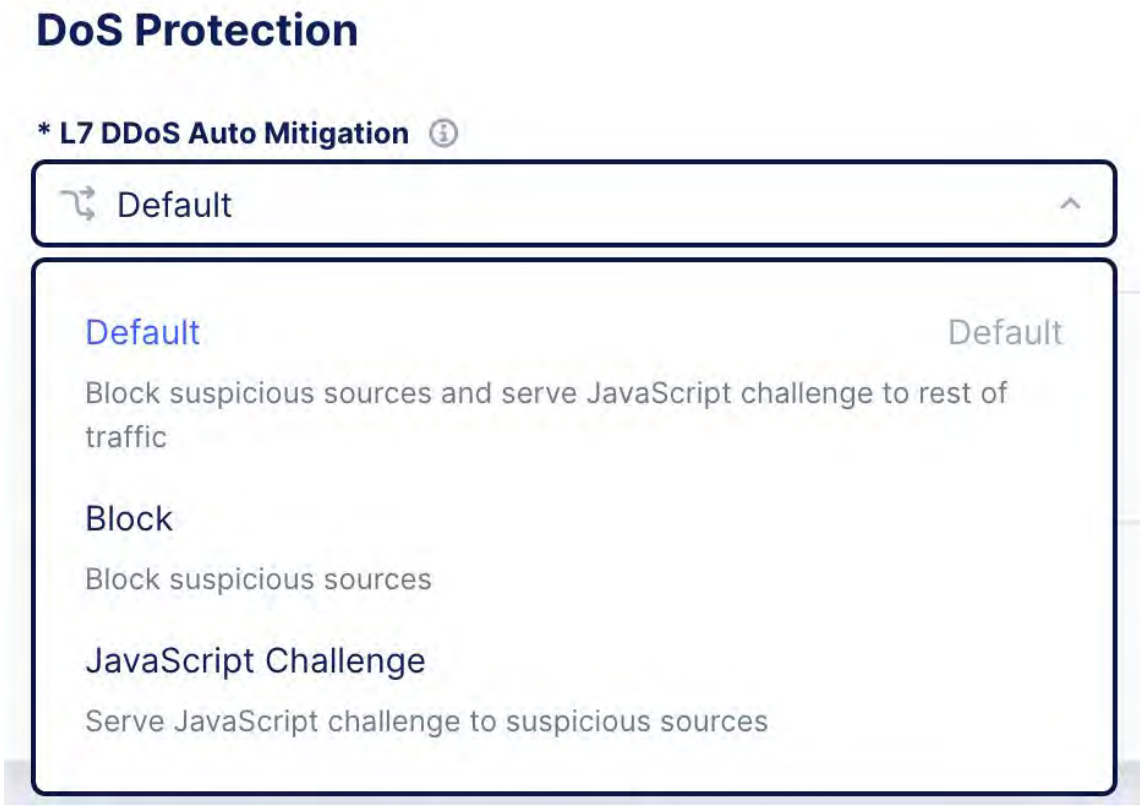


Note: All aspects of flow not represented

Auto DoS Protection

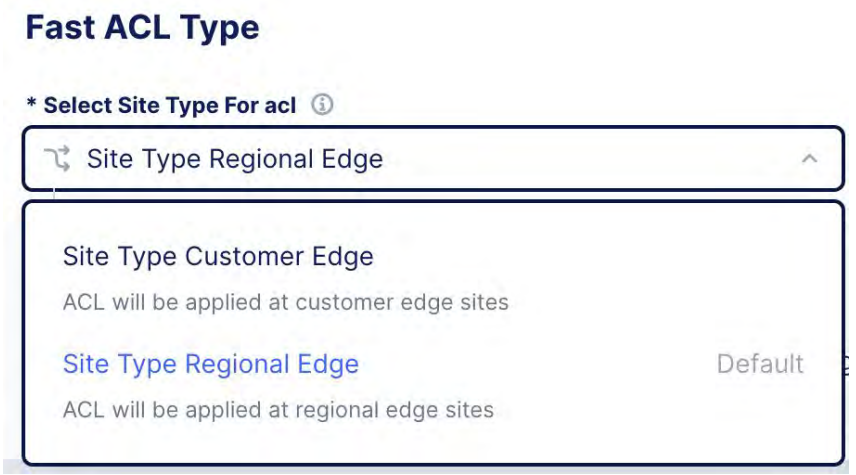
Enabled by default since Jan 2024 release

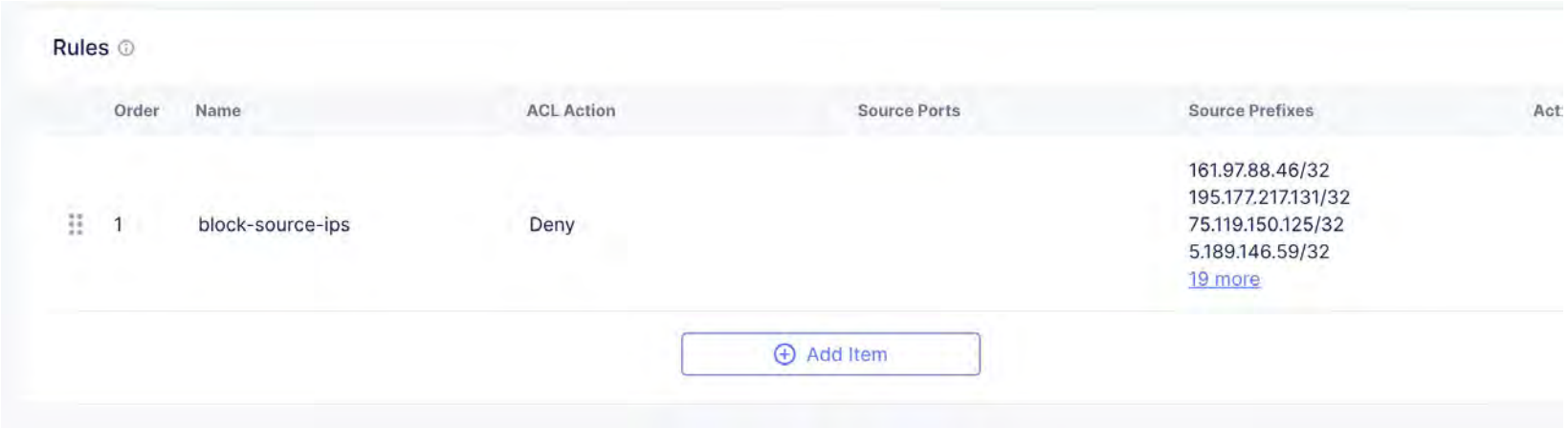
- Included as part of the base package.
- Detects anomalies for request rate, error rate, latency and throughput.
- Dynamically programming
  - Fast ACL to drop attacker at L3 layer
  - L7 ACL in envoy to drop connection based on fingerprint, geo or path
- Auto mitigation rules are created for a duration of 20 minutes, then auto deleted.
- Ability to create trusted client rules to bypass IP addresses from the mitigation.



Fast ACL rules

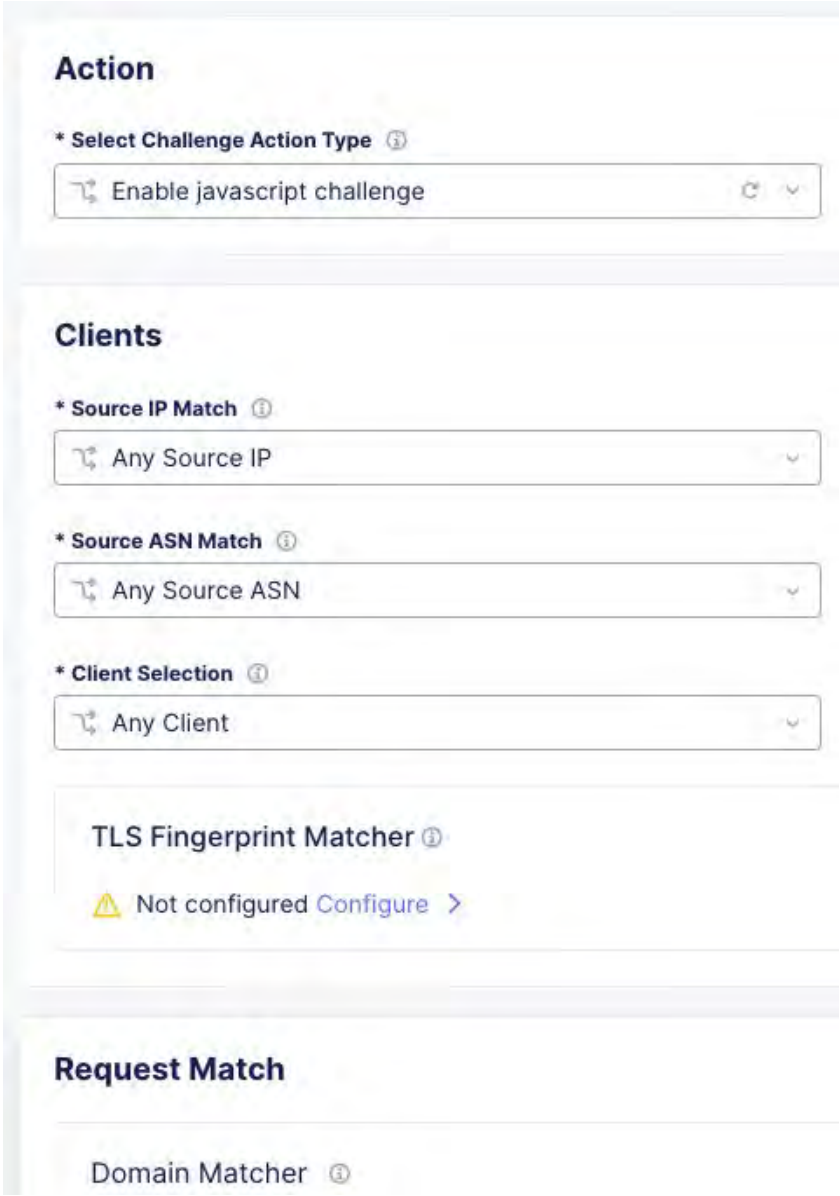
- Specified in terms of five tuple of the packet (dst ip, dst port, src ip, src port, protocol).
- Very efficient, but hard to do manually
- Block source IP attacker on L3
- Auto DoS Mitigation create them automatically





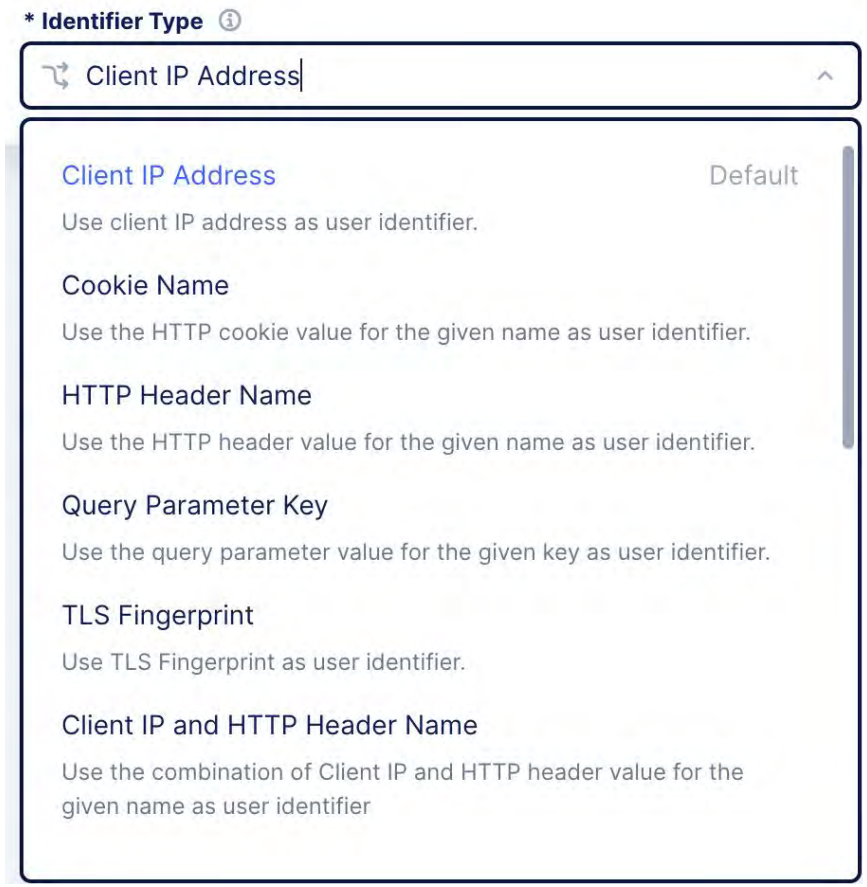
JavaScript Challenge

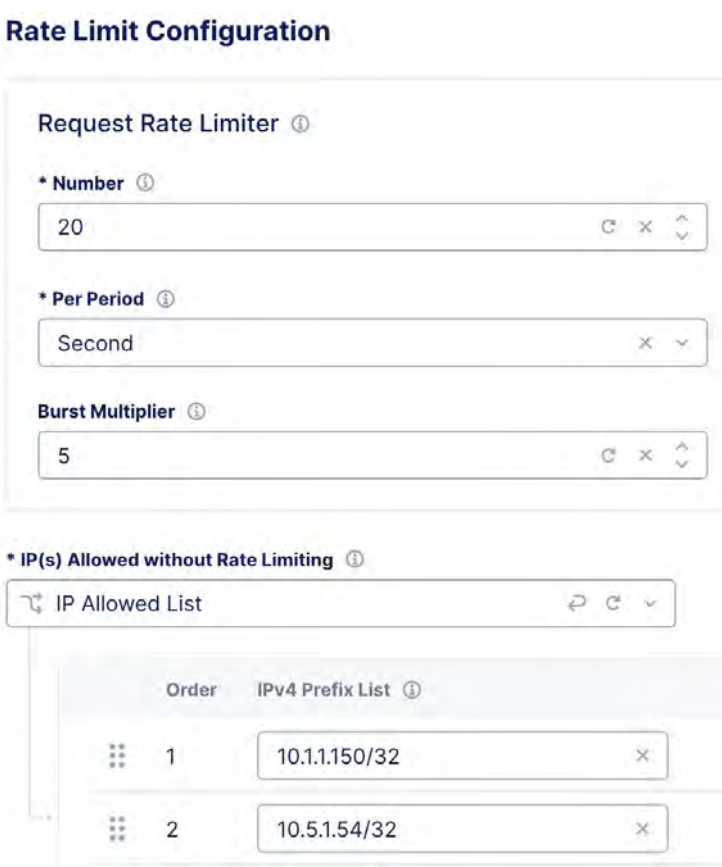
- Validate that the request is coming from a browser that is capable of running JavaScript
- Slows down a potential DoS attacks by forcing the browser to run a complex operation that requires many CPU cycles
- The load balancer tags response header with a cookie to avoid JavaScript challenge for subsequent requests.
- Can be configured via Policy Based Challenge rules for advance traffic matching criteria



Rate Limiting

- Apply on IP Addresses by default, but can be configured for other identification criteria
- Optionally exempt rate limiting for requests from specified IP prefixes
- Trigger 429 codes in the logs
- The rate limit is always evaluated before any configured network security policy sets.

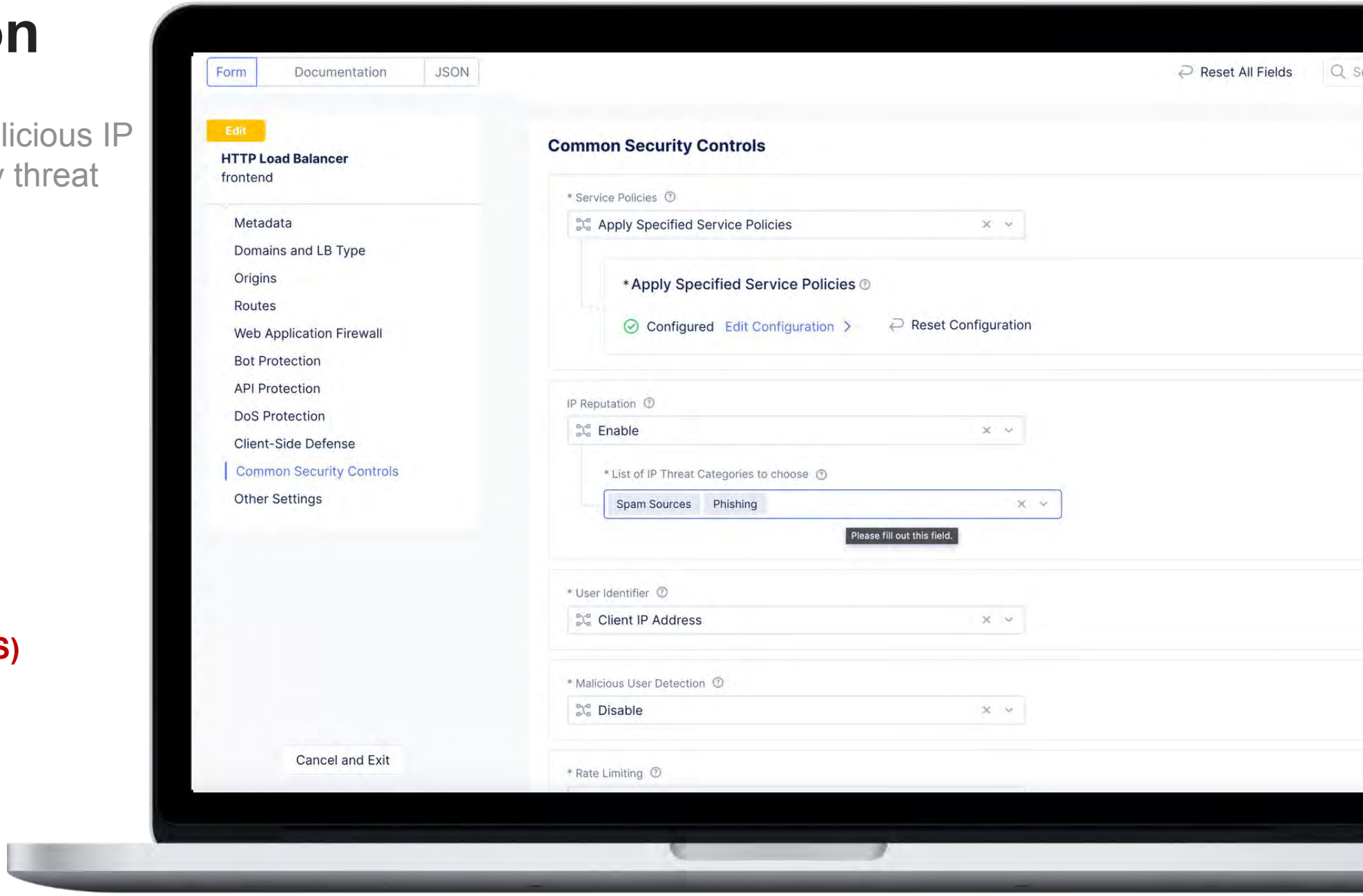




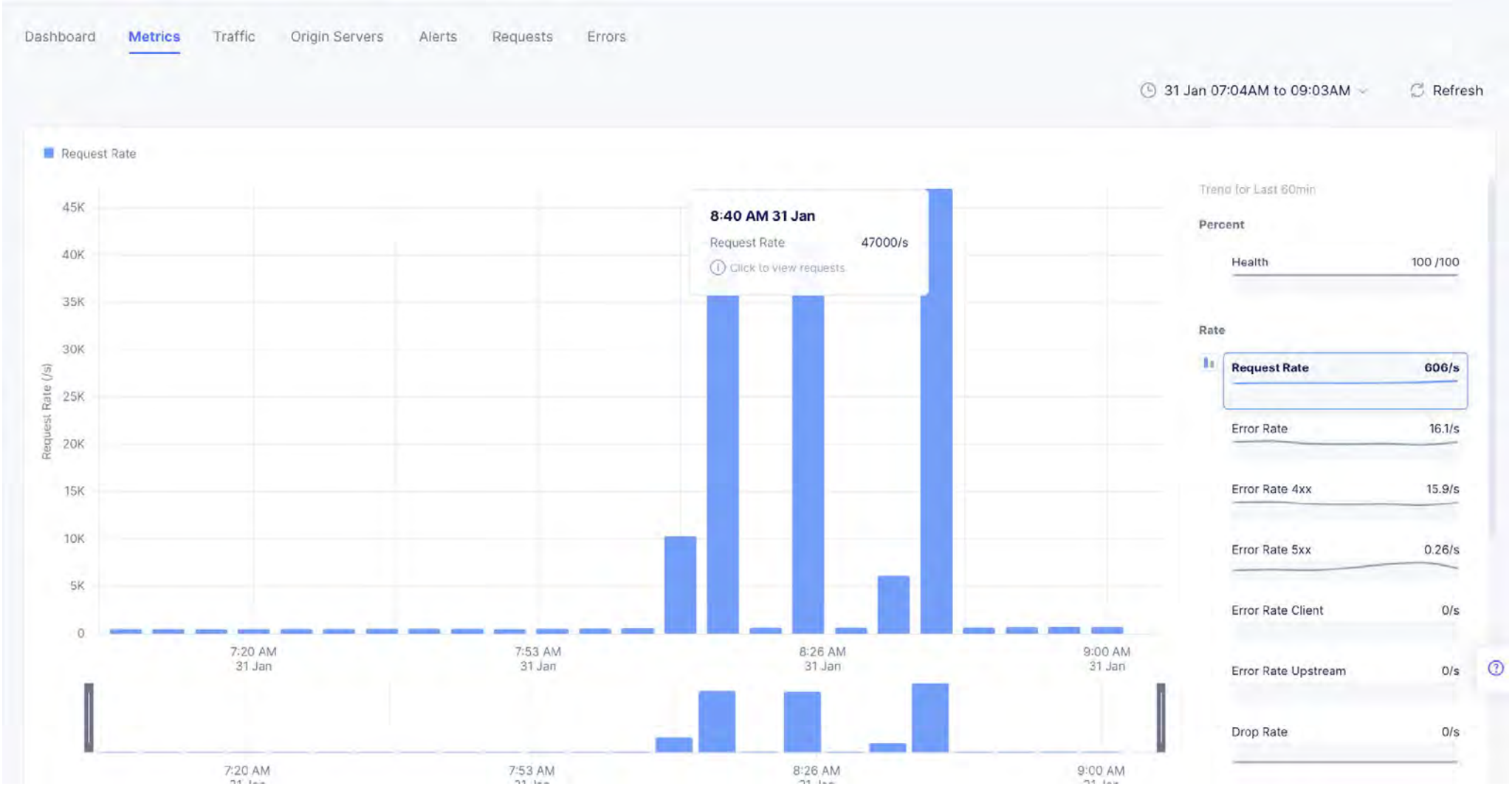
IP Reputation

Database of known malicious IP addresses classified by threat categories

- Spam sources
- Mobile threats
- Windows exploits
- Web attacks
- **Botnets**
- Scanners
- **Denial of Service (DoS)**
- Phishing



Metrics request rate & spikes



Q&A

Praktické skúsenosti z transpozície smernice NIS2 do právneho systému Českej republiky

Kybernetická bezpečnosť 2024

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Martin Švéda
vedoucí projektu přípravy nového zákona o kybernetické bezpečnosti
vedoucí oddělení regulace soukromého sektoru

TLP:GREEN

Východiska obsahu návrhu zákona

Směrnice NIS 2.0

Transpozice směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (směrnice NIS2)

Mechanismus BDŘ

Úkol z usnesení Bezpečnostní rady státu č. 41 ze dne 21. června 2022 k Bezpečnosti dodavatelských řetězců strategické infrastruktury státu, č. j. 28261/2022-UVCR

Zlepšení a zkušenosti

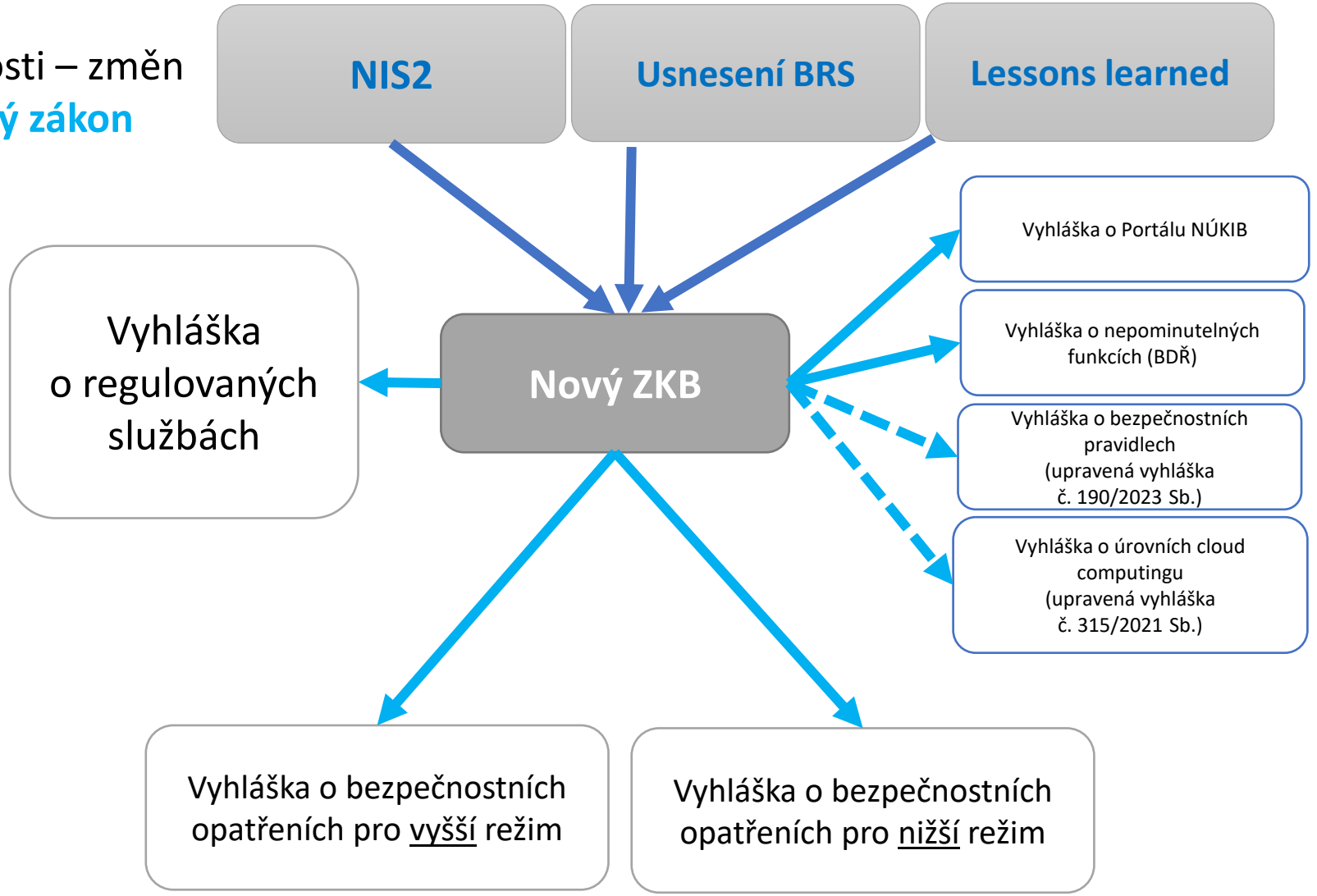
Reflexe poznatků a dosavadních zkušeností, odstranění současných nedostatků, zohlednění podnětů a připomínek a další doplňující úpravy

Nový zákon o kybernetické bezpečnosti (nZKB)

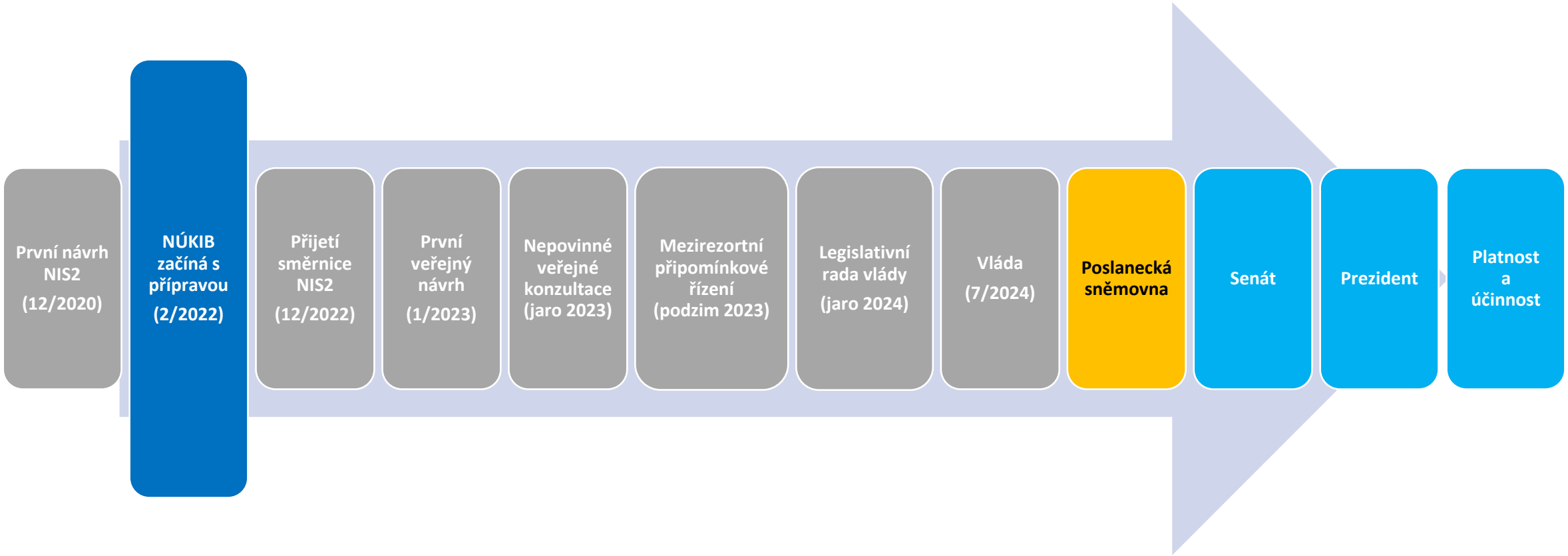
Nový zákon o kybernetické bezpečnosti – změn je tolik, že bylo **potřeba vytvořit nový zákon** (a také k němu doprovodný zákon) a k tomu **7 vyhlášek**

Celý návrh zveřejněn zde:

Sněmovní tisk 759 (psp.cz)



Harmonogram



Práce na úrovni NIS2 Cooperation group (EU)

- **Cooperation group = oficiální konzultační orgán podle NIS2**
- Platforma formující výklad NIS2, harmonizaci regulací, řešení odlišných názorů na výklad NIS2
- Zástupci regulátorů v jednotlivých členských státech, zástupci EK a ENISA
- **13 aktivních Work Streamů: bezpečnostní opatření, hlášení incidentů, dozor a spolupráce při výkonu dozoru,** volby do EP, energetika, **regulace poskytovatelů digitálních služeb,** 5G, zdravotnictví, **bezpečnost dodavatelského řetězce (NÚKIB inicioval a po dobu CZ PRES vedl),** letectví, posuzování rizik, WHOIS, finanční sektor
- **NÚKIB vede pracovní podskupinu zaměřenou na vydefinování regulovaných subjektů v odvětví digitálních služeb**
- Standardní výstupy:
  - non-papery (právně nezávazné), jednotnost postupu všech členských států v určitých otázkách (např. tlak na vyšší bezpečnost dodavatelského řetězce)
  - tlak na EK k vyřešení problematických otázek (výstupem např. 3 Q&A dokumenty k NIS2 nebo úspěšný společný tlak na změnu textu Network Code k přeshraničnímu poskytování elektřiny)
- Specifické výstupy:
  - Podkladové dokumenty pro EK pro účely vytvoření prováděcích předpisů podle NIS2 – k bezpečnostním opatřením a hlášení incidentů

Další nelegislativní činnosti spojené s přípravou nZKB

Dotazy veřejnosti

- v roce 2023 jsme přes centrální e-mail regulace@nukib.gov.cz obdrželi **194 dotazů** ke směrnici NIS2, novému zákonu a jeho dopadům
- doposud za rok 2024 již **více než 280 dotazů** ke směrnici NIS2, novému zákonu a jeho dopadům
- další desítky dotazů telefonicky či na osobní e-maily jednotlivých zaměstnanců

Osvěta

- Desítky národních i mezinárodních konferencí, seminářů
- Bilaterální zahraniční jednání

Informační podpora

- **vznik a údržba webu nis2.nukib.gov.cz**
- vytvořeny tzv. **factsheets** – shrnutí informací k zákonu

Nový ZKB - Komunikace návrhů a zapojení veřejnosti

V srpnu 2022 spuštěn **informační web věnovaný směrnici NIS2 a nové regulaci**

Nová směrnice EU o bezpečnosti sítí a informací (nukib.cz)*

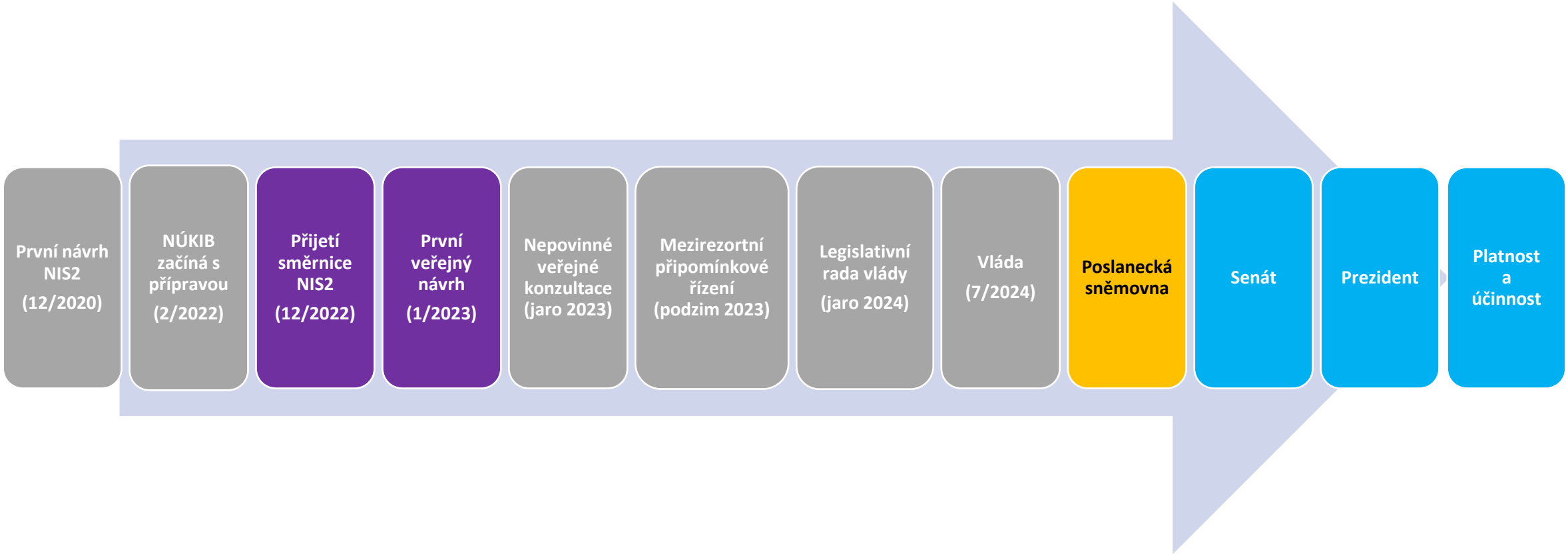
PORTÁL NÚKIB

Portál NÚKIB (gov.cz)

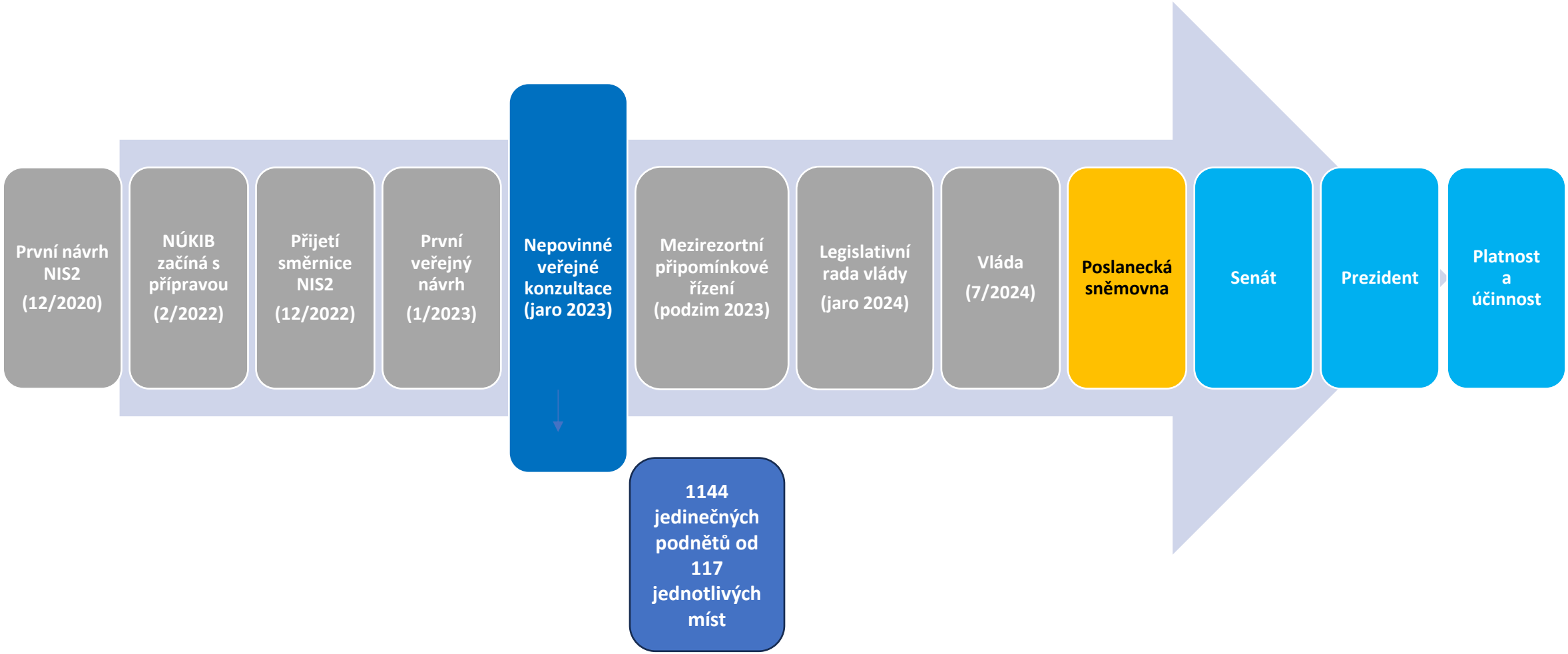
Představení problematiky na desítkách konferencí a bilaterálních jednání se zástupci úřadů a soukromého sektoru. Osloveno a komunikováno **s více než 28 svazy, oborovými sdruženími a komorami**

* vypnut v září 2024, do té doby více než 485 000 přístupů (AJ verze přes 13 000)

Harmonogram

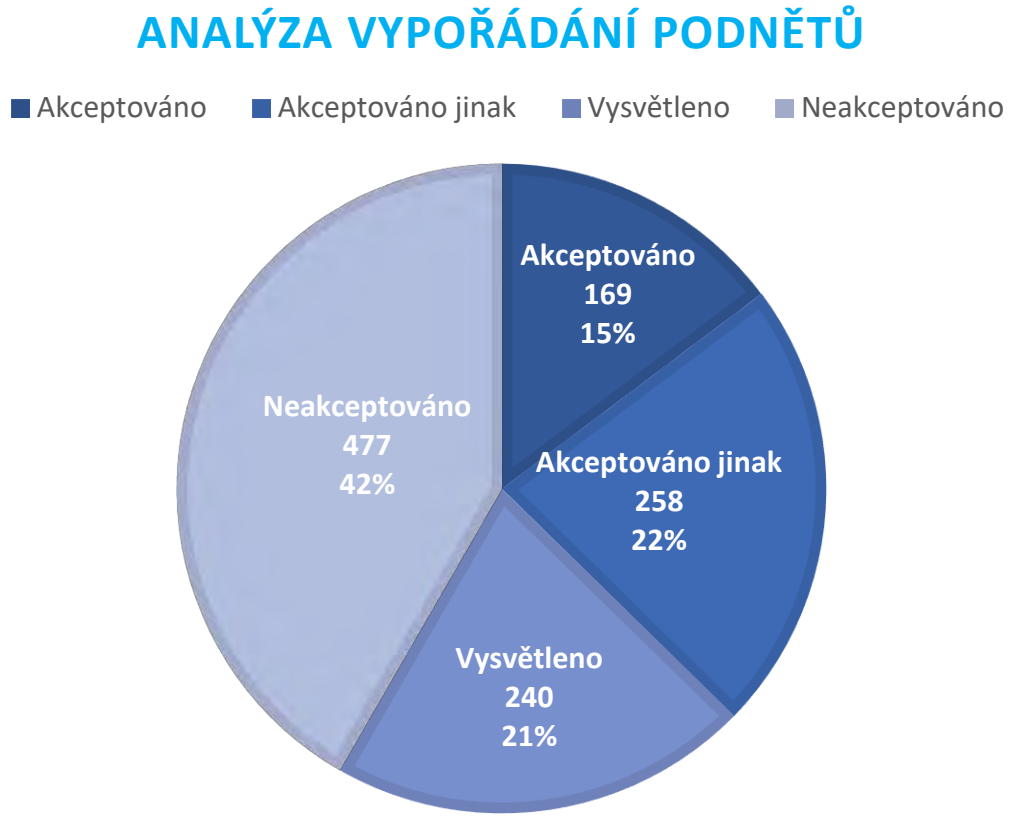


Harmonogram



Nepovinné veřejné konzultace

V rámci veřejných konzultací bylo od 26. ledna 2023 do 12. března 2023 **zasláno 1144 podnětů od 117 jednotlivých míst – odborné veřejnosti, soukromého sektoru i veřejné správy** (toho bylo 27 obsahově stejných)



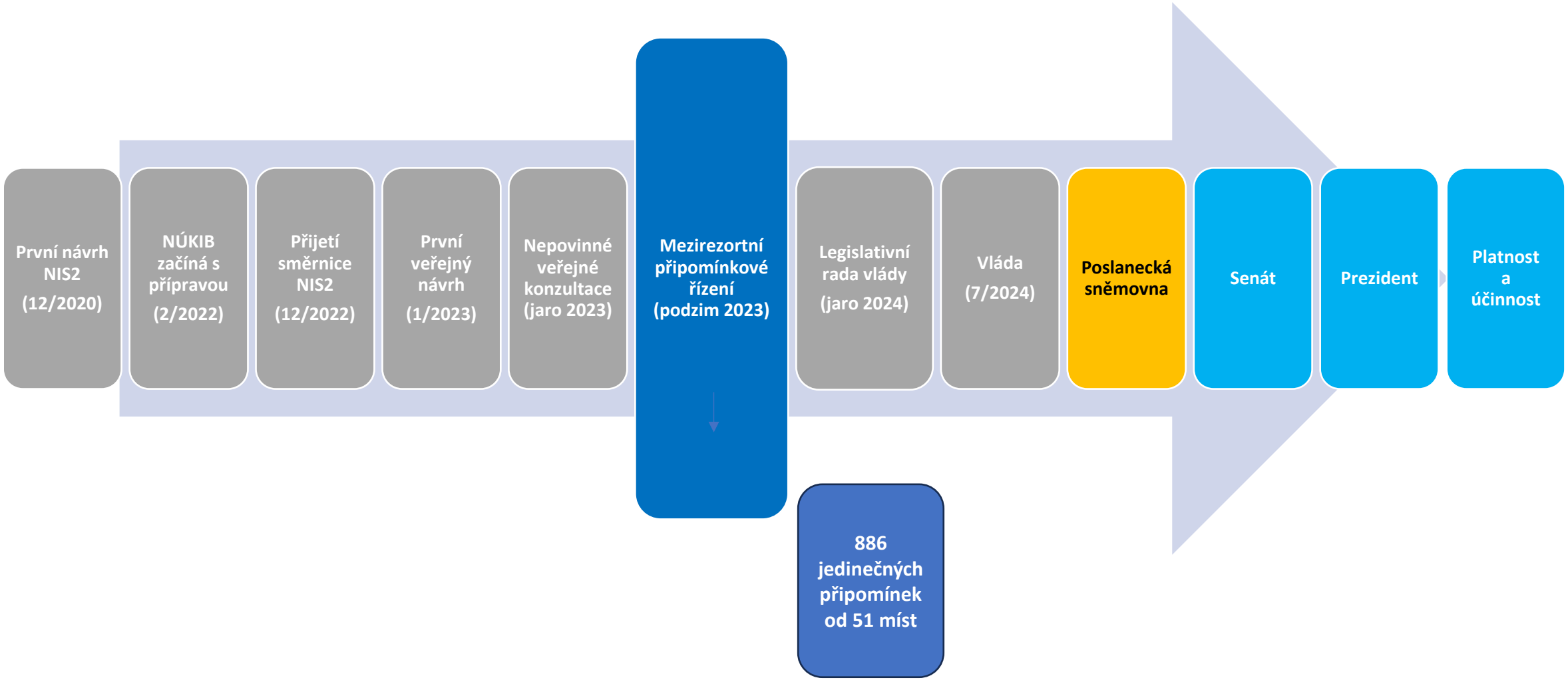
- **Akceptováno** – podnět byl zapracován do návrhu zákona či doprovodných dokumentů (RIA, důvodová zpráva, návrhy vyhlášek);
- **Akceptováno jinak** – podnět byl v návrhu zákona či doprovodných dokumentech zohledněn jinak;
- **Vysvětleno** – podnět byl shledán spíše jako dotaz nebo konstatování, tudíž byl vysvětlen či okomentován;
- **Neakceptováno** – podnět nebylo možné zapracovat do návrhu zákona či doprovodných materiálů.

Veřejné konzultace – hlavní změny

- Formulační změny, zpřehlednění a zpřesnění textu
- Nastavení inspektorů → **zrušení institutu inspektorů** !
- Obsah vyhlášky o bezpečnostních opatřeních pro režim nižších povinností

  → **zeštíhlení, zjednodušení – do MPŘ byla následně předložena zcela přepracovaná verze** !
- Lokalizace informací a dat při zpracování v zahraničí → **zcela přepracováno, nově zajištění dostupnosti strategicky významných služeb z České republiky** !
- Určovací a identifikační kritéria ve vyhlášce → **přesun určovacích kritérií, určení změny režimu do zákona a výčet odvětví pro identifikaci přímo v zákoně**
- Zákon rozdělen na dva → **hlavní zákon a změnový zákon (měnící jiné předpisy)**
- Dílčí změny v mechanismu prověřování bezpečnosti dodavatelského řetězce
- Stav kybernetického nebezpečí → **koncepční změny, provázání s krizovým řízením**

Harmonogram



Meziresortní připomínkové řízení

Oficiální meziresortní připomínkové řízení bylo zahájeno 19. června 2023 a ukončeno 26. července 2023 (téměř 6 týdnů)

- Návrh byl zaslán 85 připomínkovým místům
- Dalších 11 připomínkových míst zaslalo připomínky z vlastní iniciativy

Celkem NÚKIB obdržel 886 připomínek od 51 připomínkových míst

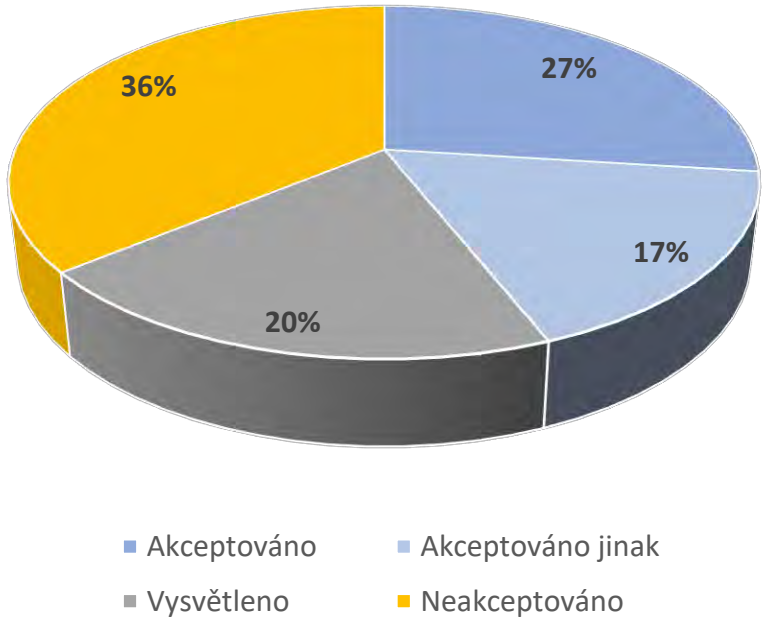
- 518 připomínek bylo zásadních, 368 připomínek bylo doporučujících

Za účelem vypořádání připomínek proběhlo 28 vypořádacích jednání

- Souhlasně bylo vypořádání 589 připomínek (**2/3 z celkového počtu**)

Rozpor přetrvává u 4 připomínkových míst

- Český telekomunikační úřad
- Svaz měst a obcí
- Asociace krajů
- Svaz průmyslu a dopravy



Nesouhlas s vypořádáním připomínek, který není předmětem rozporu přetrvává u některých dalších připomínkových míst – např. u Hospodářské komory

Dílčí vyhodnocení připomínek v MPŘ

Definice

- připomínkovány některé definice (např. aktiva, významný dopad/hrozba/incident), požadováno doplnění dalších definic

Kritéria regulované služby

- nastavení vztahu zákon – vyhláška dostatečně nevymezuje některé instituty a nechává to na vyhláškách
- požadavky na neregulování některých služeb – např. obcí III. typu nebo vědeckých institucí

Rozsah a evidence aktiv

- nesouhlas s požadavkem evidovat všechna primární aktiva

Kontaktní údaje a incidenty

- požadavek na to, aby vyšší režim nehlásil všechny incidenty, požadavek na prodloužení lhůty pro hlášení z 24 na 72 hodin

(Proti)opatření

- dílčí připomínky k reaktivnímu protiopatření nebo např. požadavek, aby institut varování nebyl

Přestupky a další sankce

- vynětí územních samosprávných celků ze sankcí, snížení pokut státní správě

Zabezpečení ISVS podle vyhlášky o nižším režimu

Stav kybernetického nebezpečí

Dílčí vyhodnocení připomínek v MPŘ

Mechanismus prověřování bezpečnosti dodavatelského řetězce

- požadavky na zrušení institutu
- nedostatečné vyhodnocení nákladů
- nedostatečně projednáno
- kompenzace – stát by měl platit náhrady
- přechodné lhůty – mají být delší
- zapojení sektorových regulátorů
- měla by to dělat vláda
- zúžení rozsahu dotčených aktiv – jen core, transportní a přístupové vrstvy ne
- pevné stanovení hloubky dodavatelského řetězce, který se bude prověřovat

Zajištění dostupnost strategicky významné služby

- nejasnosti ohledně toho kterých služeb se to týká
- obavy ohledně využívání cloudu

Projednávání mechanismu – časová osa

Červen 2022 – Listopad 2022

- Konference výboru pro bezpečnost *"Bezpečnost dodavatelského řetězce v sítích elektronických komunikací a další strategické infrastruktuře ČR"*
- Seminář *„Výstavba telekomunikačních sítí"*
- AKI summit 2022
- Konference CEVRO Institut

Prosinec 2022

- Seminář NÚKIB k bezpečnosti dodavatelského řetězce

Duben 2023

- Ministerstvo financí, ČAEK

Květen 2023

- UK Embassy – za účasti zástupců soukromého sektoru
- Svaz průmyslu a dopravy, Hospodářská komora ČR

Červen 2023

- NSS – jednání s předsedou Nejvyššího správního soudu

V průběhu roku 2023 řadě jednání na úrovni Hospodářské komory České republiky, Svazu průmyslu a dopravy a dalších.

Shrnutí rozporů z MPŘ

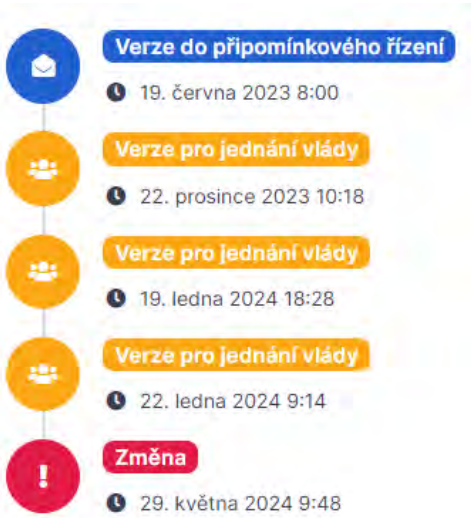
Ministerstvo financí

Rozpor přetrvává u jedné připomínky – omezení mechanismu BDŘ na nedostupnost a pouze na kritickou část

Ministerstvo dopravy

Rozpor přetrvává u jedné připomínky – obecný nesouhlas s BDŘ, požadavek oblast dále projednávat

Ministerstva své připomínky po jednání na Úřadu vlády stáhla – mohou být předmětem jednání vlády o návrhu zákona.



Český telekomunikační úřad

- **Omezení rozsahu BDŘ** pouze na kritická aktiva
- **BDŘ by se nemělo vztahovat na přístupovou část sítí** (RAN)

Svaz měst a obcí

Rozpory uplatněny u všech připomínek, tedy i u těch, kde bylo připomínkám vyhověno a byly akceptovány – zejména jde o regulaci obcí s rozšířenou působností – **požadavek na vypuštění obcí nebo vynětí z přestupkové odpovědnosti,** určovací kritéria ve vyhlášce a nikoliv v zákoně nebo zpracování dopadové analýzy RIA

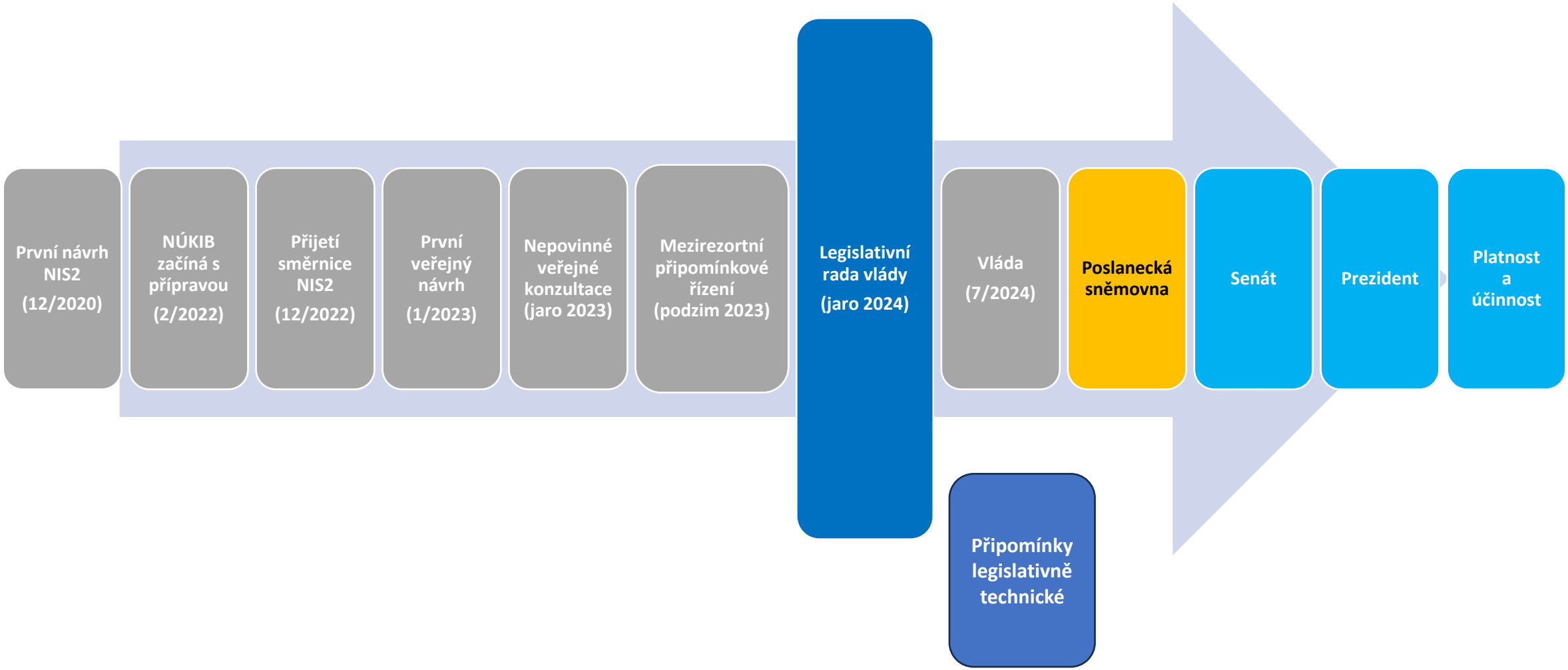
Asociace krajů

Rozpory uplatněny u všech připomínek, tedy i u těch kde bylo připomínkám vyhověno a byly akceptovány – zejména jde o **mechanismus prověřování bezpečnosti dodavatelského řetězce** (např. vyloučení RAN), **zpracování dopadové analýzy RIA** nebo určovací kritéria ve vyhlášce a nikoliv v zákoně

Svaz průmyslu a dopravy

- **Zrušení vyhlášky o nepominutelných funkcích a omezení BDŘ** jen na kritická aktiva
- **Zapojení regulátora a vlády do BDŘ**
- Určovací kritéria by měla být dána nařízení vlády a nikoli vyhláškou

Harmonogram



Nový ZKB - Legislativní rada vlády

Zákon byl ve 4 pracovních komisích

- Pracovní komise pro správní právo
- Pracovní komise pro soukromé právo
- Pracovní komise RIA
- Pracovní komise pro evropské právo

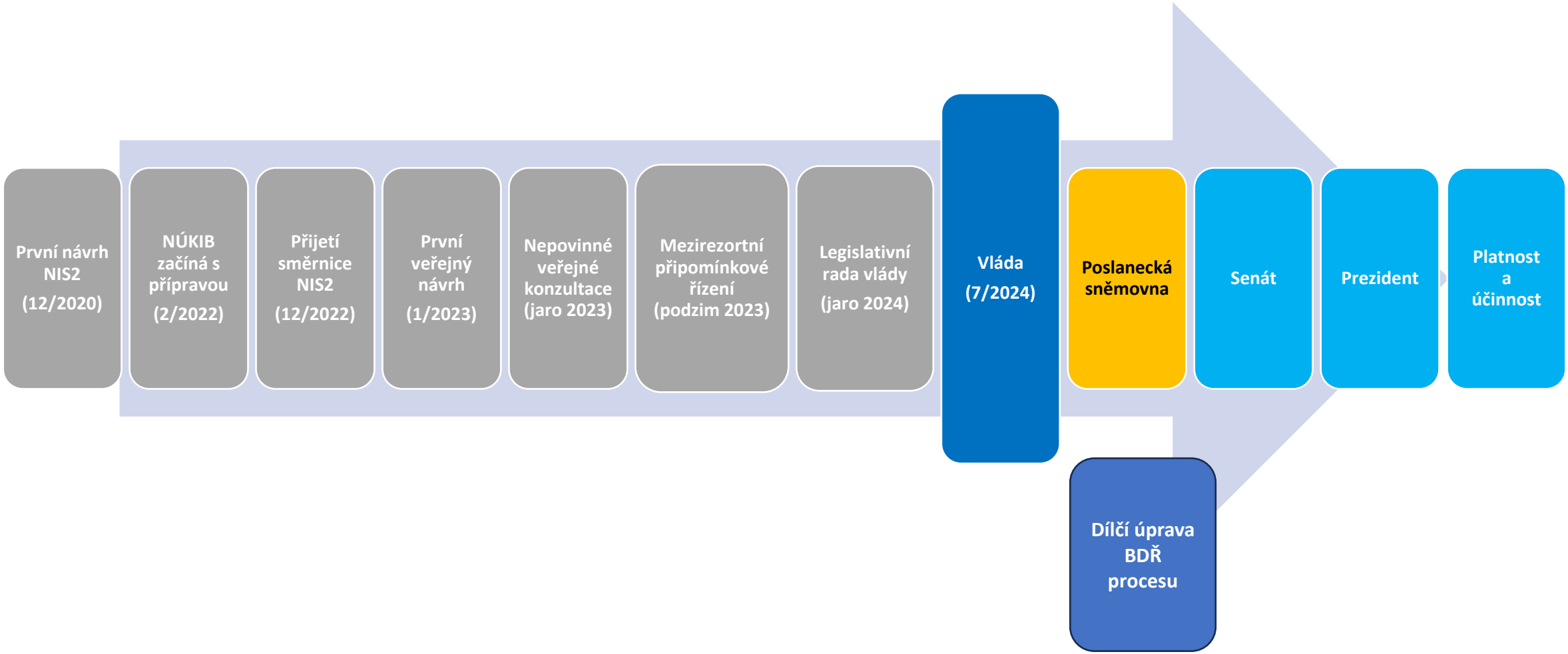
„Velká“ LRV proběhla 4. dubna 2024

- Definice
- Široká zmocňovací ustanovení
- Procesní otázky – vyloučení rozkladu
- Legislativně technické připomínky, složitý jazyk
- Sankce – zejména zákaz činnosti statutárního zástupce
- Návrh není v rozporu s ústavou

Projednávání bylo přerušeno – následně doporučující stanovisko předsedy LRV ze dne 13. června 2024.

Reakce na komentář J. Grunda na serveru Info.cz: „Vláda obchází vlastní pravidla, stejně jako při lex ČEZ“ | Vláda ČR (gov.cz)

Harmonogram



Jednání vlády – provedena změna

Na základě rozhodnutí vlády došlo k úpravě v procesu vydávání opatření obecné povahy (OOP) sloužícího k realizaci mechanismu prověřování bezpečnosti dodavatelského řetězce.

Navrhovaná verze:

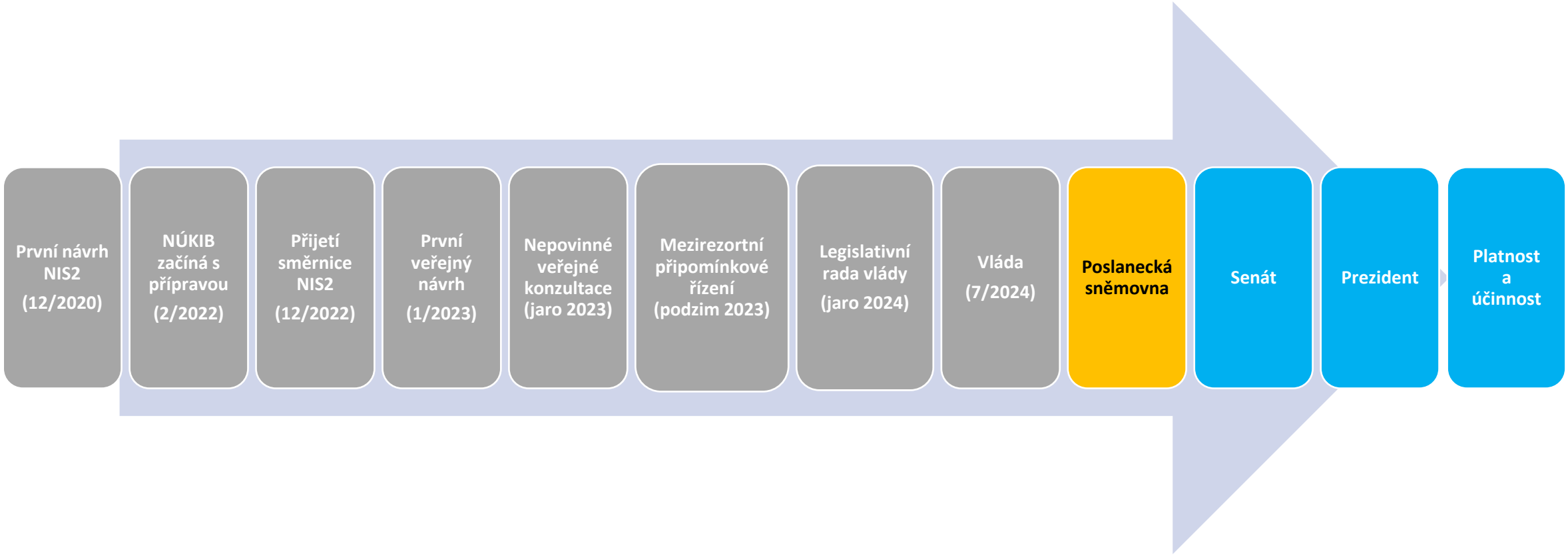
- Ministerstvo vnitra, Ministerstvo zahraničních věcí a Ministerstvo průmyslu a obchodu vydávali závazné stanovisko v případě, že je lhůta stanovena OOP kratší než odpisová lhůta nebo 5 let.

Nová verze:

Vláda ČR rozhoduje o postupu v případě, že je lhůta k vyloučení či omezení dodavatele navržená v OOP kratší než odpisová lhůta nebo 5 let.

- V určitých případech tedy dochází tedy k přímému zapojení vlády do procesu plynoucího z Mechanismu prověřování dodavatelského řetězce.
- Do procesu je nadále ve všech případech zapojena Bezpečnostní rada státu, která má možnost konkrétní případy eskalovat na vládní úroveň.

Harmonogram

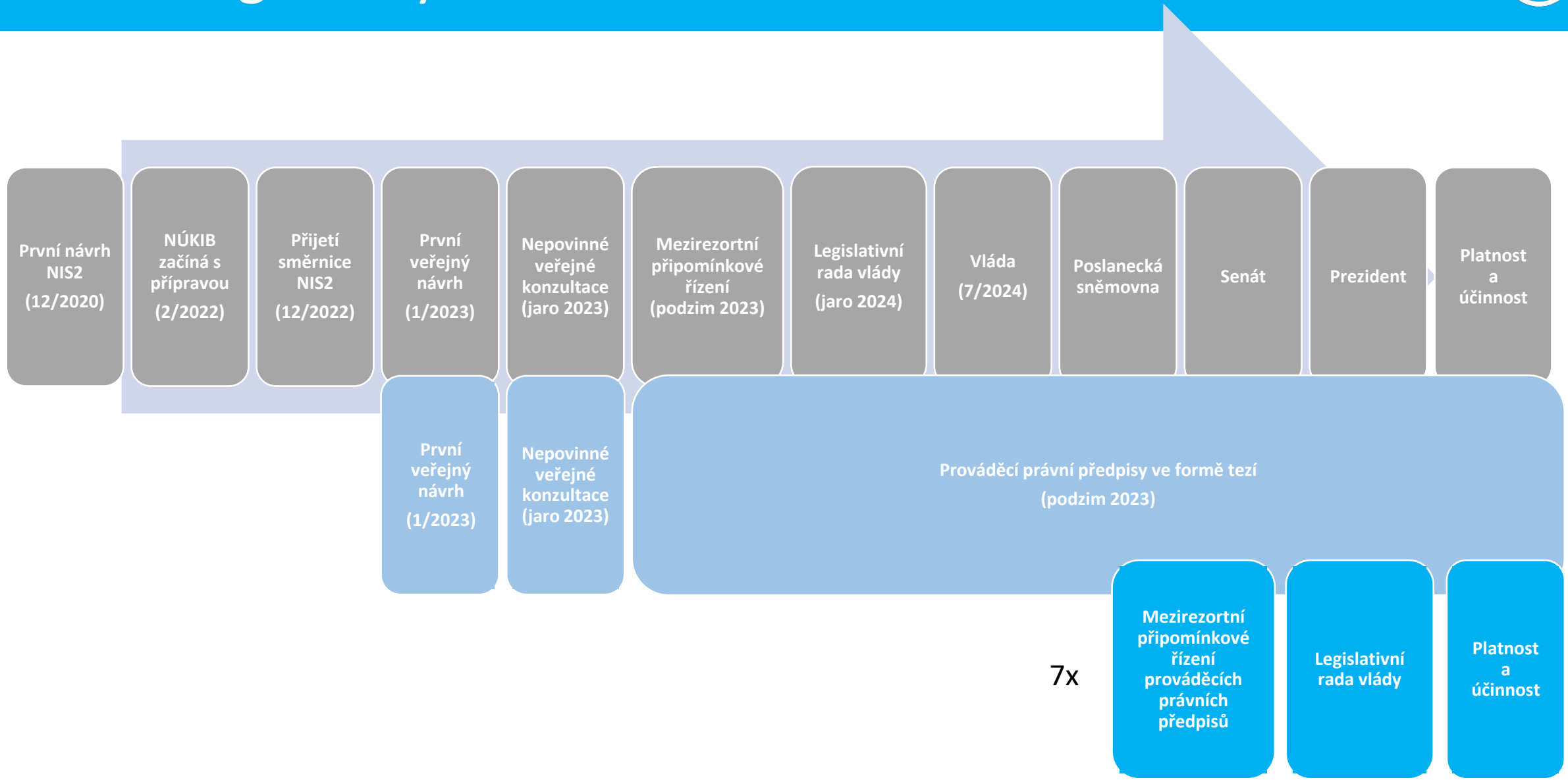


Témata nejčastěji spojená se záměrnými nepravdami

- **Mechanismus prověřování bezpečnosti dodavatelského řetězce**
- **Neomezená koncentrace pravomocí v rukou NÚKIB**
- **Nedostatek diskuze nad problematikou**
- **Vztah zákon – vyhláška**
- **Zpracování RIA**

…

Harmonogram vyhlášek



Co nás ještě čeká?

NÚKIB

DĚKUJI ZA VAŠI POZORNOST!

regulace@nukib.gov.cz

www.nukib.gov.cz

NÚKIB

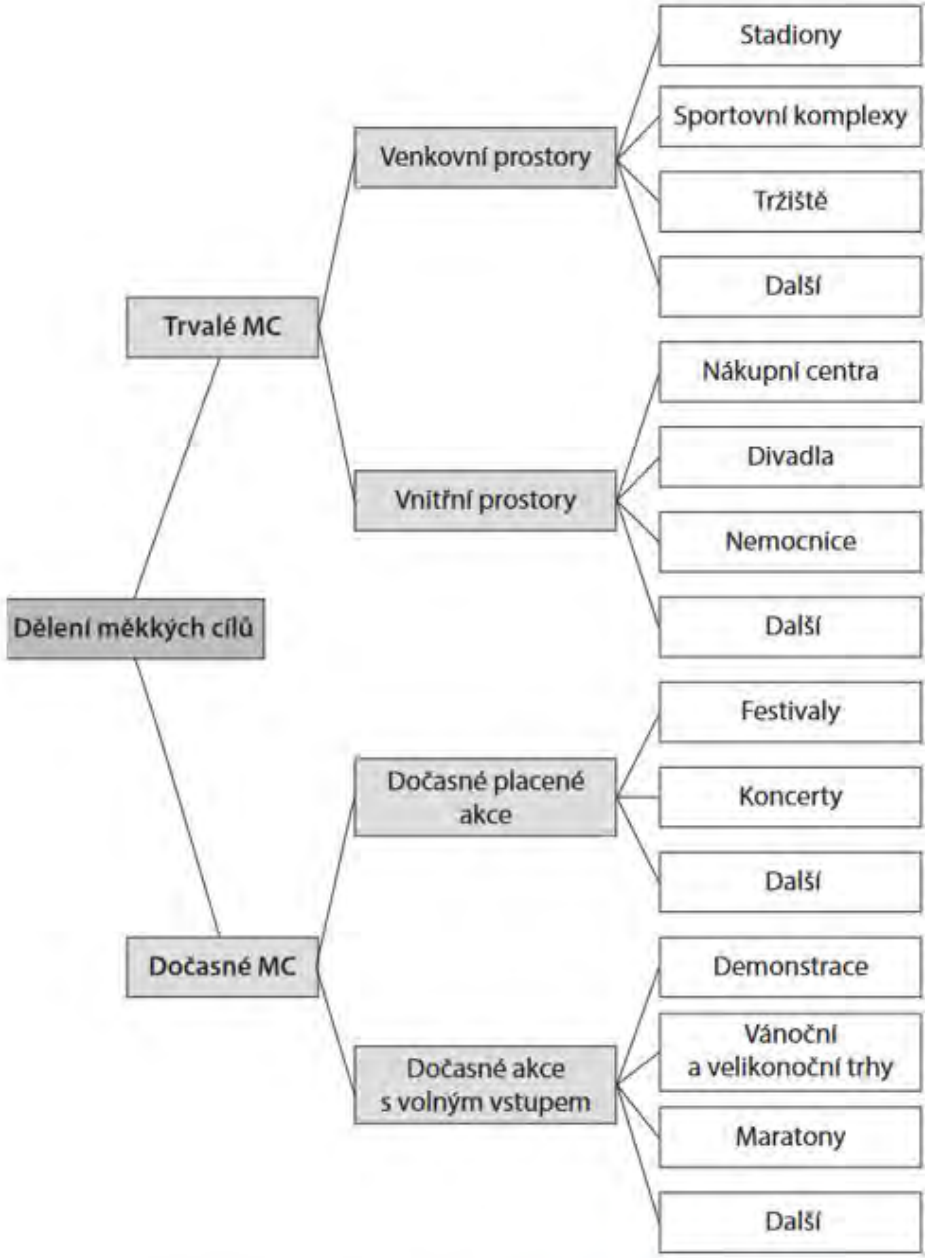
AKADÉMIA POLICAJNÉHO ZBORU

Relevancia vzdelávania a využívania AI v oblasti ochrany mäkkých cieľov

pplk. prof. JUDr. et Mgr. Jana Šimonová, PhD.
prorektor
Akadémia Policajného zboru v Bratislave

Definícia mäkkých cieľov

- Vo všeobecnosti je možné konštatovať, že mäkkým cieľom je konkrétne **vymedzený priestor** s **vysokým počtom** a **koncentráciou osôb**, ktorý je **ľahko dostupný**, **relatívne nechránený**, resp. **ťažko ochraniteľný** a teda **zraniteľný** a ktorý je potrebné chrániť pred konkrétnymi hrozbami.



Delenie mäkkých cieľov (Apeltauer, 2019)

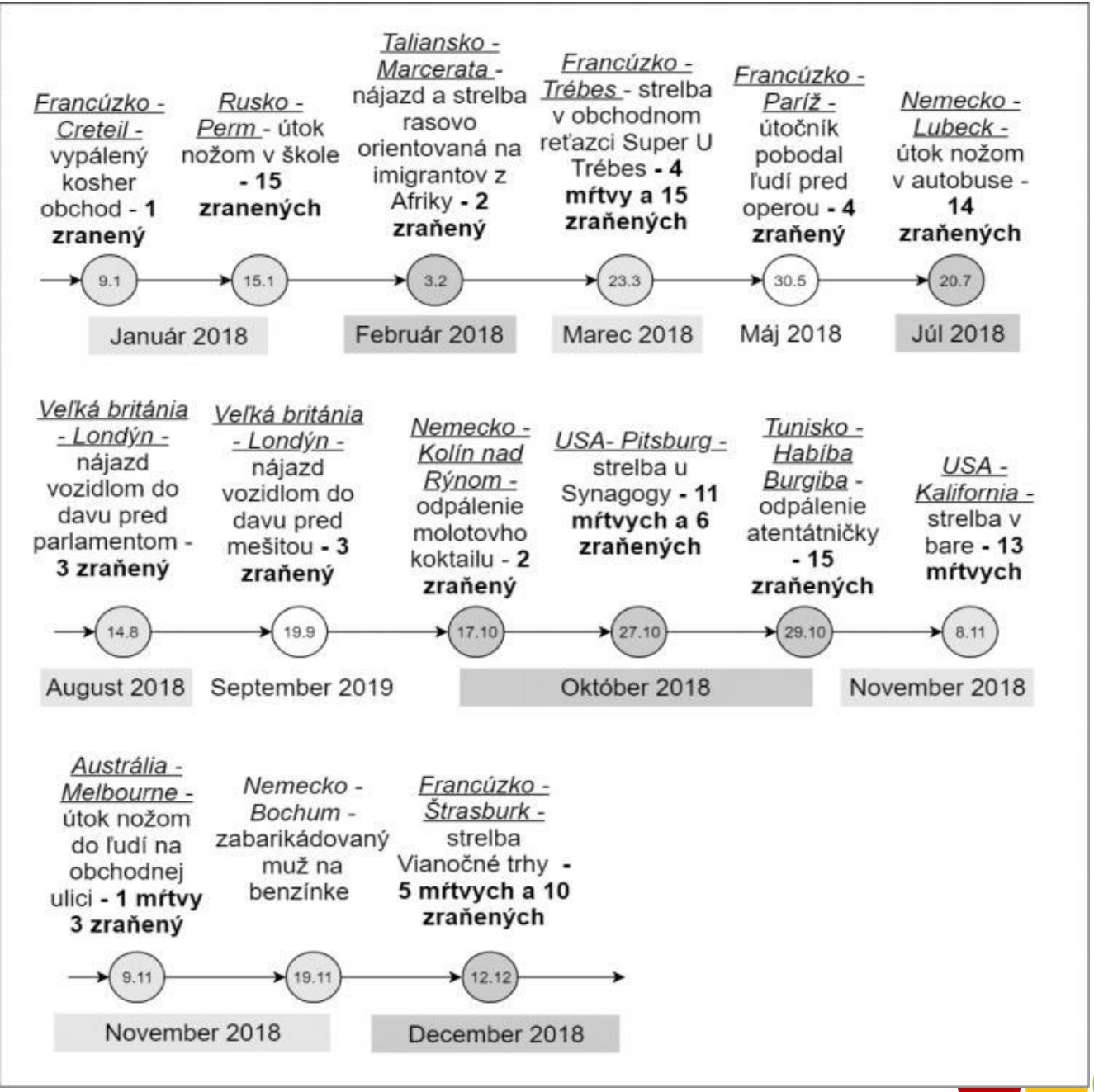
OCHRANA MÄKKÝCH CIEĽOV

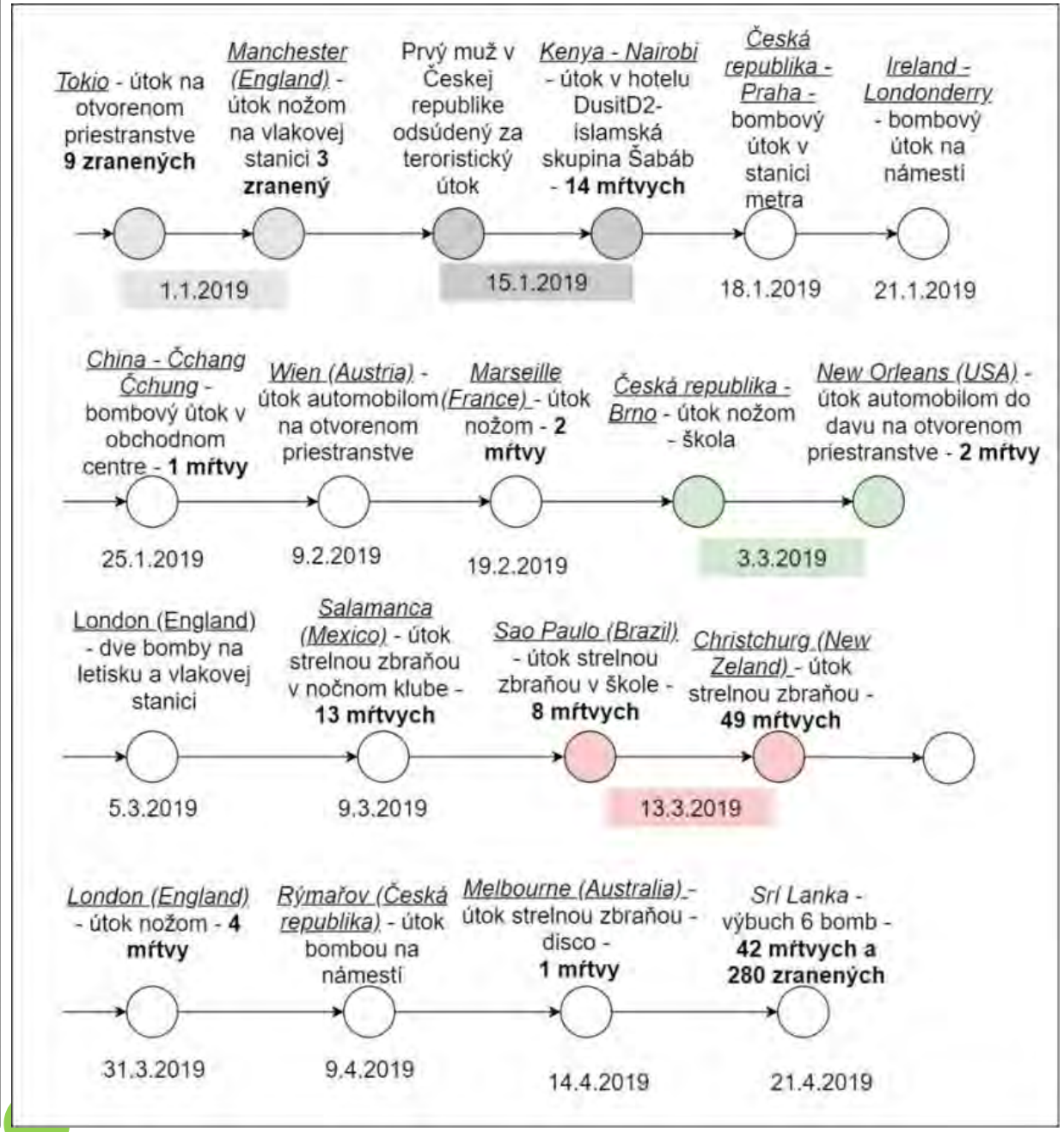
Bezpečnostné špecifiká

- ohrozenie životov
- voľný pohyb verejnosti
- nízka bezpečnosť,
- nepripravenosť MU
- nejasná zodpovedosť
- nízke rozpočty
- laický bezpečnostný manažment

Bezpečnostná situácia SR

- Útok nožom na spojenej škole, Vrútky, 2020, 22-ročný páchateľ
- Teroristický útok na Zámockej ulici, Bratislava, 2022, 19-ročný útočník
- Útok sekerou na strednej škole, Nováky, 2022, 16-ročný páchateľ
- Vyhrážky útokom sekerou na základnej škole, Mníšek nad Hnilcom, 2022, 14-ročný páchateľ
- Útok nožom vo vlaku, Spišská Nová Ves, 2023, 29-ročný páchateľ
- Bombové vyhrážky, 7. mája 2024, neznámy páchateľ

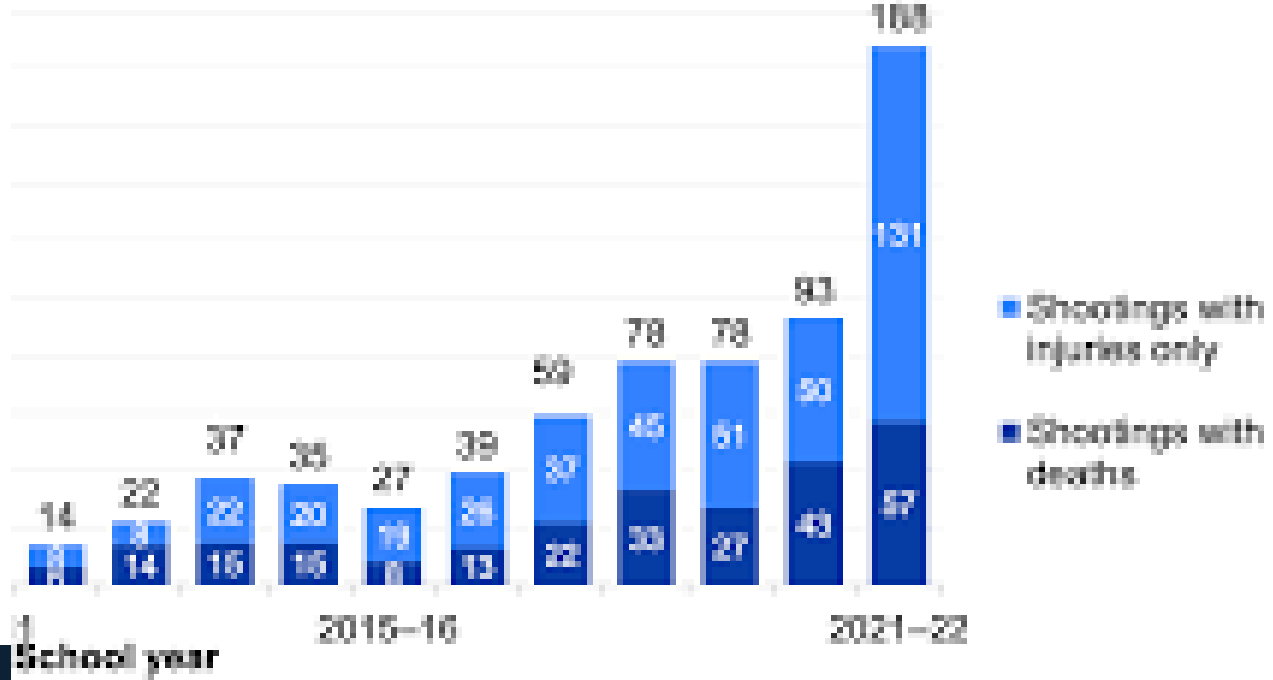

Francúzko - Creteil - vypálený kosher obchod - 1 zranený
9.1
Január 2018
Rusko - Perm - útok nožom v škole - 15 zranených
15.1
Taliansko - Marcerata - nájazd a strelba rasovo orientovaná na imigrantov z Afriky - 2 zranený
3.2
Február 2018
Francúzko - Trébes - strelba v obchodnom reťazci Super U Trébes - 4 mŕtvy a 15 zranených
23.3
Marec 2018
Francúzko - Paríž - útočník pobodal ľudí pred operou - 4 zranený
30.5
Máj 2018
Nemecko - Lubeck - útok nožom v autobuse - 14 zranených
20.7
Júl 2018
Veľká británia - Londýn - nájazd vozidlom do davu pred parlamentom - 3 zranený
14.8
August 2018
Veľká británia - Londýn - nájazd vozidlom do davu pred mešitou - 3 zranený
19.9
September 2019
Nemecko - Kolín nad Rýnom - odpálenie molotovho koktailu - 2 zranený
17.10
USA- Pitsburg - strelba u Synagogy - 11 mŕtvych a 6 zranených
27.10
Tunisko - Habíba Burgiba - odpálenie atentátničky - 15 zranených
29.10
Október 2018
USA - Kalifornia - strelba v bare - 13 mŕtvych
8.11
November 2018
Austrália - Melbourne - útok nožom do ľudí na obchodnej ulici - 1 mŕtvy 3 zranený
9.11
November 2018
Nemecko - Bochum - zabarikádovaný muž na benzínke
19.11
Francúzko - Štrasburk - strelba Vianočné trhy - 5 mŕtvych a 10 zranených
12.12
December 2018


Tokio - útok na otvorenom priestranstve 9 zranených
1.1.2019
Manchester (England) - útok nožom na vlakovej stanici 3 zranený
Prvý muž v Českej republike odsúdený za teroristický útok
15.1.2019
Kenya - Nairobi - útok v hotelu DusitD2- islamská skupina Šabáb - 14 mŕtvych
Česká republika - Praha - bombový útok v stanici metra
18.1.2019
Ireland - Londonderry - bombový útok na námestí
21.1.2019
China - Čchang Čchung - bombový útok v obchodnom centre - 1 mŕtvy
25.1.2019
Wien (Austria) - útok automobilom na otvorenom priestranstve
9.2.2019
Marseille (France) - útok nožom - 2 mŕtvy
19.2.2019
Česká republika - Brno - útok nožom - škola
3.3.2019
New Orleans (USA) - útok automobilom do davu na otvorenom priestranstve - 2 mŕtvy
London (England) - dve bomby na letisku a vlakovej stanici
5.3.2019
Salamanca (Mexico) - útok strelnou zbraňou v nočnom klube - 13 mŕtvych
9.3.2019
Sao Paulo (Brazil) - útok strelnou zbraňou v škole - 8 mŕtvych
Christchurg (New Zeland) - útok strelnou zbraňou - 49 mŕtvych
13.3.2019
London (England) - útok nožom - 4 mŕtvy
31.3.2019
Rýmařov (Česká republika) - útok bombou na námestí
9.4.2019
Melbourne (Australia) - útok strelnou zbraňou - disco - 1 mŕtvy
14.4.2019
Srí Lanka - výbuch 6 bomb - 42 mŕtvych a 280 zranených
21.4.2019

Prípady

- Vrútky, Slovenská republika (2020) 2 mŕtvi, 5 zranených – útok nožom
- • Florida, USA (2018) 17 mŕtvych, 17 zranených - streľba
- • Žďár nad Sázavou, Česká republika (2014) 1 mŕtvy - útok nožom, rukojemníci
- • Beslan, Rusko (2004) 385 mŕtvych, 1100 rukojemníkov - streľba, rukojemníci
- • Brindisi, Taliansko (2012) 1 mŕtvy, 7 zranených - bomba pred školou
- 1999 dvaja študenti Columbine High School, USA, streľba v škole, 12 m., 24 zr.
- 2014 Barbora Orlová, útok nožom na strednej škole, 1 m., 2 zr.;
- 2011 Anders Behring Breivik, streľba na ostrove, Nórsko, 77 mr.;
- 2023 Filozofická fakulta Praha – 15 mr.


Not active shooter
Active shooter


14
22
37
35
27
39
59
78
78
93
188
131
57
49
27
13
22
15
15
Shootings with injuries only
Shootings with deaths
2015–16
2021–22
School year

D:\VIDEO-2023-10-17-07-16-05.mp4

Brusel

D:\VIDEO-2024-03-22-20-54-24.mp4

D:\VIDEO-2024-03-22-20-50-08.mp4

Moskva

Koncertná hala v nákupnom stredisku

Individuálne rizikové vplyvy

- Osobná/osobnostná kríza
- Prežitá trauma
- Konflikt identity/hľadanie vlastnej identity
- Vzory- dospelí, rovesníci
- Túžba po statuse/postavení
- Nadmerné trávanie času v online prostredí
- Nestabilné/zhoršené mentálne zdravie
- Problematické vzťahy – romantické, pracovné
- Predchádzajúca účasť na delikvencii

Typy páchateľov

Strelec z frustrácie- zúfalstvo, strata zamestnania, sklamanie v láske

Strelec z fanatizmu –vyhľadávajú veľké zhromaždenie ľudí, ktoré považujú za zlo, intolerancia, neznášanlivosť voči svetu, naplánovanie (moravsko sliezky kraj – nemocnica, páchateľ si podľa netu zistil rakovinu, preto zabil 7 osob, 2 zranil)

Strelci kultového zamerania – inšpirácia, mladí, detailné plánovanie

Strelci s duševnou poruchou- schizofrenia, depresia, paranoia (Uherský Brod)

Masový a sériový vrah - + 4 mŕtve osoby na jednom mieste (rozdielnosť názorov)

Ako zodolniť mäkké ciele

Synergické doplnenie systému

ochrany verejného poriadku a bezpečnosti

Všeobecné princípy zodolnenia OMC

- Proaktívny prístup– dlhodobo, systematicky
- Bezpečnosť je vecou všetkých dotknutých subjektov
- Identifikácia zraniteľnosti v oblasti bezpečnosti
- Bezpečnostný audit
- Prijímanie účelných opatrení zameraných na elimináciu nedostatkov a potenciálnych rizikových situácii
- Odborná príprava a koordinácia zamestnancov za účelom prípravy na krízovú situáciu
- Primárna prevencia a zmierňovanie dopadov potenciálnych útokov
- Zvyšovanie bezpečnostného povedomia by nemalo byť limitované len na zamestnancov
- Štandardizácia postupov pre prípad krízových situácii podľa ich druhu
- Spolupráca medzi subjektmi (školou, zriaďovateľom, samosprávou a bezpečnostnými zložkami)

Desatoro OMC

1. **Charakterizuj a analyzuj MC, svoju zraniteľnosť a bezpečnost**
2. **Nastav jednotný postup identifikácie hrozby**
3. **K zabezpečeniu MC využi metodickú podporu pre tvorbu bezpečnostního a krízového plánu a urči zodpovedené osoby pre plnenie čiastkových opatrení**
4. **Nastav režimové opatrenia a ich dodržiavanie si vyžaduj a kontroluj**
5. **Štandardizuj postupy evakuácie a invakuácie (unifikovať)**
6. **Vytvor plán internej komunikácie a koordinačný plán pre prípad incidentu (bezp.protokol)**
7. **Nastav pravidelné vzdelávania zamestnancov, využívaj aj info z BOZP a OPP**
8. **Realizuj pravidelné interné nácviky pre zvládnutie mimoriadnej situácie, metodika USB**
9. **Spolupracuj so zložkami IZS a územnou samosprávou**
10. **Buď pripravený, pri prípravách sa neboj zavolať a požiadať o odbornú konzultáciu a pomoc (email, Linka pre OMC????)**

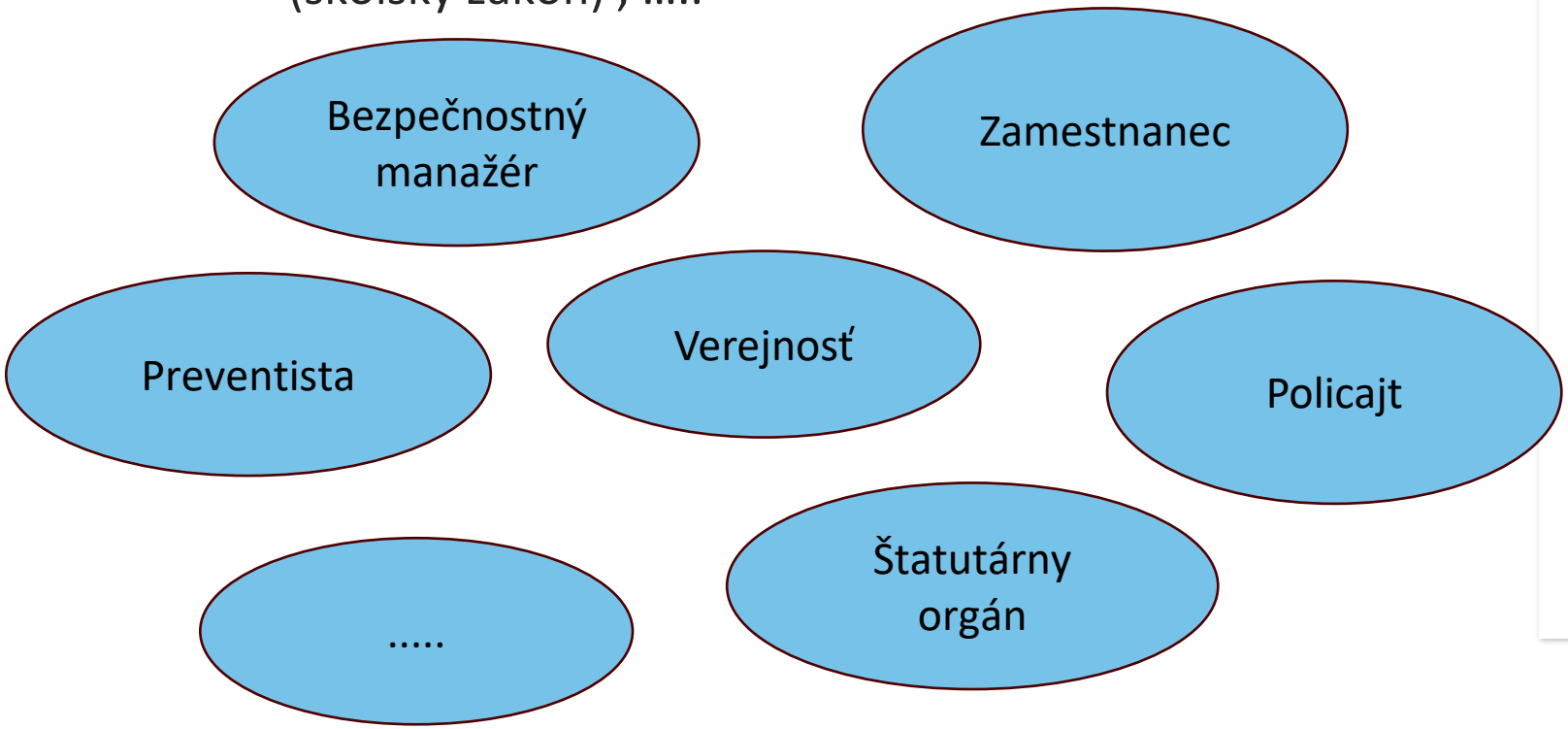
Čo robiť?

1. Vyhodnotenie bezpečnostného rizika (pre konkrétny druh MC, kategorizácia hrozieb)
2. Vytvorenie bezpečnostných postupov, opatrení (bezpečnostný plán k zmierneniu dopadov rizika, krízový plán)
3. Systém internej a externej krízovej komunikácie (prenos informácii pre MU)
4. Školenia interné – komunikácia, bezpečnostný a krízový plán
5. Školenia externé – OMC, ako sa správať v MU, úloha a činnosti koordinačního/krízového štábu
6. Ostatné nácviky a cvičenia
7. Súčinnostné cvičenia (nutnosť partnerov)

Vzdelávanie OMC

Zákon č. 568/2009 Z. z. o celoživotnom vzdelávaní a o zmene a doplnení niektorých zákonov,

Zákon č. 245/2008 Z. z. o výchove a vzdelávaní (školský zákon) , ...



Ministerstvo vnútra Slovenskej republiky

AKADÉMIA POLICAJNÉHO ZBORU

Ministerstvo vnútra
Slovenskej republiky

AKADÉMIA POLICAJNÉHO ZBORU

Vzdelávacie moduly

1 + 2. Prevencia kriminality

3. OMC

4. Základy fyzickej a objektovej bezpečnosti

5.+ 6. viktimológia a poradenská prax

7.+ 8. Príprava vzdelávania a didaktické postupy

Ministerstvo vnútra
Slovenskej republiky

AKADÉMIA POLICAJNÉHO ZBORU

Teoretické, právne, taktické, metodologické a inštitucionálne aspekty ochrany mäkkých cieľov

Teoretické východiská ochrany mäkkých cieľov

Právny rámec a legislatíva ochrany mäkkých cieľov

Bezpečnosť, nebezpečenstvo, základné aspekty bezpečnosti. Verejný poriadok.

Bezpečnostný štandard ochrany mäkkých cieľov

Reakcie na náročné, rizikové a nebezpečné situácie, osoba páchateľa

Vnímanie a rozpoznanie indikátorov, riešenie situácie. Zmena štandardných vzorcov správania.

Ozbrojený útočník, metodika USB

Krízová komunikácia

Fyzická a objektová bezpečnosť

Štandardy bezpečnostného auditu

Objektová bezpečnosť. (perimeter, obvodová ochrana objektu, plášťová ochrana, priestorová ochrana, predmetová ochrana, fyzická ochrana)

Reakcia na vonkajšie hrozby, pripravenosť, informovanosť, spôsob vyrozumievania.

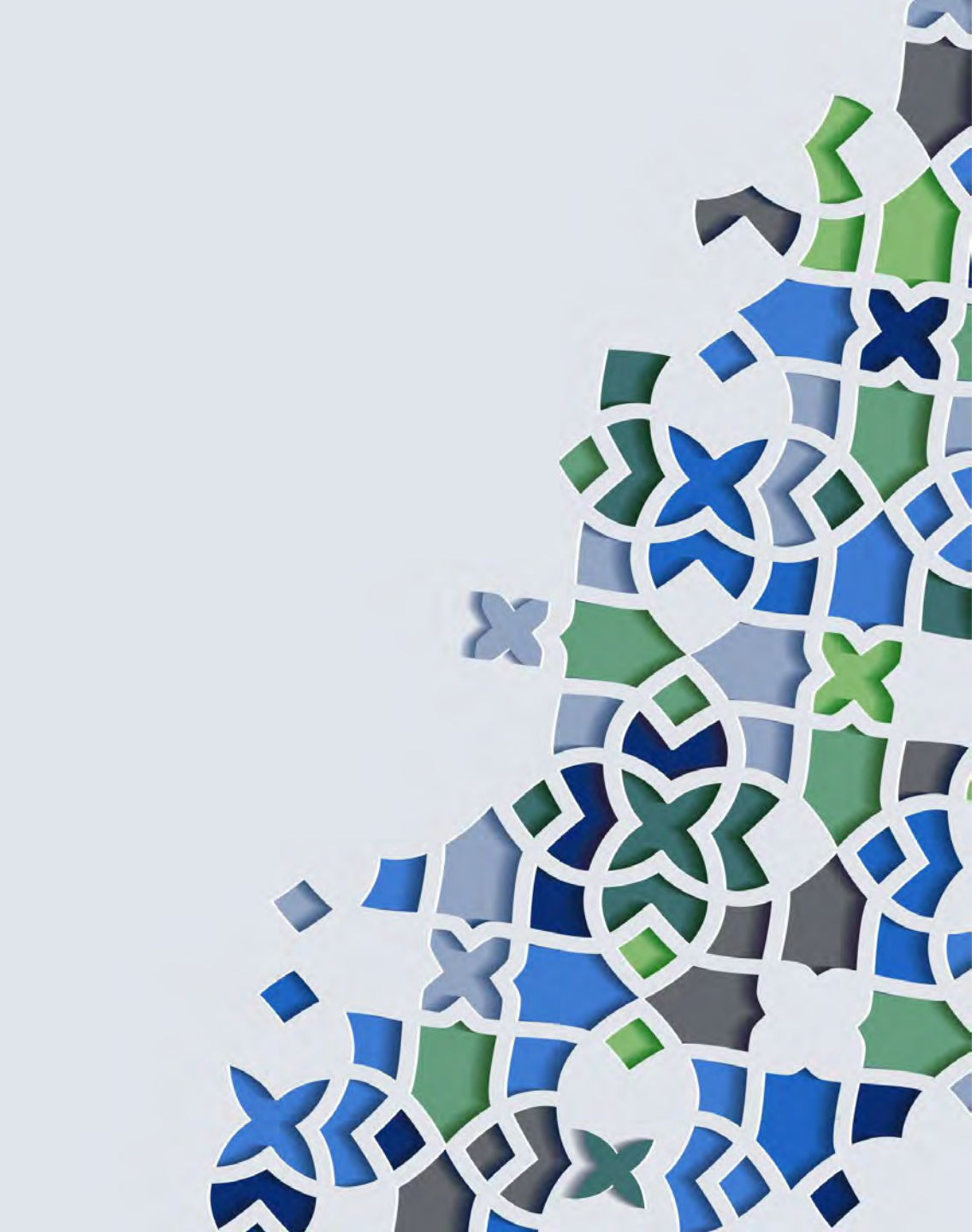
Návrh režimových opatrení.

Prevencia ako významný nástroj predchádzania vzniku útoku.

Spracovanie, príprava bezpečnostných procedúr a krízového riadenia, bezpečnostných protokolov.-

OMC a AI

- Využívanie pri vzdelávaní
- AI v oblasti prevencie
- AI v policajných činnostiach
- AI a identifikácia rizikového správania/hrozby/
- Predvídanie rizikového správania
- Tvorba bezpečnostných plánov/projektov
- Detekcia nevhodného správania v online priestore



ĎAKUJEM ZA POZORNOSŤ

- pplk. prof. JUDr. et Mgr. Jana Šimonová, PhD.
- Profesor v odbore Bezpečnostné vedy
- Prorektor
- Akadémia Policajného zboru v Bratislave
- jana.simonova@akademiapz.sk

Penetračné testovanie verejného sektora a kritickej infraštruktúry v Spojenom kráľovstve

30.9.2024

O mne - Matúš Mihok

- BSc Computer Science, následne MSc Cyber Security
- Certifikáty zamerané primárne na ofenzívnu bezpečnosť
- CHECK Team Leader
- V skratke – „etický hacker a tech nadšenec“
- …zakladateľ spoločnosti Remediata

REMEDIATA

Vysvetlenie pojmov

- CHECK schéma / program
- CHECK Team Leader – CTL (web alebo inf)
- CHECK Team Member – CTM
- Government Communications Headquarters – GCHQ
- National Cyber Security Centre – NCSC
- UK Cyber Security Council – The Council

REMEDIATA

Čo je CHECK schéma?

Štátny program riadený NCSC, ktorého úlohou je akreditovať dodávateľov služieb ofenzívnej bezpečnosti, dohliadať na kvalitu dodávaných služieb, zbierať a vyhodnocovať dáta z projektov ofenzívnej bezpečnosti zameraných na verejný sektor a kritickú infraštruktúru štátu.

REMEDIATA

Čo je CHECK schéma?

NCSC zastrešuje:

- Akreditáciu dodávateľov (spoločností)
- Akreditáciu jednotlivcov (zamestnancov spoločností)
- Zber dát
- Analýzu dát
- Dohľad nad kvalitou dodávaných služieb

REMEDIATA

Testované subjekty

- Ministerstvá, agentúry a úrady
- Kritická infraštruktúra – energetika, doprava, zdravotníctvo, atď
- Obranné agentúry spolupracujúce s MO (MoD)
- Organizácie ktoré pracujú s utajovanými informáciami
- Iné organizácie pripojené na Public Services Network (PSN)

REMEDIATA

Ako a kedy testovať subjekty?

Pravidelne, v 12 mesačných intervaloch – povinne platí napr. pre územné celky (317 okresov - councils). Testovanie poznáme pod pojmom IT Health Check

Po nasadení nového systému/aplikácie do prevádzky

Po významnej zmene v existujúcom systéme/aplikácií

Po závažnom bezpečnostnom incidente

REMEDIATA

Požiadavky na dodávateľov

Sídlo v Spojenom kráľovstve

UK bezpečnostná previerka (Security Clearance)

Skúsenosti a referencie

Kvalifikovaný personál:

- CHECK Team Leader a CHECK Team Member

REMEDIATA

Požiadavky na dodávateľov

Štandardizovaná metodika testovania

Štandardizované výstupné správy

Technické a procesné zabezpečenie

Zmluva medzi NCSC a dodávateľom

Audity

Etické štandardy

REMEDIATA

Požiadavky na jednotlivcov – CTL

CHECK Team Leader je zodpovedný za exekúciu celého projektu, za technickú kvalitu a kvalitu výstupov.

Požiadavky na CTL:

- Technické znalosti
- Skúsenosti s manažovaním komplexných projektov ofenzívnej bezpečnosti
- Bezpečnostná previerka (UK) - minimálne III. Stupeň
- Certifikácia CREST (CCT APP/INF) alebo Cyber Scheme (CSTL APP/INF)
- *2024 – The Council chartership – level CHARTERED / PRINCIPAL

REMEDIATA

Požiadavky na jednotlivcov - CTM

CHECK Team Member má za úlohu participovať na projektoch pod vedením CTL. Nezodpovedá za kvalitu výstupov.

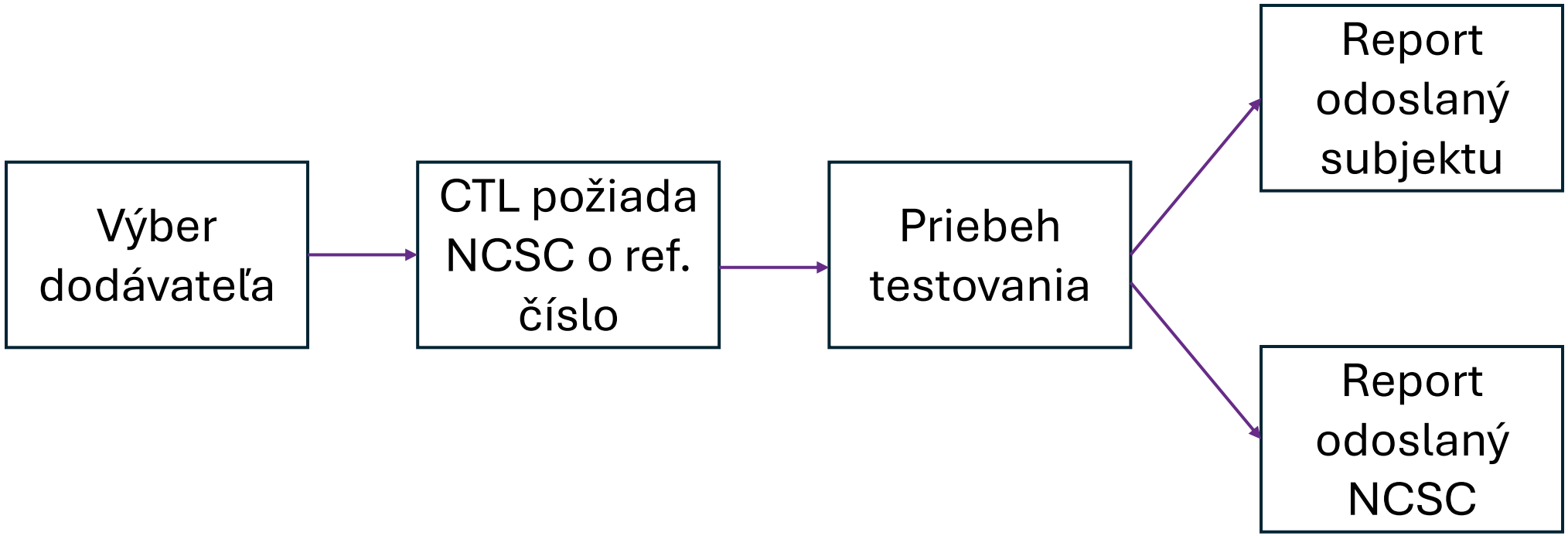
Požiadavky na CTM:

- Technické znalosti
- Bezpečnostná previerka (UK) - minimálne III. Stupeň
- Certifikácia CREST (CRT) alebo Cyber Scheme (CSTM)

CTL/CTM – subdodávanie pod CHECK schémou **nie je možné!**

REMEDIATA

Proces dodania projektu



REMEDIATA

CHECK v číslach

- NCSC eviduje:
  - 205 CHECK Team Leaders
  - 213 CHECK Team Members
  - 2 256 vyprodukovaných reportov za rok 2023
  - 70% CTL WEB, 30% CTL INF

REMEDIATA

inks for your feedback!

ır feedback helps us inform
l improve the website.

Assurance Details

Certified status	Certified

Verify a CHECK professional

Use our verification tool to confirm if someone is currently registered as a CHECK Team Leader or Team Member and eligible to work under the CHECK scheme.

All listed individuals hold a minimum of SC clearance.

matus mihok (Team leader - Infrastructure), is registered

REMEDIATA

Sellafield – sklad rádioaktívneho odpadu

Sheffield – elektráreň na biomasu

Salisbury - Defence Science and Technology Laboratory (DSTL)

Faslane - HMNB Clyde – základňa jadrových ponoriek

REMEDIATA

„Slovenská CHECK schéma“

Slovensko 5.5mil (2022): 17 CTLs

Dohľad nad kvalitou a štandardizácia služieb

Zber a vyhodnocovanie dát

Sledovanie trendov

Zabraňovanie subdodávkam služieb

Argument pre rozpočtovú politiku

REMEDIATA

QA

30.9.2024

REMEDIATA


Cybersecurity Marketplace:
Faster and more efficient access
to proven services
Innovation supported by Digital Europe
www.gamo.sk
Co-funded by
the European Union
ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE
GAMO
INFORMAČNÉ TECHNOLÓGIE

Zuzana Holý Omelková

CCO, CISO

*"The key words today are time and preparedness. Let's start **Decoding Cybersecurity**"*

zuzana.omelkova@gamo.sk

Zuzana Holý Omelková

Decision for Digital Europe

- product for foreign markets
- the need for rapid investment
- transparent evaluation of projects
- 75% project funding

Co-funded by the European Union
ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE
GAMO
INFORMACNE TECHNOLOGIE

Road to approval

grant agreement

project approval

incorporation of comments

first submission of a project

two weeks of intensive creation


CYBER
PLACE
KEEP YOUR DATA SAFE

CYBER PLACE

Helps increase resilience to cyber attacks, increase knowledge of cybersecurity processes and solutions, support public and private organizations in achieving a baseline level of cybersecurity awareness, eliminate the risk of managerial failure

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

GAMO INFORMACNE TECHNOLOGIE

CYBER PLACE

- cybersecurity marketplace
- the MPS segment within the EU
- development of innovative products
- partnership programme
- 24 months
- KPI‘s

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
GAMO INFORMACNE TECHNOLOGIE

Part of CYBER PLACE

Cybersecurity Products and Services

Interconnecting Experts

Education

Knowledge Transfer

Providing Expertise

Co-funded by
the European Union

ECCC

GAMO
INFORMAČNÉ TECHNOLÓGIE

www.cyber-place.eu

Co-funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

GAMO
INFORMACNE TECHNOLOGIE

Prepojenie ochrany mäkkých cieľov a kybernetickej bezpečnosti:

Efektívne stratégie na zvládnutie súčasných hrozieb

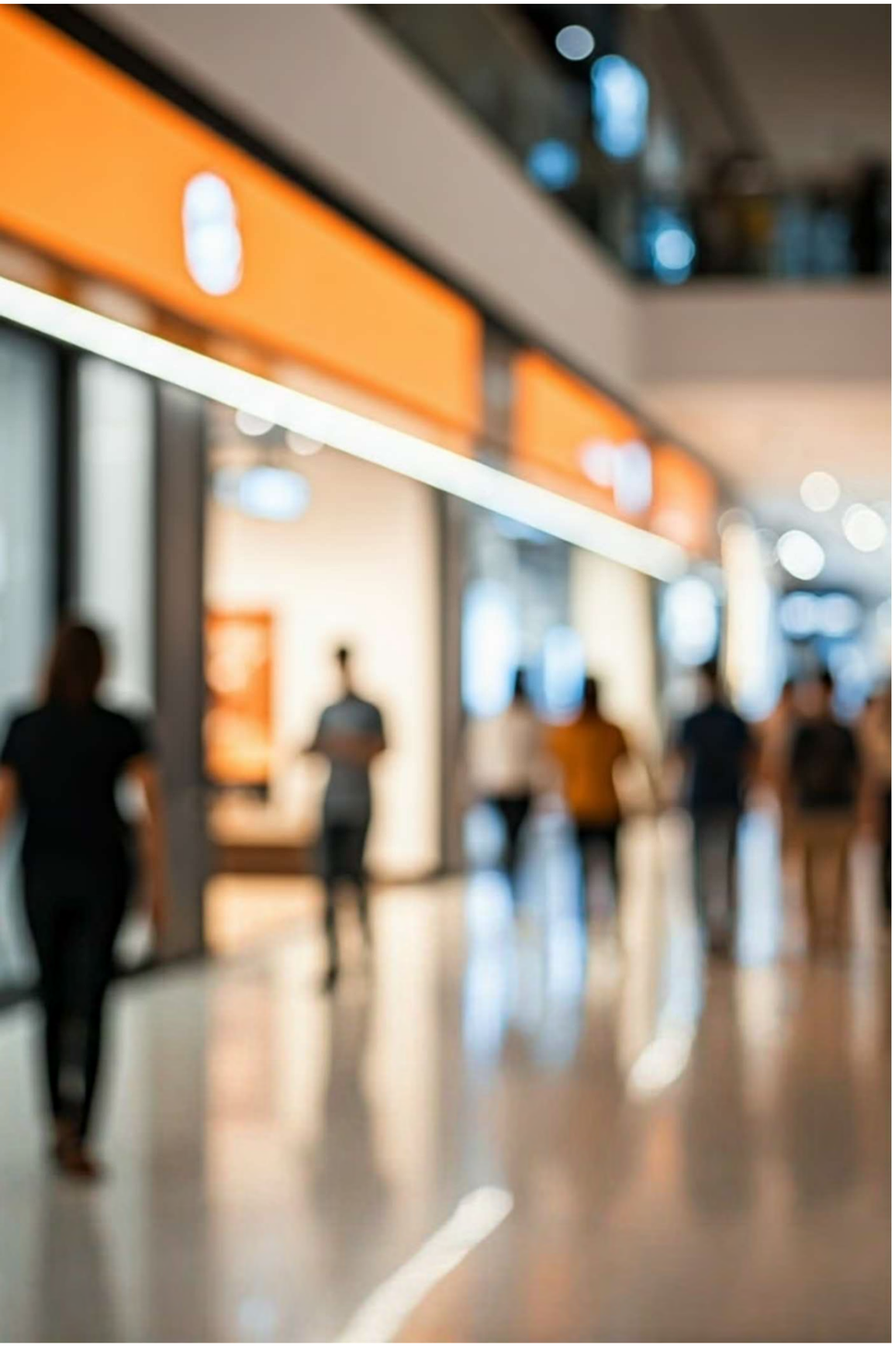
Kybernetická bezpečnosť je súčasťou ochrany mäkkých cieľov.

Predstavenie aktuálnych a budúcich iniciatív na Slovensku.

Pozvanie do spolupráce.

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

PREVENCIA KRIMINALITY



Čo sú mäkké ciele?

Definícia

Verejné miesta s veľkou koncentráciou ľudí a nízkou ochranou.

Zraniteľnosť

Vystavené fyzickým aj kybernetickým hrozbám.

Prepojenie hrozieb

Kyberútoky môžu vyvolať fyzické riziká.

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

PREVENCIA KRIMINALITY

Súčasné hrozby pre mäkké ciele

Fyzické útoky

Bombové hrozby, fyzické útoky, vandalizmus.

Kybernetické hrozby

Útoky na nemocnice, školy, obchodné centrá, verejné inštitúcie a pod.

Prepojenie hrozieb

Kybernetické útoky ako príprava na fyzické útoky.

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

PREVENCIA KRIMINALITY

Integrácia fyzickej a kybernetickej bezpečnosti

1

Technologické riešenia

Inteligentné kamery, prístupové a komunikačné systémy potrebujú kybernetickú ochranu.

2

Fyzická bezpečnosť

Napadnuté digitálne systémy ohrozujú fyzickú bezpečnosť.

3

Vzdelávanie

Prepojenie bezpečnostných tímov a IT špecialistov.

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

PREVENCIA KRIMINALITY

Slovenský kontext – Kde sme dnes?

1 Súčasné opatrenia

Základné kroky zavedené. Budujeme integrovaný prístup.

2 Príklady z praxe

Nedávne bombové hrozby v školách.

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

PREVENCIA KRIMINALITY

Profil páchateľa útoku v školskom prostredí (na čo sa zamerať)

Vek

Najčastejšie mladiství alebo mladí dospelí vo veku 13–21 rokov.

Sociálny status

Často pochádzajú z dysfunkčných rodín, sociálne izolovaní, s nízkym sociálno-ekonomickým statusom.

Predchádzajúce správanie

História agresívneho alebo antisociálneho správania, ako je šikana, zneužívanie návykových látok alebo predchádzajúce delikty.

Motívy

Pomsta za vnímané krivdy, šikana, pocit menejcennosti, potreba prejavu moci alebo pozornosti.

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

PREVENCIA KRIMINALITY

Prevencia pre ochranu mäkkých cieľov

Druh / Čas	Primárna prevencia	Sekundárna prevencia	Terciárna prevencia
Sociálna prevencia	Vzdelávanie verejnosti o rizikách a správnych reakciách, posilnenie sociálnych služieb **(MV SR, MŠVVM SR, MPSVR SR, školy)**	Identifikácia rizikových skupín a školenie zamestnancov škôl **(MŠVVM SR, školy)**	Psychologická podpora pre obete a programy reintegrácie **(MZ SR, MPSVR SR)**
Situačná prevencia	Inštalácia kamerových systémov, zvýšenie fyzickej ochrany objektov **(zriaďovatelia škôl, školy)**	Včasné varovné systémy, poplašné systémy v školách **(zriaďovatelia škôl, školy)**	Zvýšený monitoring v rizikových oblastiach, bezpečnostné zásahy **(bezpečnostné zložky, IZS)**
Viktimačná prevencia	Vzdelávanie žiakov a zamestnancov, ako sa správať pri hrozbách **(MŠVVM SR, školy, MV SR)**	Podpora pre rizikové skupiny, prevencia zameraná na zraniteľných jedincov **(MŠVVM SR – CPP, MPSVR SR)**	Podpora pre rizikové skupiny, prevencia zameraná na zraniteľných jedincov **(MŠVVM SR – CPP, MPSVR SR)**

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

PREVENCIA KRIMINALITY

Aktivity MV SR v roku 2024 pre školy

Zber a spracovanie dát

Vypracovanie bezpečnostného dotazníka pre základné a stredné školy. Spolupráca s Ministerstvom školstva, OPP PPZ, APZ, UNIZA a OPK MV SR.

odporúčania pre školy

Vzdelávacie aktivity

Realizácia vzdelávacích aktivít v oblasti radikalizácie, extrémizmu a (kyber)šikany, Online bezpečnosti, Mediálnej gramotnosti, Nenávistných prejavov a Antisemitizmu.
+ 3.824 aktivít pre 94.600 žiakov ZŠ a SŠ
+ 30 aktivít pre 920 zamestnancov

Odborné materiály

Vypracovanie príručky **pre kontaktných policajtov**.

Vypracovanie **bezpečnostných štandardov pre vysoké školy**.

Predloženie návrhu **Postupu škôl pri výskyte špecifických prípadov pre MŠVVM SR**.

Vypracovanie informačných materiálov k ochrane mäkkých cieľov - **letáka U-S-B**.

Realizácia **videospotu U-S-B**.

Školenia

Pre kontaktných policajtov v každom kraji

Pripravujeme pre zástupcov mestských polícií

Spolupráca

Vyčlenenie **2050 príslušníkov PZ** na spoluprácu so školami

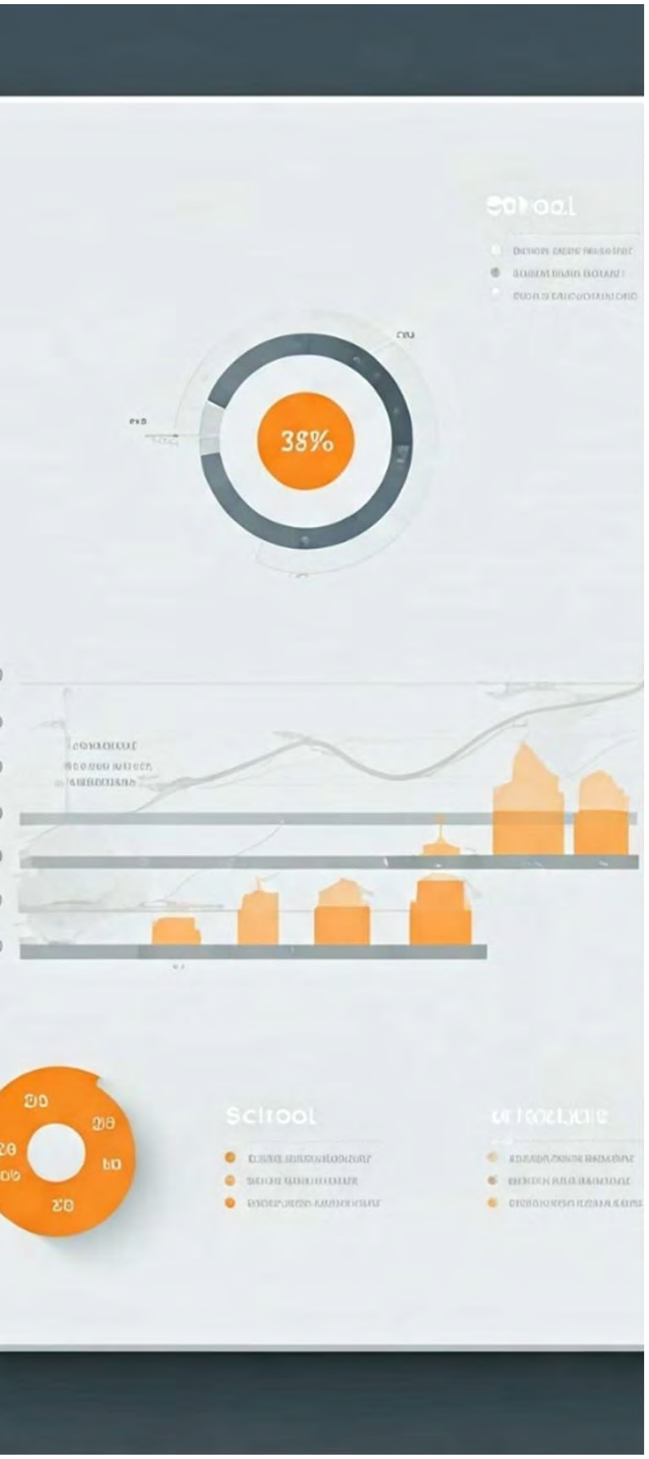
16 informačných kancelárií pre obete

Pomoc Obetiam

Poskytovanie pomoci obetiam vrátane radikalizácie, extrémizmu a (kyber)šikany.
Informačné kancelárie pre obete poskytujú **pomoc viac ako 1000 klientom ročne**.

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

PREVENCIA KRIMINALITY



Dáta z 2781 škôl

Monitorovaný areál školy kamerovým systémom	41% škôl (1137)
Monitorované vnútorné priestory kamerovým systémom	30% škôl (821)
Zabezpečené vybrané vnútorné priestory detektormi pohybu alebo narušenia	34% škôl (946)
Príprava žiakov na vonkajšie hrozby	64% škôl (1778)
Príprava zamestnancov na vonkajšie hrozby	50% škôl (1380)
Vážne verbálne napadnutie učiteľa žiakom za posledných 5 rokov	12% škôl (332)
Fyzické napadnutie učiteľa za posledných 5 rokov	3% škôl (89)

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

PREVENCIA KRIMINALITY

Aktuálne opatrenia OPK MV SR

1

Akreditácia v oblasti prevencie kriminality

Budovanie siete expertov na ochranu mäkkých cieľov.

2

Akčný plán ochrany mäkkých cieľov pre rok 2025

Zavádzanie komplexných bezpečnostných opatrení pre školy a verejné inštitúcie.

3

Kriminologický inštitút

Spolupráca s expertmi na ochranu mäkkých cieľov, vývoj a analýza nových bezpečnostných opatrení.

4

Rozširovanie siete informačných kancelárií

Ministerstvo rozširuje sieť informačných kancelárií, ktoré poskytujú obetiam trestných činov bezplatné právne, psychologické a sociálne poradenstvo, a občanom tiež informácie o ich právach a možnostiach ochrany.

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

PREVENCIA KRIMINALITY

Aktivity OPK MV SR

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

PREVENCIA KRIMINALITY

Uteč-Skry sa-Bojuj

https://www.minv.sk/?aktuality-omk

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

PREVENCIA KRIMINALITY

Odporúčania a ďalšie kroky

Legislatívne opatrenia	Zmeny na podporu prepojenia kybernetickej a fyzickej ochrany?
Financovanie	Zabezpečenie zdrojov pre nové technológie
Vzdelávanie	Školenia zahŕňajúce fyzické aj digitálne hrozby

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

PREVENCIA KRIMINALITY

Záver

1 Výzva na spoluprácu

Medzi bezpečnostnými inštitúciami, technologickými firmami a odborníkmi.

2 Spoločný cieľ

Ochrana mäkkých cieľov je nevyhnutná.

3 Urgentnosť

Je potrebné konať hneď, hrozby nepočkajú.

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

PREVENCIA KRIMINALITY

Tešíme sa na spoluprácu

Jozef Halcin

riaditeľ

odbor prevencie kriminality

Ministerstvo vnútra Slovenskej republiky

Odbor prevencie kriminality je zodpovedný za rozvoj a implementáciu stratégií na prevenciu kriminality. Odbor zabezpečuje spoluprácu s rôznymi organizáciami a inštitúciami s cieľom zvýšiť povedomie aj o ochrane mäkkých cieľov.

www.minv.sk

prevencia@minv.sk

@prevenciakriminality

#prevenciakriminality

Obrázky vygenerovala umelá inteligencia

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

PREVENCIA KRIMINALITY

Riadenie dodávateľského reťazca v KB

EPI konferencia Kybernetická bezpečnosť 2024

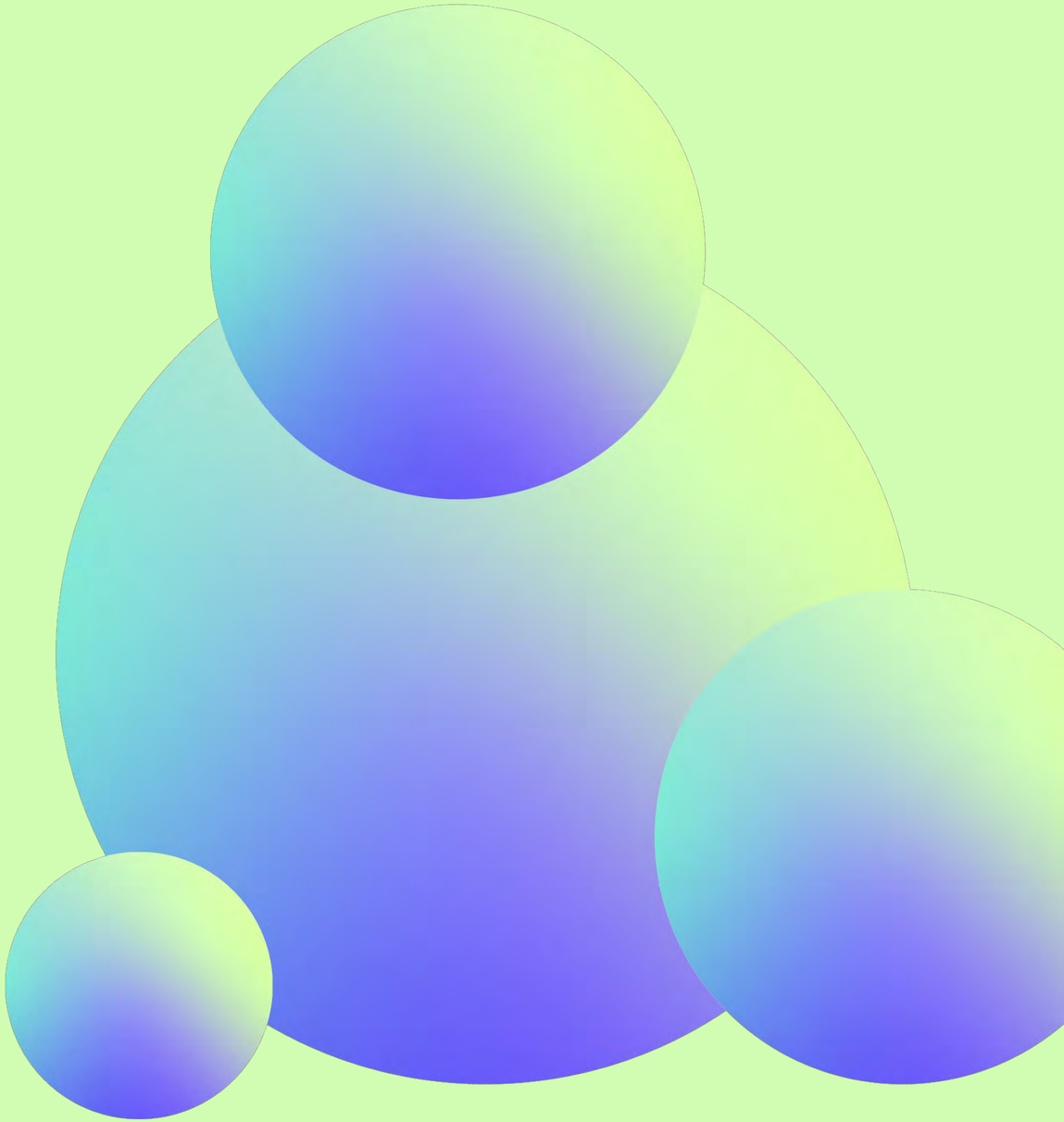
JUDr. Štefan PILÁR
advokát / partner
Jasná, október 2024

OBSAH

OBSAH

- Tretia strana
- Analýza rizík tretích strán
- Zmluva s treťou stranou

Tretia strana



Tretia strana

osoba vykonávajúca činnosť, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby

alebo

priamo súvisí s prevádzkou sietí a informačných systémov prevádzkovateľa základnej služby

Tretia strana

(„*po novele*“)

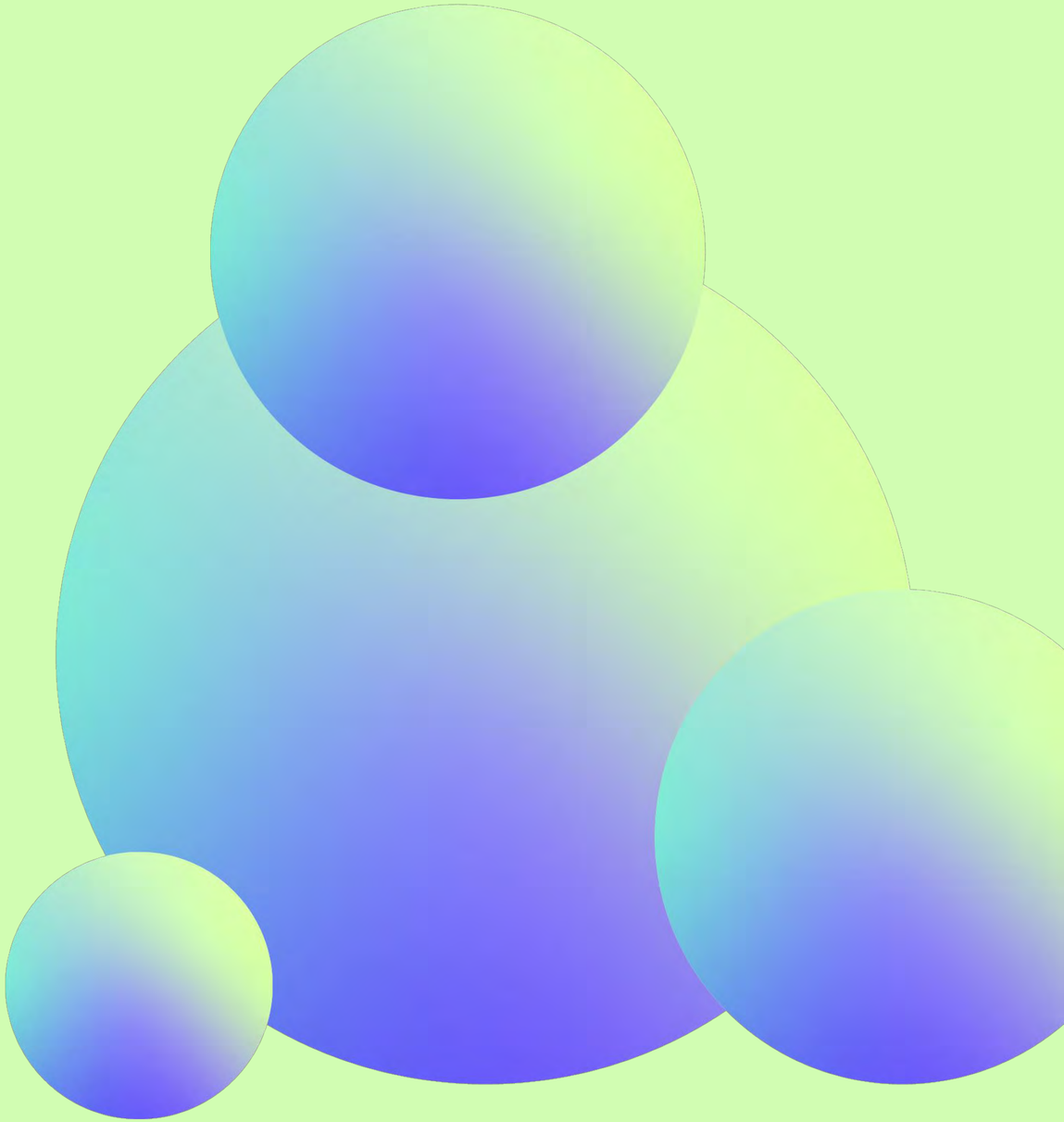
osoba vykonávajúca činnosť, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby

Tretia strana

(„*po novele*“)

- tretia strana (*kritická základná služba*) má „postavenie PZS“:
  - povinný zápis do registra PZS
  - realizácia bezpečnostných opatrení (zmluva + ZoKB)
  - kontrola
- výnimka § 19/3 sa nevzťahuje na kritické služby
- tretia strana (*sektor Digitálna infraštruktúra*) = relevantný subjekt (*PZS*)

Analýza rizík



Analýza rizík

Členské štáty zabezpečia, aby subjekty pri zvažovaní toho, ktoré opatrenia uvedené v odseku 2 písm. d) sú vhodné, ***zohľadňovali zraniteľnosti špecifické pre každého priameho dodávateľa a poskytovateľa služieb*** *a celkovú kvalitu produktov a postupy svojich dodávateľov a poskytovateľov služieb KB vrátane ich postupov bezpečného vývoja.*

Členské štáty tiež zabezpečia, aby subjekty pri zvažovaní toho, ktoré opatrenia uvedené v uvedenom písmene sú vhodné, boli povinné zohľadňovať ***výsledky koordinovaných posúdení bezpečnostných rizík*** *kritických dodávateľských reťazcov vykonaných v súlade s článkom 22 ods. 1.*

Analýza rizík

/ § 19 ods. 2 ZoKB/ ... pri uzatvorení zmluvy sa vykonáva analýza rizík.

a

/ § 9 ods. 1 V/ ...pri uzatvorení zmluvy s treťou stranou podľa § 19 / 2 ZoKB sa analyzujú riziká dodávateľských služieb, spôsobom podľa § 6.

/ § 6 V/ (*zraniteľnosti, hrozby, riziká s ohľadom na aktívum, vlastník rizika, opatrenia, BIA, preskúmanie*)

Analýza rizík

(*„po novele“*)

/ZoKB/ **---** .

a

/V/ ??? .

Výkon Analýzy rizík

(*metodika*)

- podľa metodiky osvojenej organizáciou alebo inej metodiky (napr. NBÚ)
- porovnateľnosť výsledkov a opakovateľnosť!

Výkon Analýzy rizík

(*začiatok*)

- checklist
- vyjadrenie tretej strany
- podklady od tretej strany - dôkazy na preukázanie vyjadrení tretej strany (bezpečnostná dokumentácia, analýza rizík, BCM, prístupy, riadenie zraniteľností, incidentov...)

zero trust = ak nepreukáže / nepredloží, mám za to, že

nemá / neplní / neexistuje

Výkon Analýzy rizík

(*postup*)

- aktíva (*vzťah k činnosti tretej strany*)
- hrozby (*podmnožina katalógu hrozieb*)
- zraniteľnosti (*u tretej strany*)
- implementované bezpečnostné opatrenia (*u tretej strany!*)
- rizikové scenáre a ich vyhodnotenie (*P x D*)
- návrh bezpečnostných opatrení (*GAP*)

Výkon Analýzy rizík

(*obsah a rozsah bezpečnostných opatrení*)

- **<u>Minimálne</u>**:

  - riadenie prístupov
  - hodnotenie zraniteľností a bezpečnostné aktualizácie
  - ochrana proti škodlivému kódu
  - sieťová a komunikačná bezpečnosť
  - zaznamenávanie udalostí a monitorovanie
  - riešenie kybernetických bezpečnostných incidentov

Výkon Analýzy rizík

(*obsah a rozsah bezpečnostných opatrení*)

- **<u>Optimálne</u>** (*vyžadované ZoKB*):

  - na základe výsledkov analýzy rizík

Zmluva s treťou stranou

Zmluva s treťou stranou

(*dnes*)

- podstatné náležitosti v zmysle § 9 ods. 2 V

Zmluva s treťou stranou

(*po novele*)

- explicitná požiadavka Smernice NIS 2 *(„bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi jednotlivými subjektmi a ich priamymi dodávateľmi alebo poskytovateľmi služieb“)*
- nová bezpečnostná vyhláška
- rovnaký názov zmluvného typu

- *rovnaký obsah*?

Zmluva s treťou stranou

(*bezpečnosť po uzatvorení*)

- nutnosť pravidelne overovať splnenie a udržiavanie (kontrola / audit)
- detailné pravidlá pre proces nápravy
- auditné / kontrolné zistenia - režim nápravy
- zabezpečenie / podpora plnenia:

  - zmluvné pokuty
  - podstatné porušenie a vzájomná závislosť zmlúv

Otázky?

JUDr. Štefan PILÁR
stefan.pilar@signum.legal

SIGNUM.LEGAL

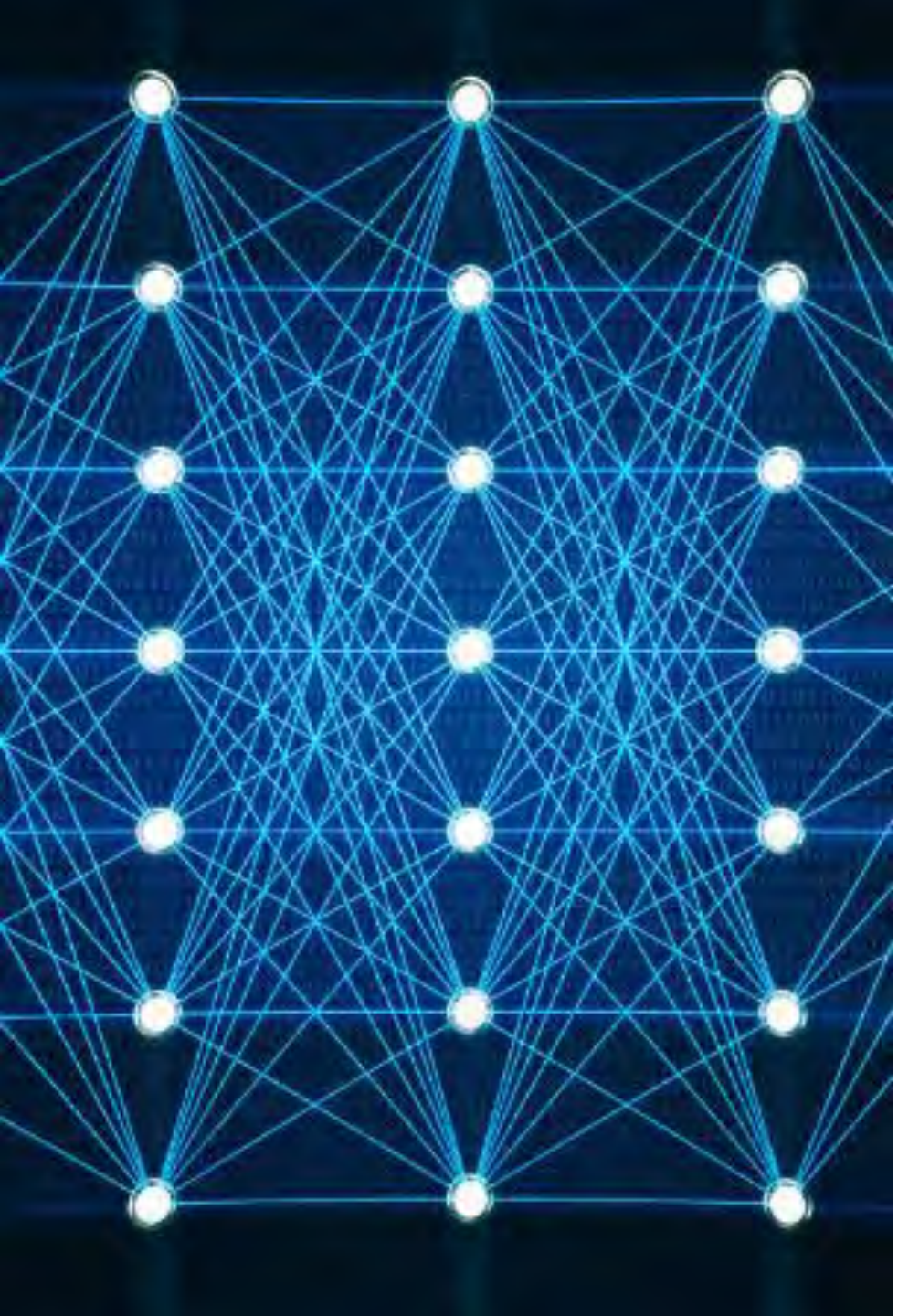
Úskalia implementácie systémov umelej inteligencie a hľadanie zjednodušení na základe požiadaviek právnych predpisov

MGR. MAREK ZEMAN PHD. CRISC

Požiadavky na systémy umelej inteligencie

Dôveryhodná AI musí byť

1. Funkčná
2. Zákonná
3. Odolná
4. Etická



Implementácia prístupov vzhľadom na aplikácie.

Zvážiť technické algoritmy a riešenia

Vyžadovať jasné informácie o funkčnosti a možnostiach

Zabezpečiť vývoj systémov

Sledovať a Dohliadať vývoj systémov

Vyžadovať sledovateľnosť a kontrolovateľnosť

Riadiť riziká systémov

Zákonné rámce na ochranu systémov AI.

EU Artificial Intelligence Act

GDPR

General Data Protection Regulation

Riadenie rizík systémov AI

Aplikačné riziká

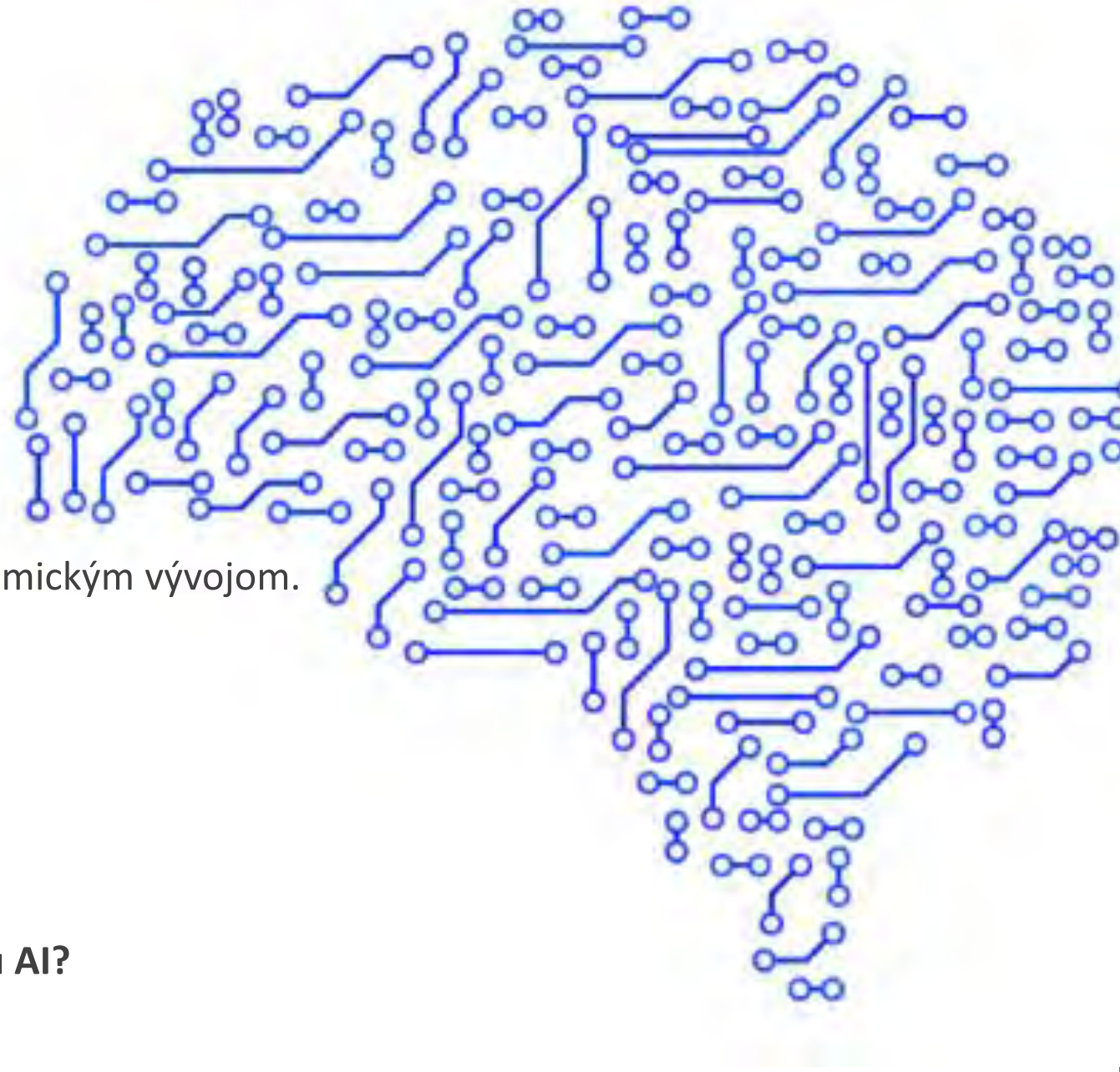
Algoritmické riziká
- Algoritmus ako taký
- Algoritmus po naštartovaní samoučenia

Ochrana súkromia a GDPR

Ľudský faktor

Sociálny pohľad

Odporúčania:
Ako v súčasnosti pokryť systémy AI?



Ochrániť systémy pred narušením (dáta, app)

Riadiť riziká z pohľadu existujúceho algoritmu.

Zvažovať riziká, vznikajúce samoučením alebo algoritmickým vývojom.

Ochrana súkromia a GDPR

Pohľad dopadu algoritmu na klienta

Sociálny pohľad.

ČO JE VLASTNE INÉ AKO KEĎ SME BOLI BEZ dodatku AI?

Návrh riešenia.

Minimum
- GDRP požiadavky
- Aplikačná bezpečnosť
- Dátová bezpečnosť
- **Etické požiadavky**

Rozšírenie
AIA požiadavky

Dobrá rada
Majte riadenie cez risk manažment

?

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Cesta od Cybergame k European Cybersecurity Challenge (ECSC)

Príprava a vedenie národného tímu mladých kybertalentov

1.10.2024

Alexandra Húsková, Lukáš Balážik
Cyber Security Competence Centre

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autorov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

CYBERGAME

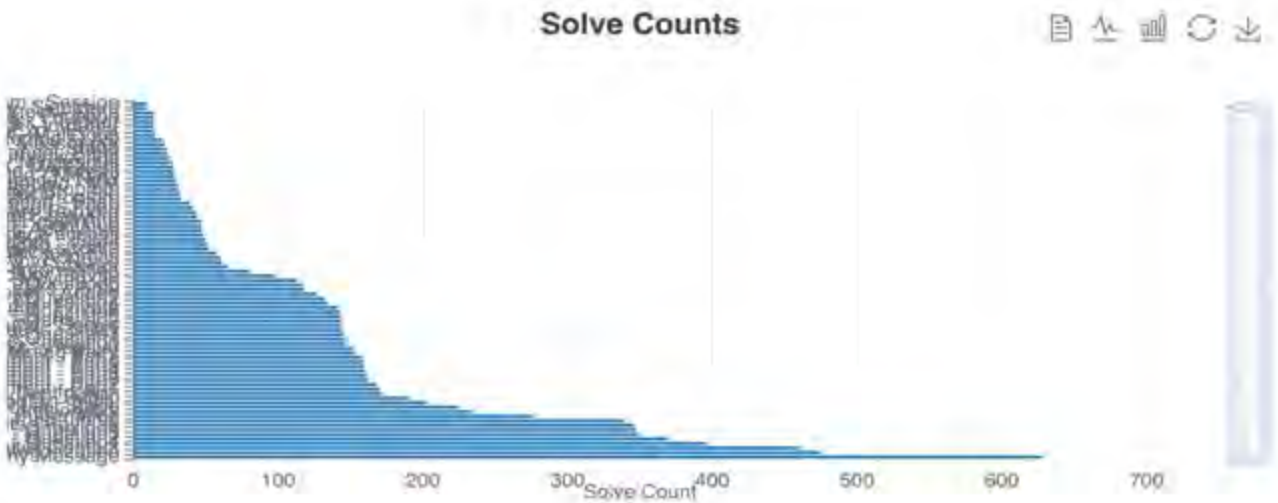
- CYBERGAME je kybernetická súťaž štýlu CTF
  - Capture The Flag (Jeopardy, Boot2Root, Attack&Defense)
  - Zamerané na analýzu
  - Vetva ➤ Scenár ➤ Úloha
    - Body za úlohu
    - Body za scenár
  - Rôzne obtiažnosti

Ako sme dopadli tento rok?

- 15 scenárov, 79 úloh
- 2312 registrovaných, 874 aktívnych
- z 874 aktívnych bolo až 606 študentov

2312 users registered
4835 IP addresses

550 total possible points
79 challenges
[★☆☆] **UniqueCrypto - Funny Message** has the most solves with 628 solves
[★★★] **Modernism - Session** has the least solves with 9 solves

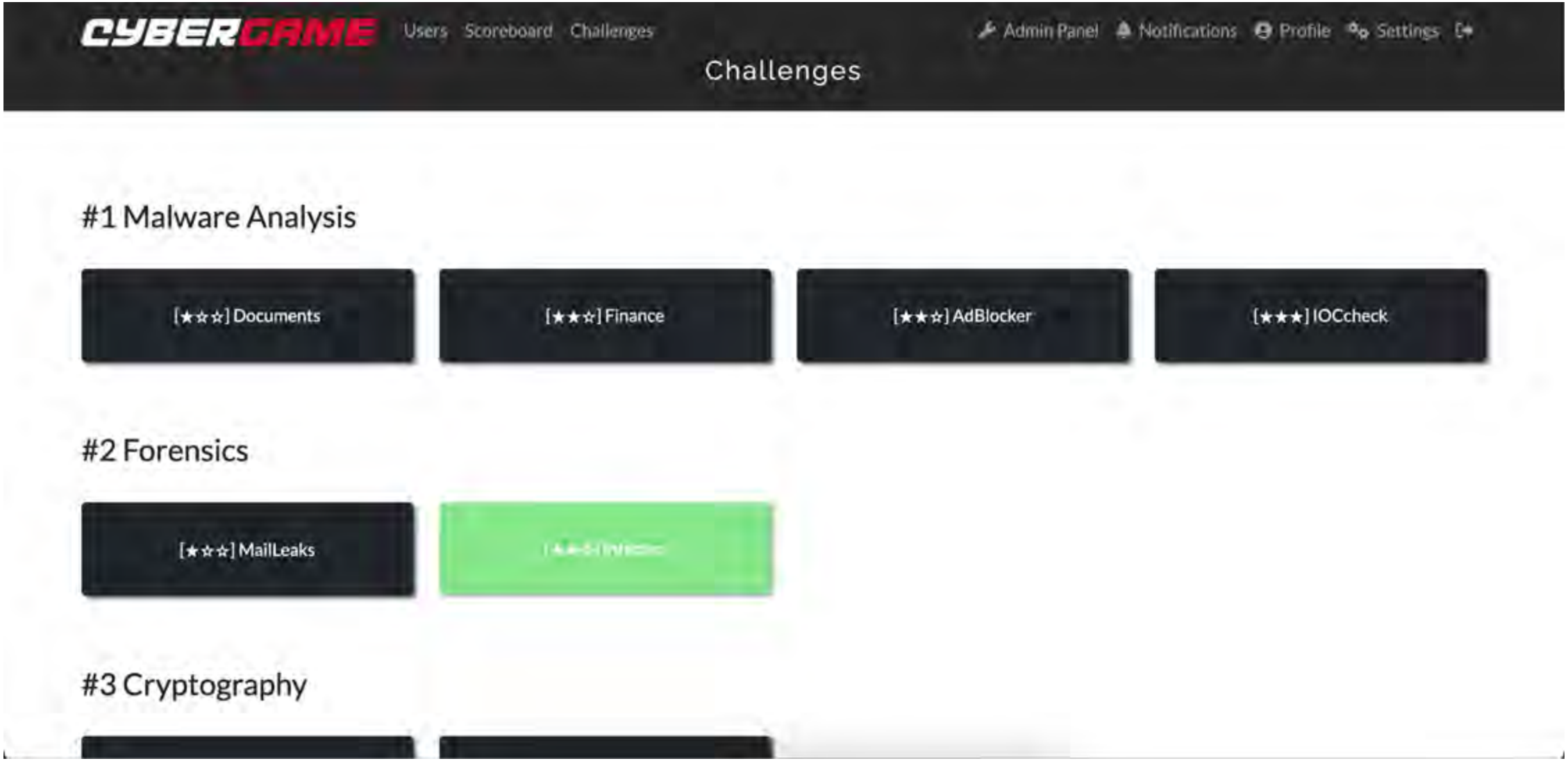


Čo bolo nové tento rok?

CYBERGAME 2024

- Zmena platformy na širšie používané CTFd
- Nová vetva "Ofenzívna bezpečnosť"
- Viac interaktívnych scenárov

Náhľad


CYBERGAME
Users
Scoreboard
Challenges
Admin Panel
Notifications
Profile
Settings
Challenges
#1 Malware Analysis
[★☆☆] Documents
[★★☆] Finance
[★★☆] AdBlocker
[★★★] IOCcheck
#2 Forensics
[★☆☆] MailLeaks
#3 Cryptography

Čo plánujeme do budúcna?

- Viac scenárov na ofenzívnu bezpečnosť
- Vyššia interaktívnosť scenárov
- Zvýšenie obtiažnosti "3 hviezdičkových" scenárov

Finále ECSC 2023, Hamar, Nórsko (Vikingskipet)

Team Czechia a Team Slovakia

Čo je to European Cyber Security Challenge ?

- 2-dňové finále súťaže národných tímov členských krajín EÚ a hostí
- Onsite/online úlohy - CTF (Capture The Flag)
  - Jeopardy
  - Attack & Defense
- Národný tím pozostáva z 10 členov, ktorých nominuje každá krajina
- Zúčastniť sa môžu hráči od 15 do 25 rokov v rozdelení na juniorov (do 20r.) a seniorov (21-25 r.)
- Hostiteľom je vždy jedna z krajín EÚ, aktivitu zastrešuje ENISA (každý štát má svojho zástupcu v Riadiacom výbore ECSC)
- 8.-11.10 2024 Turín, Taliansko - 40 krajín – 40 tímov – 400 mladých „hekerov“

Spolufinancovaný Európskou úniou

Team Slovakia 2022 Viedeň, Rakúsko
Team Slovakia 2023 Hamar, Nórsko

Ako vzniká Team Slovakia?

- Máj 2024 : výber 15 úspešných riešiteľov CyberGame do 25 rokov
- Jún 2024 : účasť na medzinárodnom bootcampe vo Viedni (10 zúčastnených štátov, prezentácie, workshopy, teambuilding a spoločné CTF)
- Júl – september 2024 : 6 vzdelávacích/tréningových bootcampov v kaštieli v Brunovciach a výber finálovej desiatky, národného tímu „Team Slovakia 2024"
  - Prezentácie expertov, workshopy, domáce úlohy
  - Online CTF turnaje
- August 2024 : medzinárodný bootcamp v Brunovciach za účasti slovenských, českých a rakúskych hráčov
  - Spoločný tím pod názvom „Habsburg Anarchy" získal v online CTF Sekai 6. miesto z viac ako 1200 zaregistrovaných tímov
- Október (7.-12.10 2024) : finále European Cybersecurity Challenge v Turíne
- November 2024 – marec 2025 : pravidelné bootcampy členov výberu, ako aj členov Team Slovakia 2022 a 2023, príprava Team Slovakia 2025

Za oponou projektu ...

- Life-changer – účasť v národnom tíme môže byť životnou zmenou pre niektorých účastníkov
- Obrovská šanca objaviť mladé talenty a povzbudiť ich k tomu, aby sa venovali kariére v oblasti kybernetickej bezpečnosti.
- Úžasné odhodlanie, nadšenie a vášeň manažérov a koučov tímov, víkendy strávené prácou s tímom na bootcampoch.

Team Slovakia 2024 a partneri

NCC-SK

SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Financované Európskou úniou

Vyjadrené názory a postoje sú názormi a vyhláseniami autorov a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za nich nepreberajú žiadnu zodpovednosť.

Kybernetická bezpečnosť 2024
Verejnosť SR

Výsledky reprezentatívneho online prieskumu

Zber dát: 25. 7. – 31. 7. 2024

1. ZARIADENIA POUŽÍVANÉ V DOMÁCNOSTI

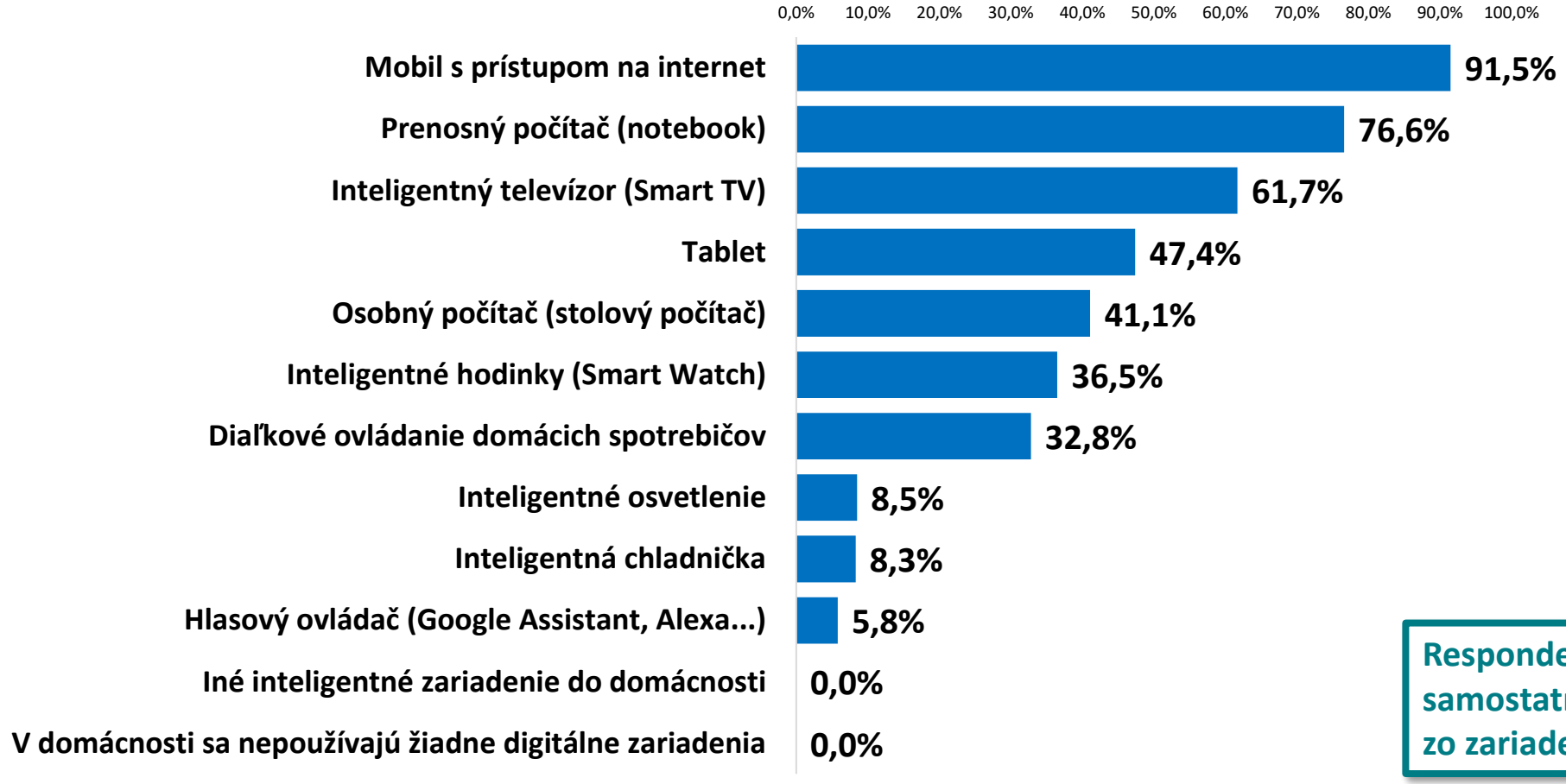
„Ktoré z nasledujúcich zariadení sú používané vo vašej domácnosti? Označte prosím tie zariadenia, ktoré sa vo vašej domácnosti nachádzajú v počte minimálne 1ks.“

1. ZARIADENIA POUŽÍVANÉ V DOMÁCNOSTI

„Ktoré z nasledujúcich zariadení sú používané vo vašej domácnosti? Označte prosím tie zariadenia, ktoré sa vo vašej domácnosti nachádzajú v počte minimálne 1ks.“

Odpovede všetkých respondentov (online zručných členov online panelu)

N= 1000

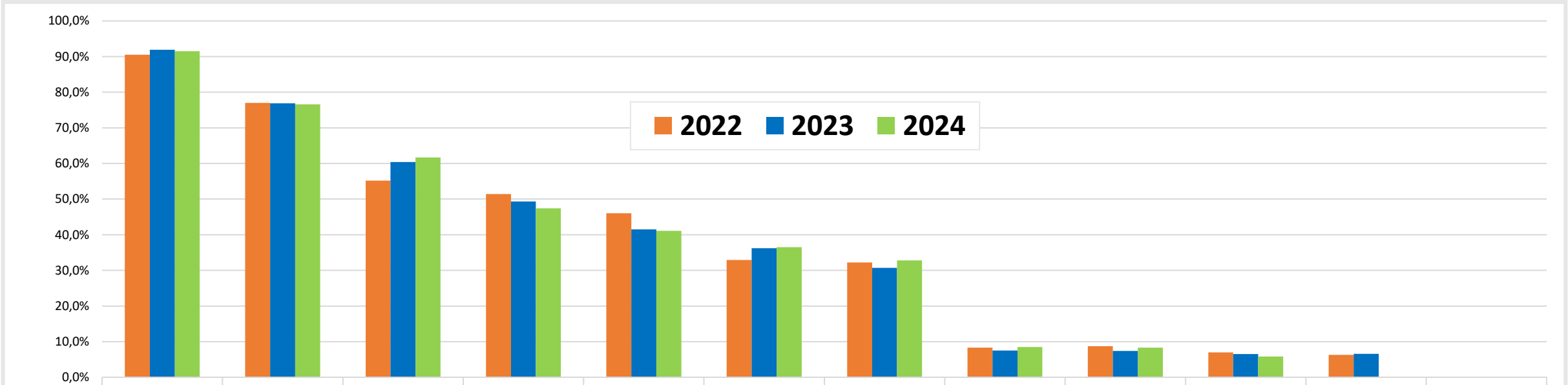


Respondent sa vyjadroval samostatne ku každému zo zariadení.

1. ZARIADENIA POUŽÍVANÉ V DOMÁCNOSTI

„Ktoré z nasledujúcich zariadení sú používané vo vašej domácnosti? Označte prosím tie zariadenia, ktoré sa vo vašej domácnosti nachádzajú v počte minimálne 1ks.“

Porovnanie s minulými prieskumami

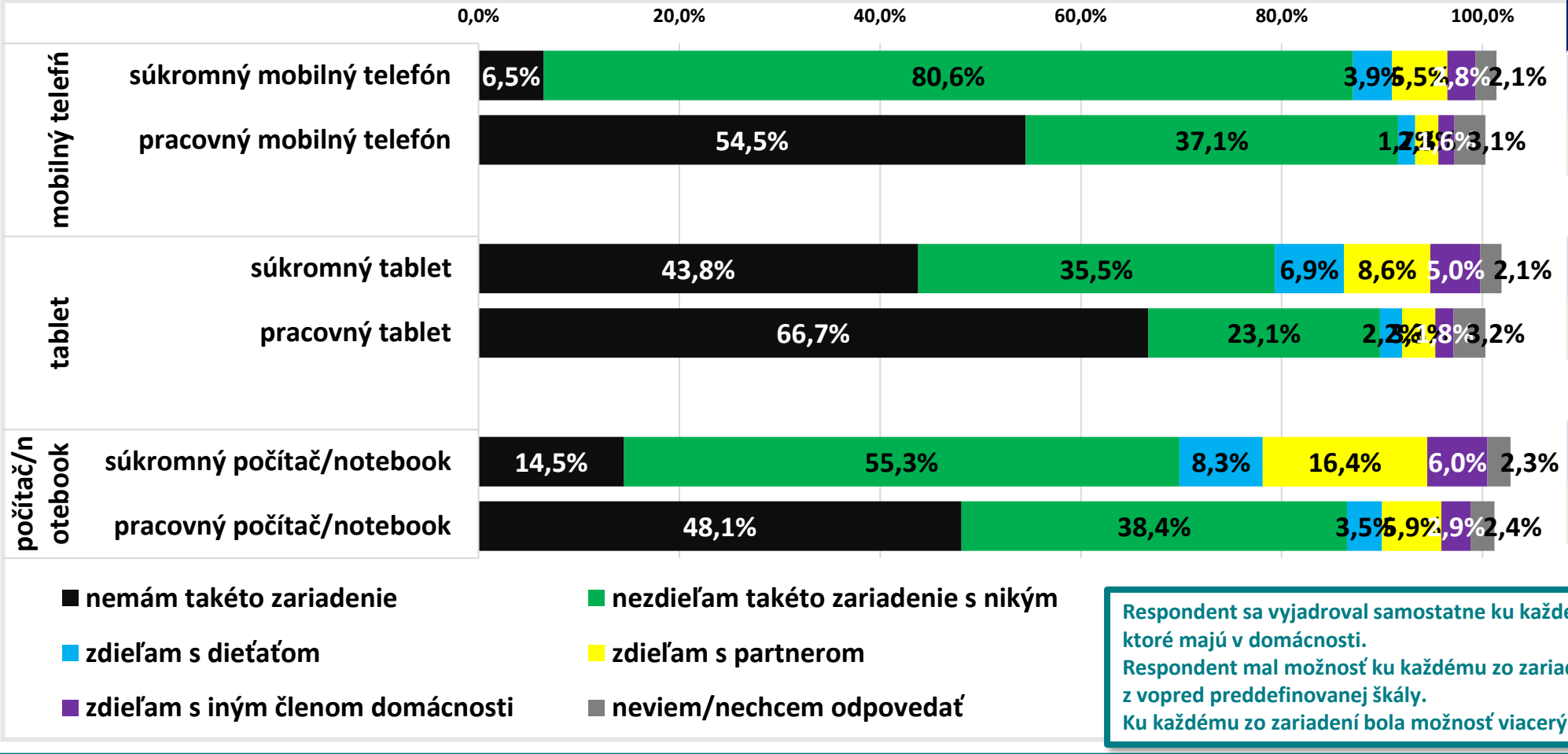


	Mobil s prístupom na internet	Prenosný počítač (notebook)	Inteligentný televízor (Smart TV)	Tablet	Osobný počítač (stolový počítač)	Inteligentné hodinky (Smart Watch)	Diaľkové ovládanie domácich spotrebičov	Inteligentné osvetlenie	Inteligentná chladnička	Hlasový ovládač (Google Assistant a pod.)	Iné inteligentné zariadenie	V domácnosti sa nepoužívajú žiadne
2022	90,5%	77,0%	55,2%	51,4%	46,0%	32,9%	32,2%	8,3%	8,7%	7,0%	6,3%	0,0%
2023	91,9%	76,9%	60,4%	49,3%	41,5%	36,2%	30,7%	7,5%	7,4%	6,5%	6,6%	0,0%
2024	91,5%	76,6%	61,7%	47,4%	41,1%	36,5%	32,8%	8,5%	8,3%	5,8%	0,0%	0,0%

3. ZDIEĽANIE ZARIADENÍ S INÝMI ČLENMI DOMÁCNOSTI

N= 1000

„S ktorými z iných členov domácnosti zdieľate nasledujúce elektronické zariadenia:
Ku každému odpovedajte podľa škály:“
Odpovede všetkých respondentov



ZDIEĽAM
12,2%
5,6%
20,5%
7,3%
30,7%
12,3%

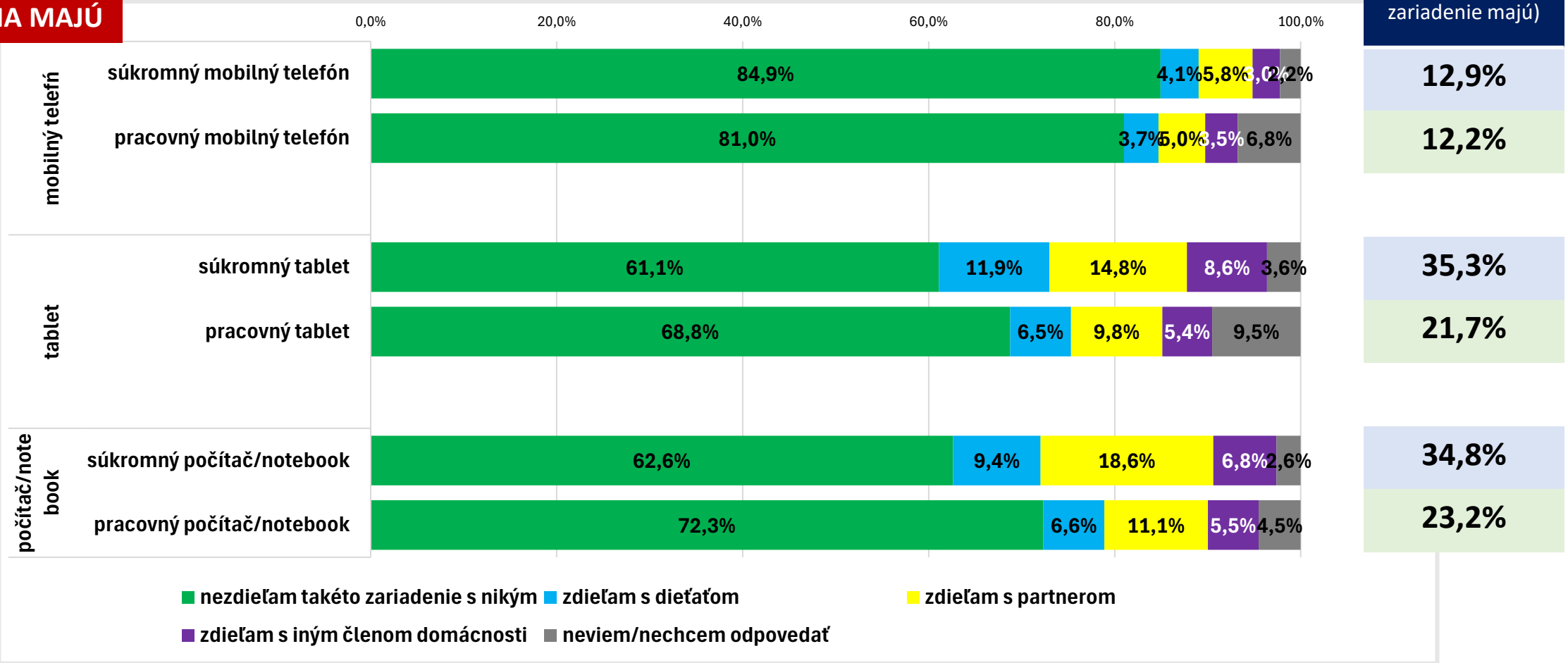
Respondent sa vyjadroval samostatne ku každému zo zariadení, ktoré majú v domácnosti.
Respondent mal možnosť ku každému zo zariadení vybrať odpovede z vopred preddefinovanej škály.
Ku každému zo zariadení bola možnosť viacerých odpovedí.

3. ZDIEĽANIE ZARIADENÍ S INÝMI ČLENMI DOMÁCNOSTI

PREPOČET LEN Z RESPONDENTOV, KTORÍ DANÝ TYP ZARIADENIA MAJÚ

„S ktorými z iných členov domácnosti zdieľate nasledujúce elektronické zariadenia: Ku každému odpovedajte podľa škály:“

Odpovede všetkých respondentov

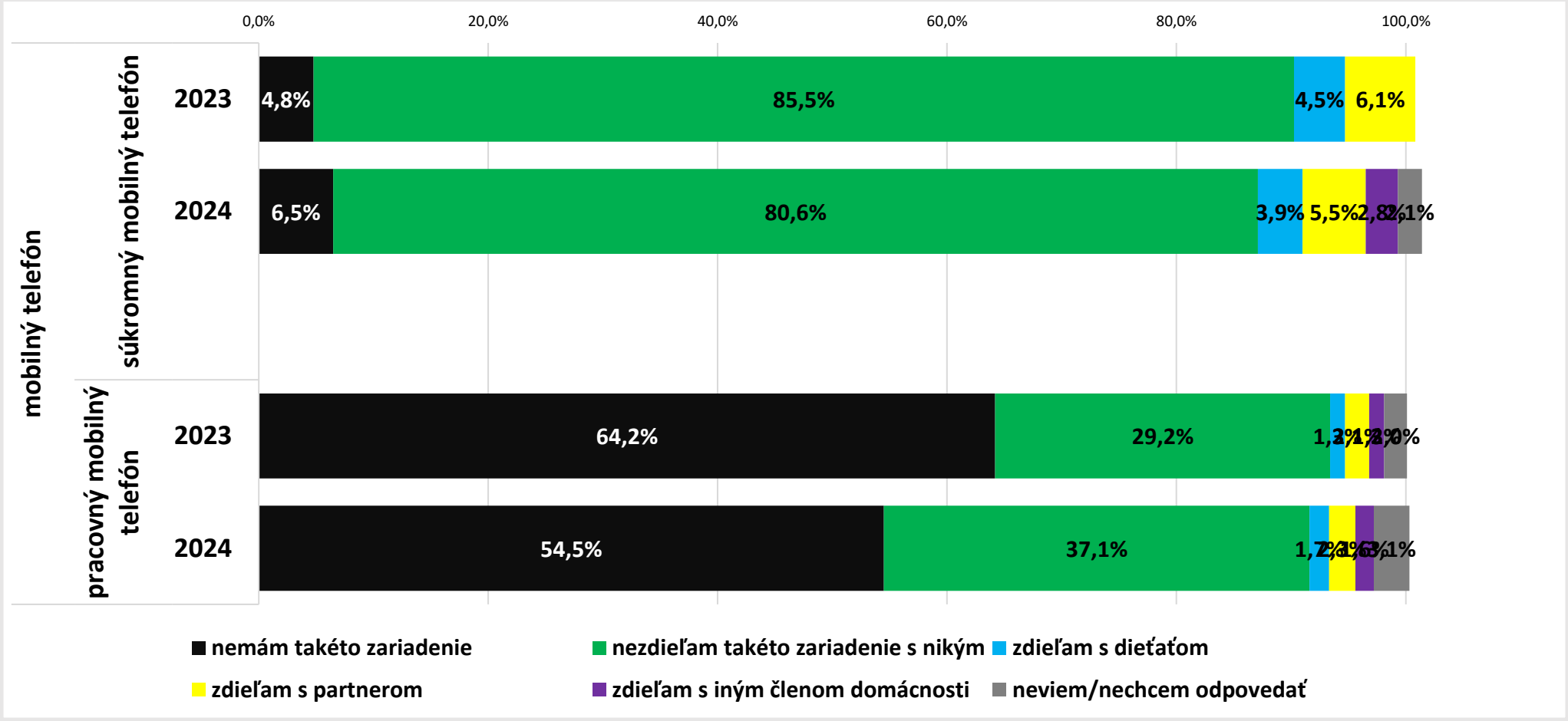


ZDIEĽAM (z tých, ktorí dané zariadenie majú)
12,9%
12,2%
35,3%
21,7%
34,8%
23,2%

3. ZDIEĽANIE ZARIADENÍ S INÝMI ČLENMI DOMÁCNOSTI

„S ktorými z iných členov domácnosti zdieľate nasledujúce elektronické zariadenia: Ku každému odpovedajte podľa škály:“

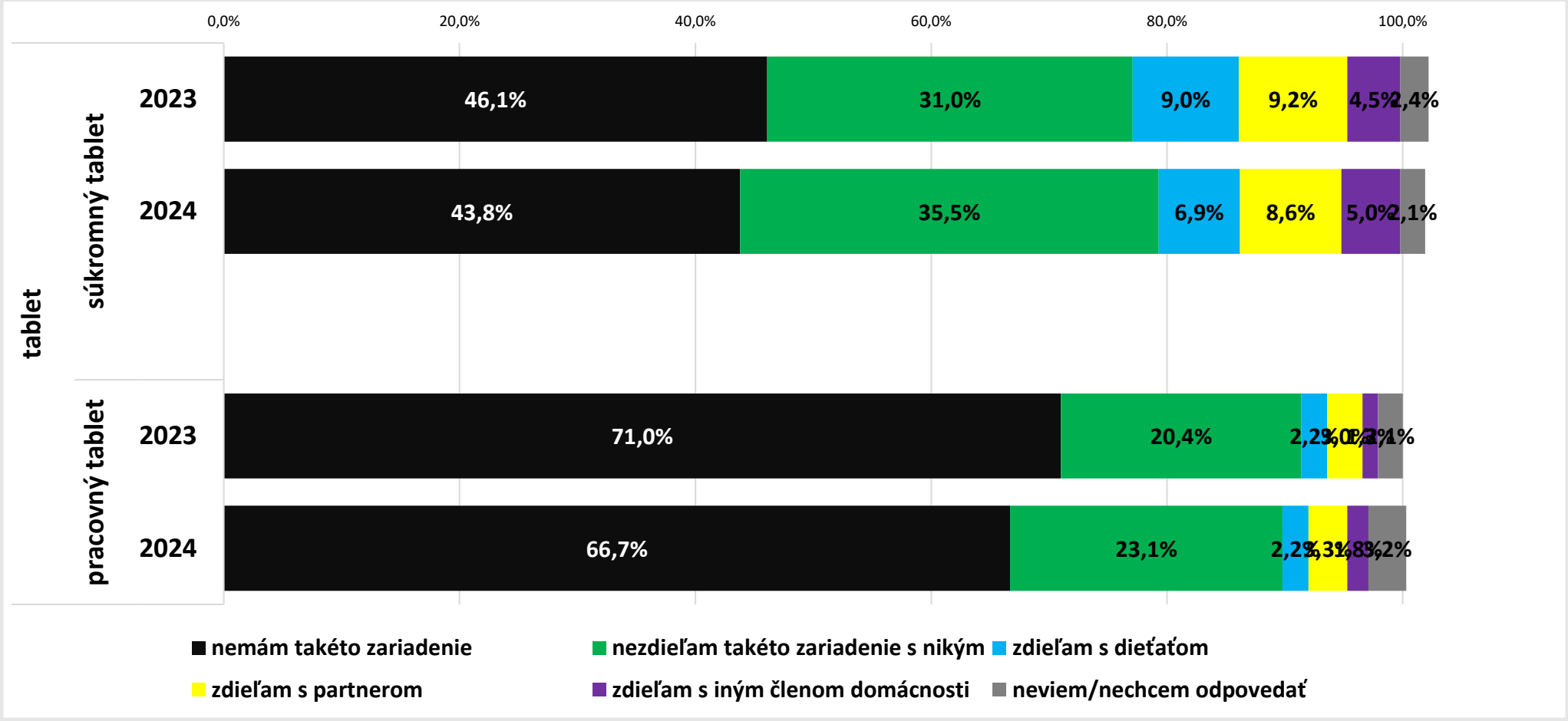
Porovnanie s minulými prieskumami



3. ZDIEĽANIE ZARIADENÍ S INÝMI ČLENMI DOMÁCNOSTI

„S ktorými z iných členov domácnosti zdieľate nasledujúce elektronické zariadenia: Ku každému odpovedajte podľa škály:“

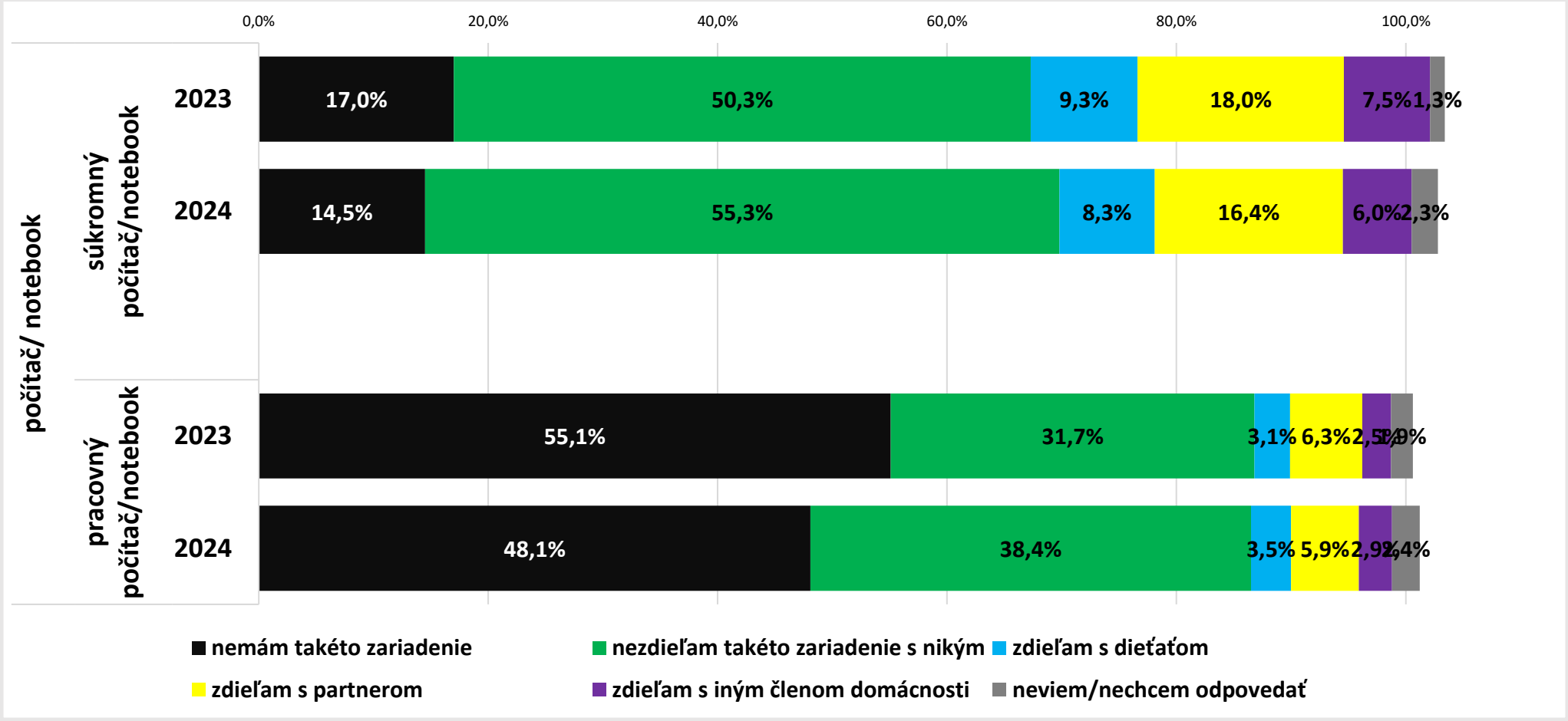
Porovnanie s minulými prieskumami



3. ZDIEĽANIE ZARIADENÍ S INÝMI ČLENMI DOMÁCNOSTI

„S ktorými z iných členov domácnosti zdieľate nasledujúce elektronické zariadenia: Ku každému odpovedajte podľa škály:“

Porovnanie s minulými prieskumami



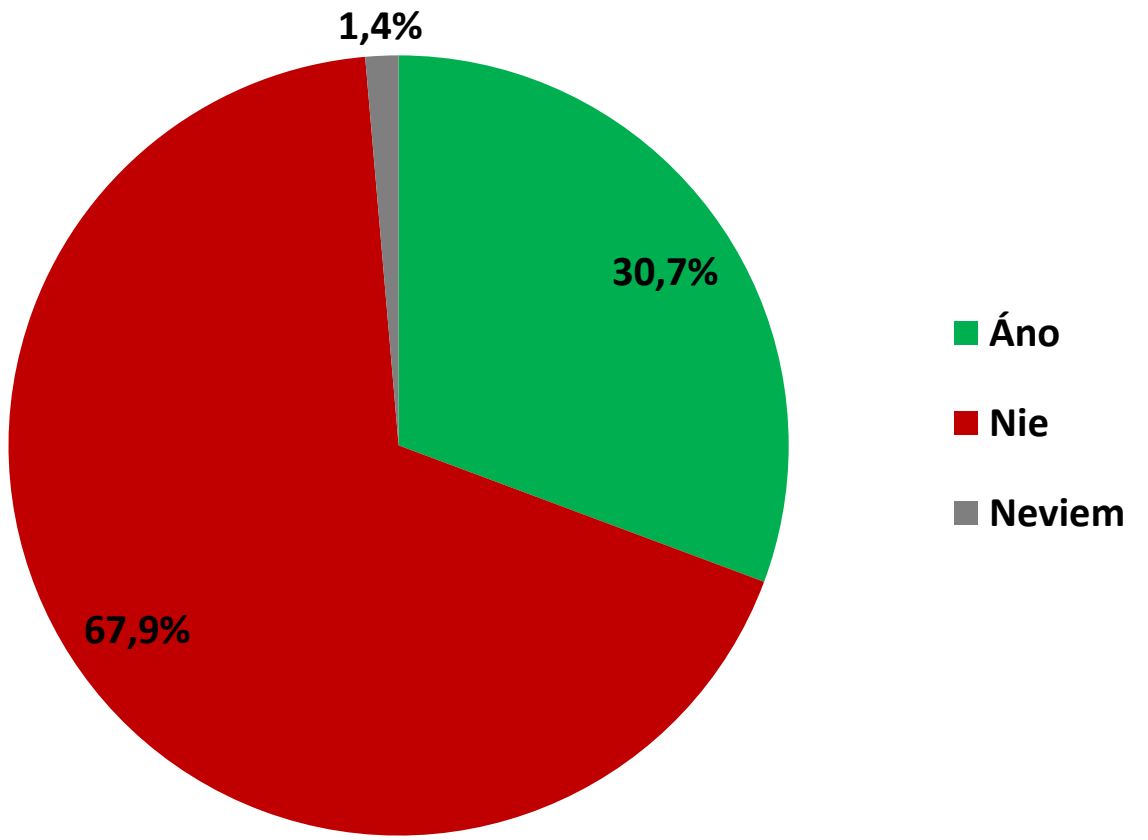
4. NÁSTROJE NA KONTROLU DETÍ V DIGITÁLNOM PRIESTORE

„Používate vo vašej domácnosti nástroje na kontrolu detí v digitálnom priestore (rodičovská kontrola)?“

4. NÁSTROJE NA KONTROLU DETÍ V DIGITÁLNOM PRIESTORE

„Používate vo vašej domácnosti nástroje na kontrolu detí v digitálnom priestore (rodičovská kontrola)?“
Odpovede respondentov, ktorí uviedli, že s nimi v domácnosti žijú deti

N= 344



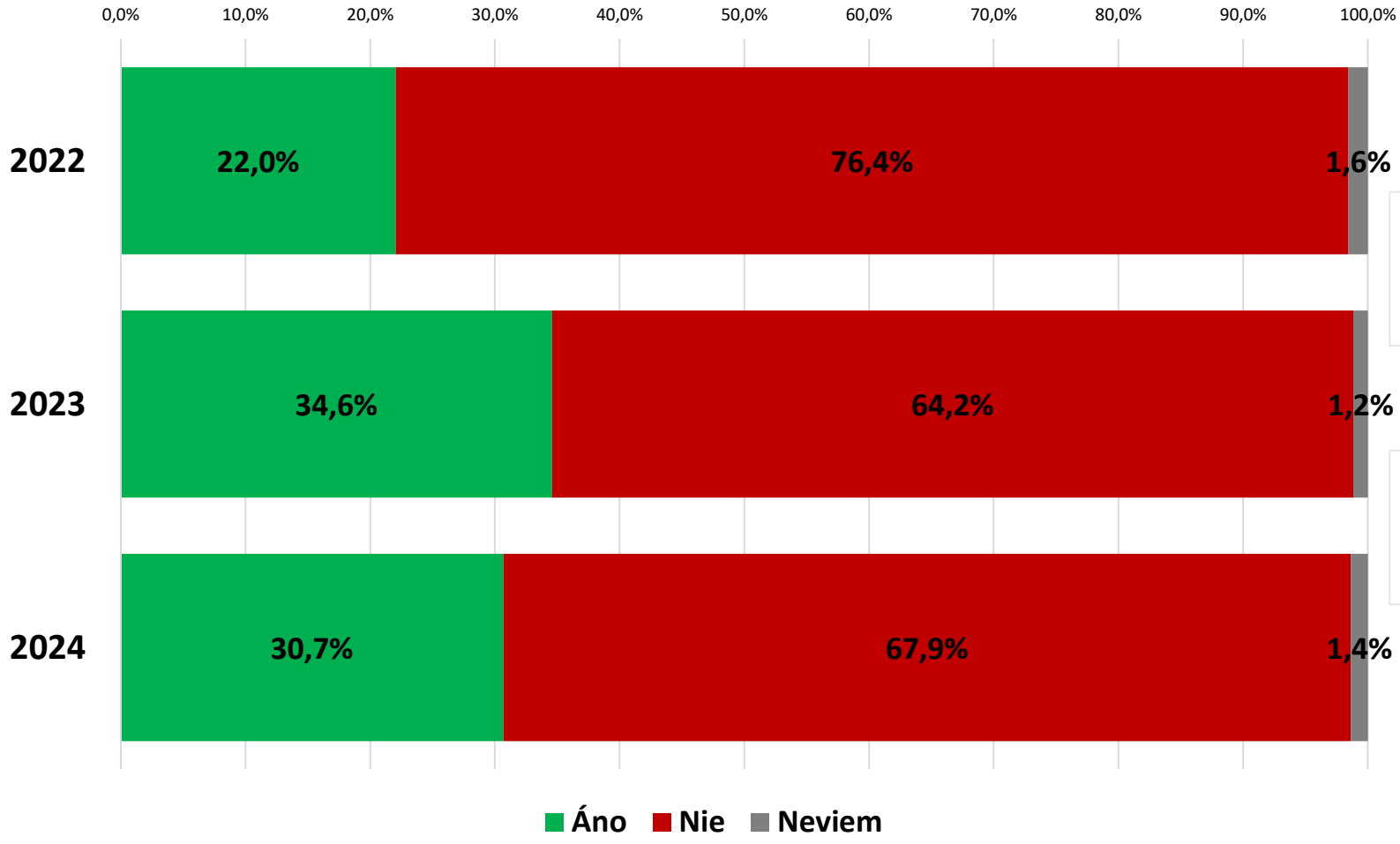
Respondent mal možnosť vybrať odpoveď z vopred preddefinovanej škály odpovedí.

Škála bola respondentom predkladaná v rotovanom poradí.

Možnosť len jednej odpovede.

4. NÁSTROJE NA KONTROLU DETÍ V DIGITÁLNOM PRIESTORE

„Používate vo vašej domácnosti nástroje na kontrolu detí v digitálnom priestore (rodičovská kontrola)?“
Porovnanie s minulými prieskumami



Medzi **2022 a 2023:**
Nárast o 12,6
percentuálneho bodu.

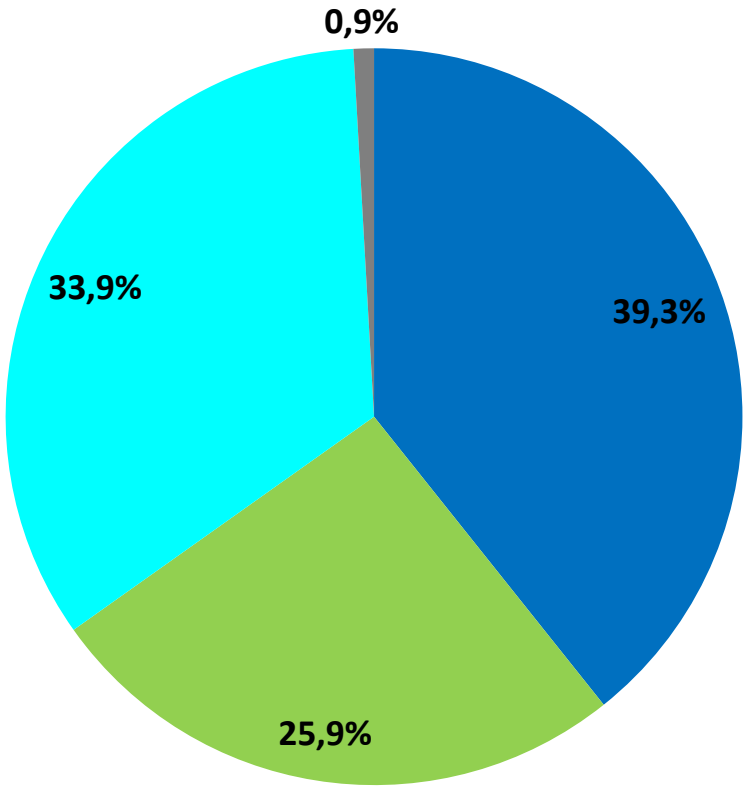
Medzi **2023 a 2024**:
Pokles o 3,9
percentuálneho bodu.

4. NÁSTROJE NA KONTROLU DETÍ V DIGITÁLNOM PRIESTORE

„Akým spôsobom sa táto rodičovská kontrola u vás uplatňuje?“
Odpovede respondentov, ktorí uviedli, že s nimi v domácnosti žijú deti a používajú nástroje na kontrolu detí v digitálnom priestore

N=112

Malá veľkosť vzorky!



- Monitorovací režim (t. j. aktivity dieťaťa len pozorujete)
- Reštriktívny režim (t. j. obmedzujete čas pri/na zariadení a aktivity, ktoré môže dieťa vykonávať)
- Kombinované monitorovanie aj obmedzenia
- Neviem/ Nechcem odpovedať

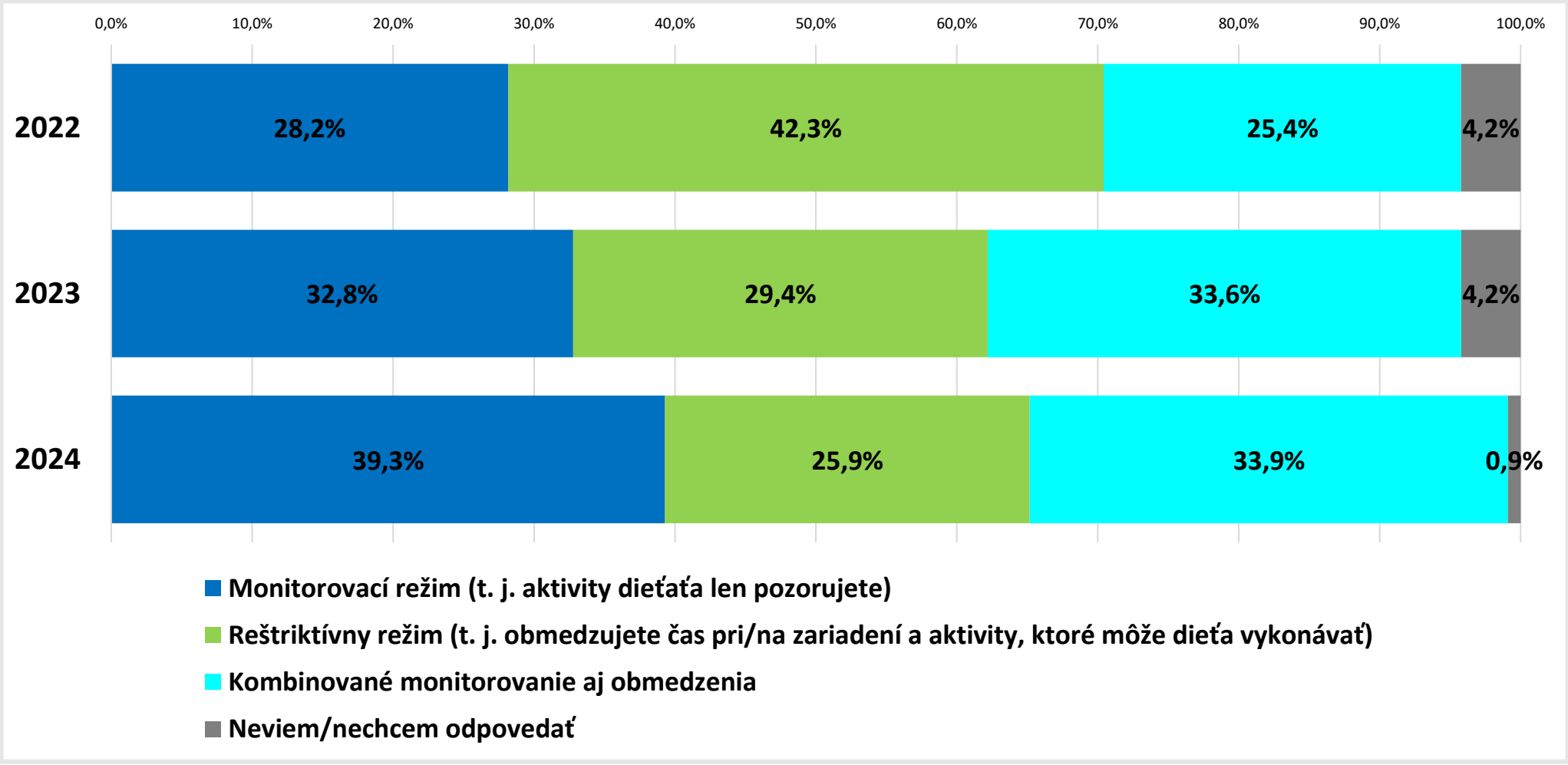
Respondent mal možnosť vybrať odpoveď z vopred preddefinovaných variantov odpovedí.

Varianty odpovedí boli respondentom predkladané v rotovanom poradí.

Možnosť len jednej odpovede.

4. NÁSTROJE NA KONTROLU DETÍ V DIGITÁLNOM PRIESTORE

„Akým spôsobom sa táto rodičovská kontrola u vás uplatňuje?“
Porovnanie s minulými prieskumami



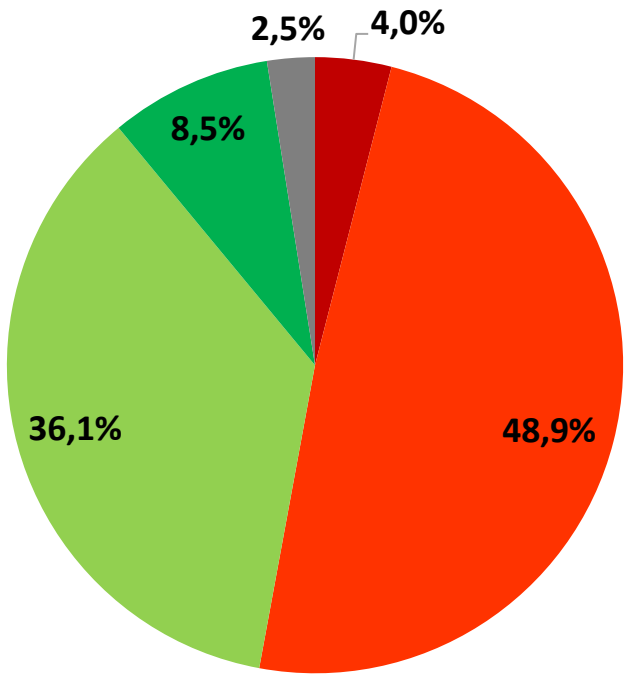
5. DIGITÁLNE ZRUČNOSTI

„Aké sú vaše digitálne zručnosti? Ako pristupujete k práci s elektronickými informáciami?“

5. DIGITÁLNE ZRUČNOSTI

„Aké sú vaše digitálne zručnosti? Ako pristupujete k práci s elektronickými informáciami?“
Odpovede všetkých respondentov

N= 1000



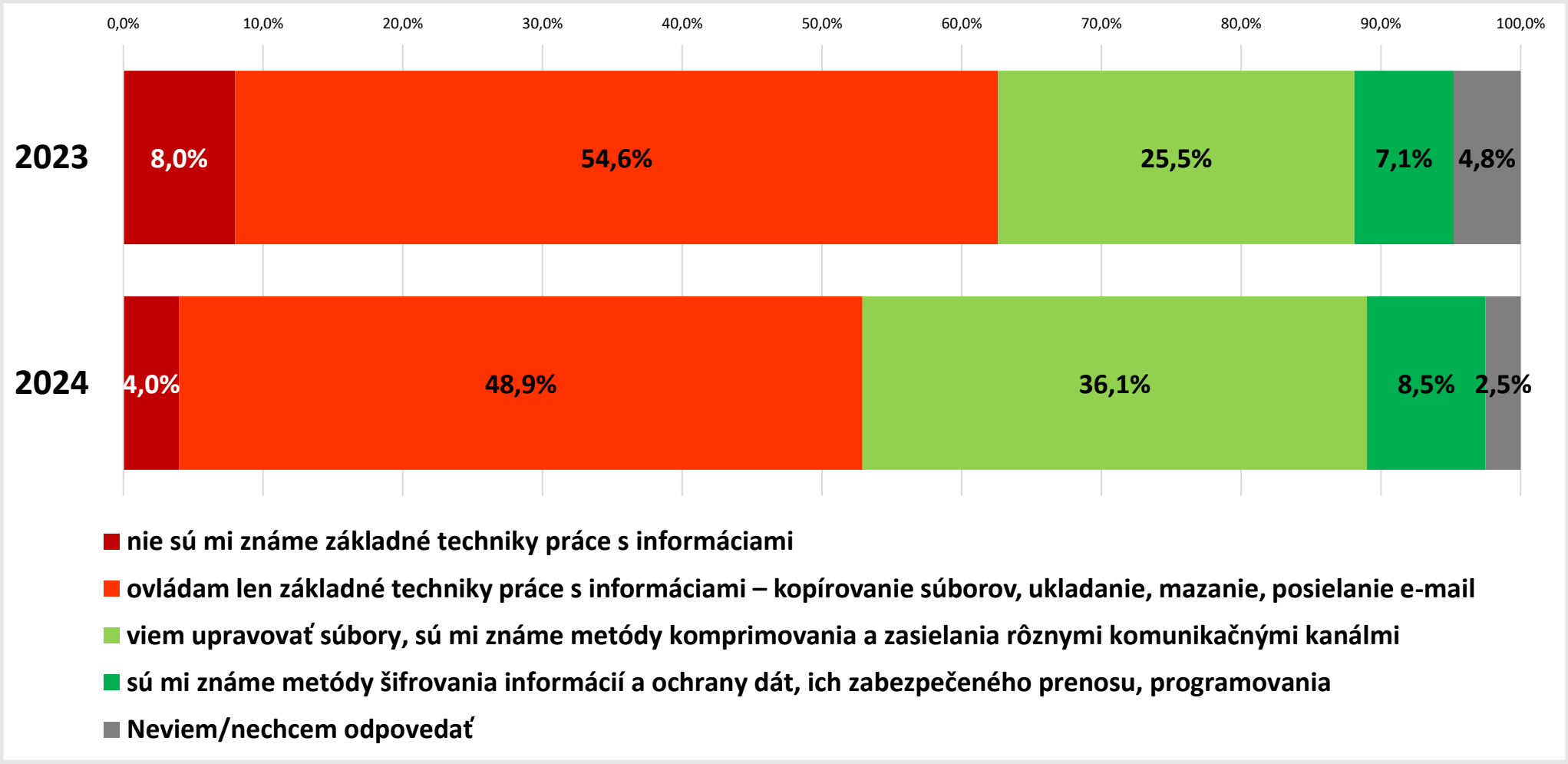
Respondent mal možnosť vybrať odpoveď z vopred preddefinovaného zoznamu variantov.

Varianty boli respondentom predkladané v rotovanom poradí.

Možnosť viacerých odpovedí.

5. DIGITÁLNE ZRUČNOSTI

„Aké sú vaše digitálne zručnosti? Ako pristupujete k práci s elektronickými informáciami?“
Porovnanie s predchádzajúcim prieskumom



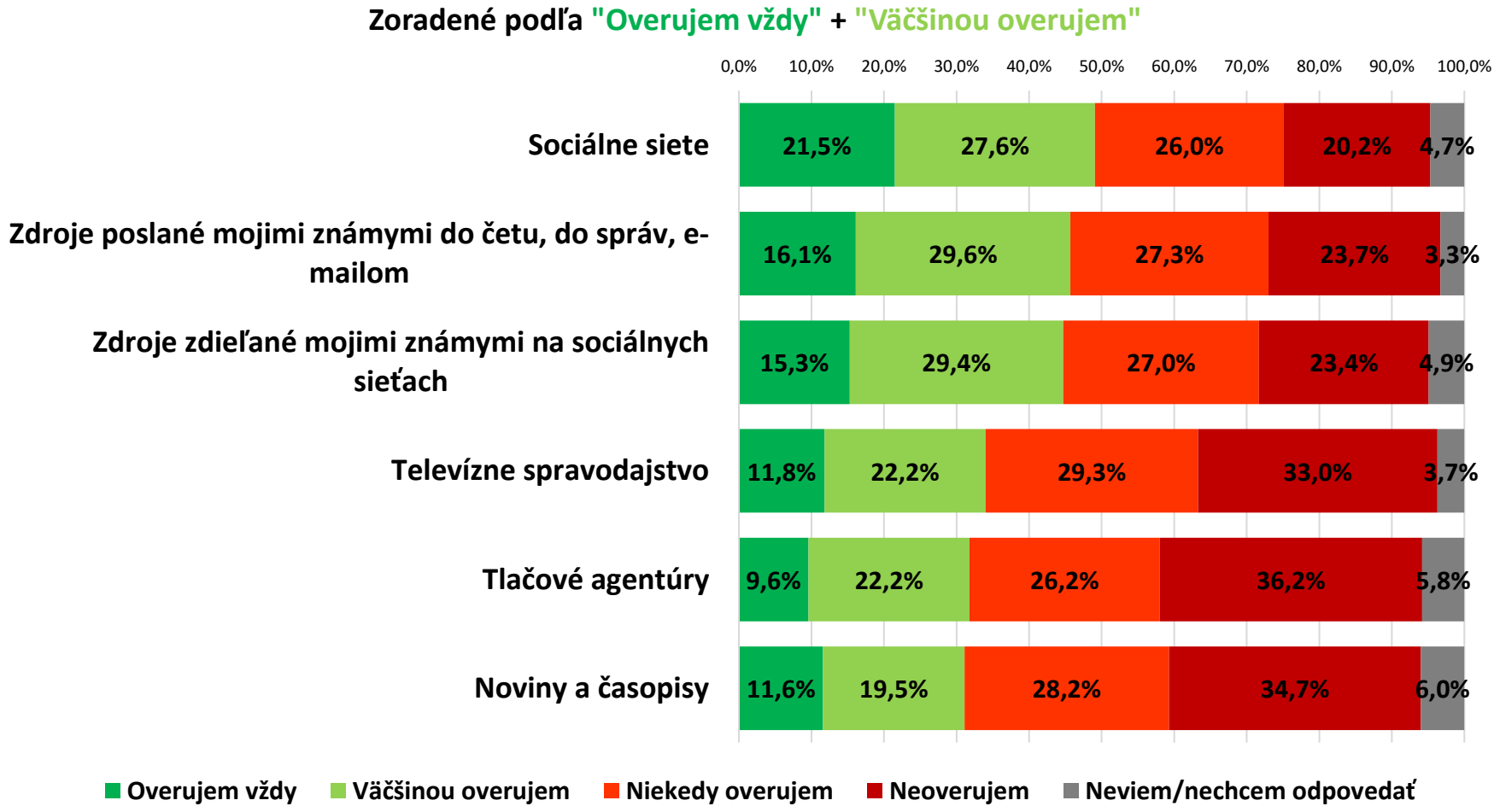
6. OVEROVANIE INFORMÁCIÍ

„Overujete si informácie ktoré ste získali z nasledujúcich zdrojov? Odpovedajte podľa škály.“

6. OVEROVANIE INFORMÁCIÍ

„Overujete si informácie ktoré ste získali z nasledujúcich zdrojov? Odpovedajte podľa škály.“
Odpovede všetkých respondentov

N= 1000



Respondent mal možnosť vybrať odpoveď z vopred preddefinovanej škály ku každému zo zdrojov.

Zdroje boli respondentom predkladané v rotovanom poradí.

Možnosť len jednej odpovede ku každému zo zdrojov. .

7. ZNALOSŤ HROZIEB KYBERNETICKEJ BEZPEČNOSTI

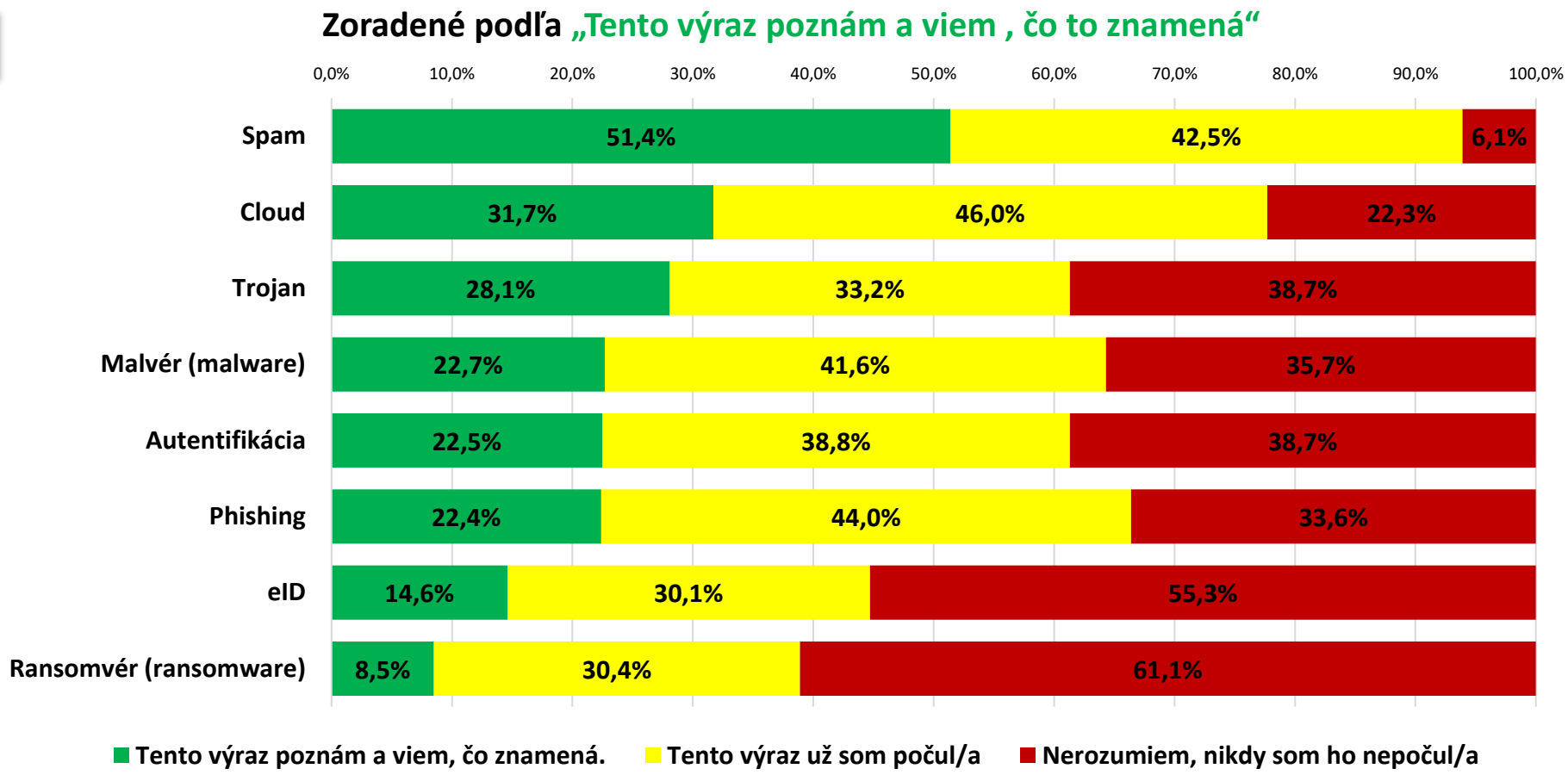
„Do akej miery ste sa stretli s nasledovnými výrazmi z počítačového prostredia? Ku každému výrazu prosím zaznačte.“

7. ZNALOSŤ HROZIEB KYBERNETICKEJ BEZPEČNOSTI

„Do akej miery ste sa stretli s nasledovnými výrazmi z počítačového prostredia? Ku každému výrazu prosím zaznačte.“

Odpovede všetkých respondentov

N= 1000



Respondent sa vyjadroval samostatne ku každému z výrazov.

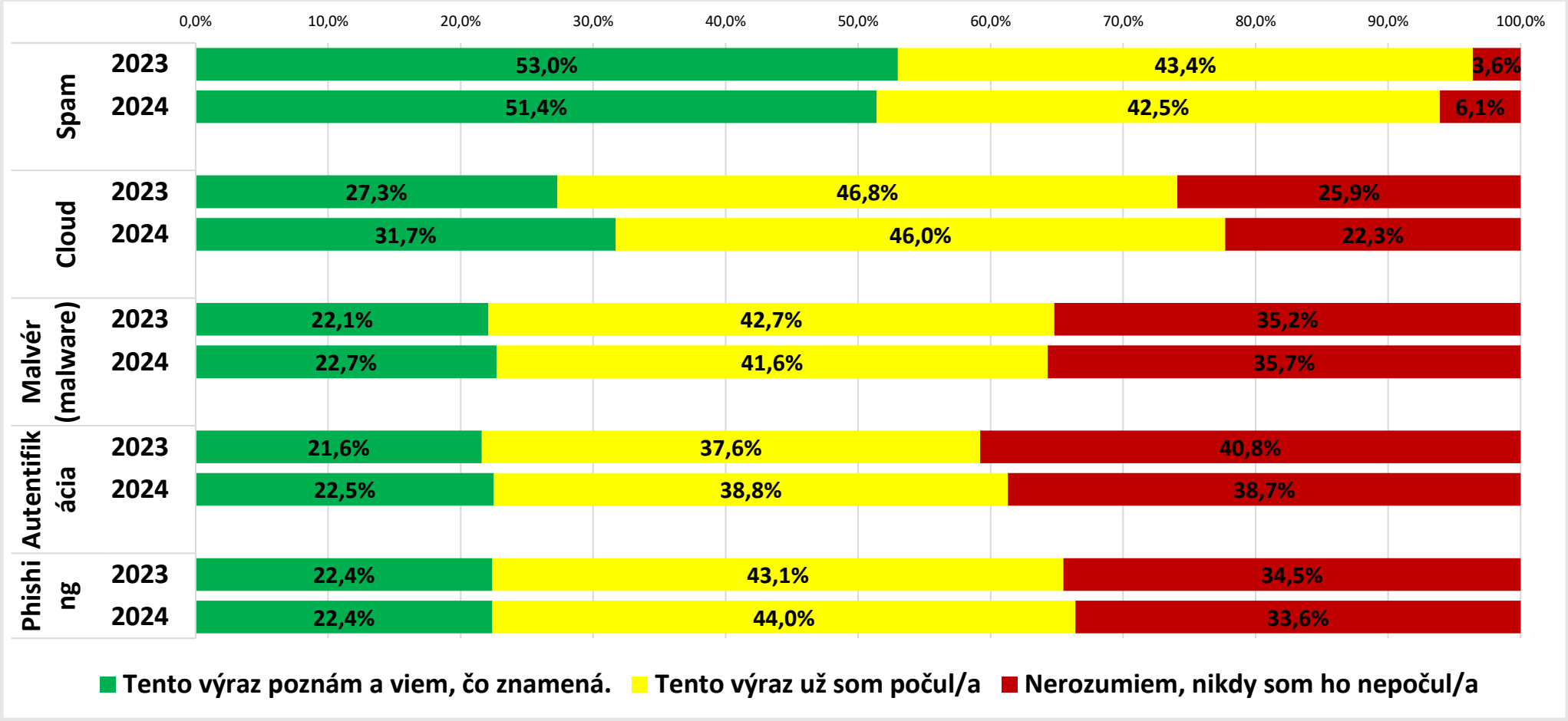
Respondent mal možnosť ku každému z výrazov vybrať odpoveď z vopred preddefinovanej škály.

Ku každému z výrazov bola možnosť len jednej odpovede.

7. ZNALOSŤ HROZIEB KYBERNETICKEJ BEZPEČNOSTI

„Do akej miery ste sa stretli s nasledovnými výrazmi z počítačového prostredia? Ku každému výrazu prosím zaznačte.“

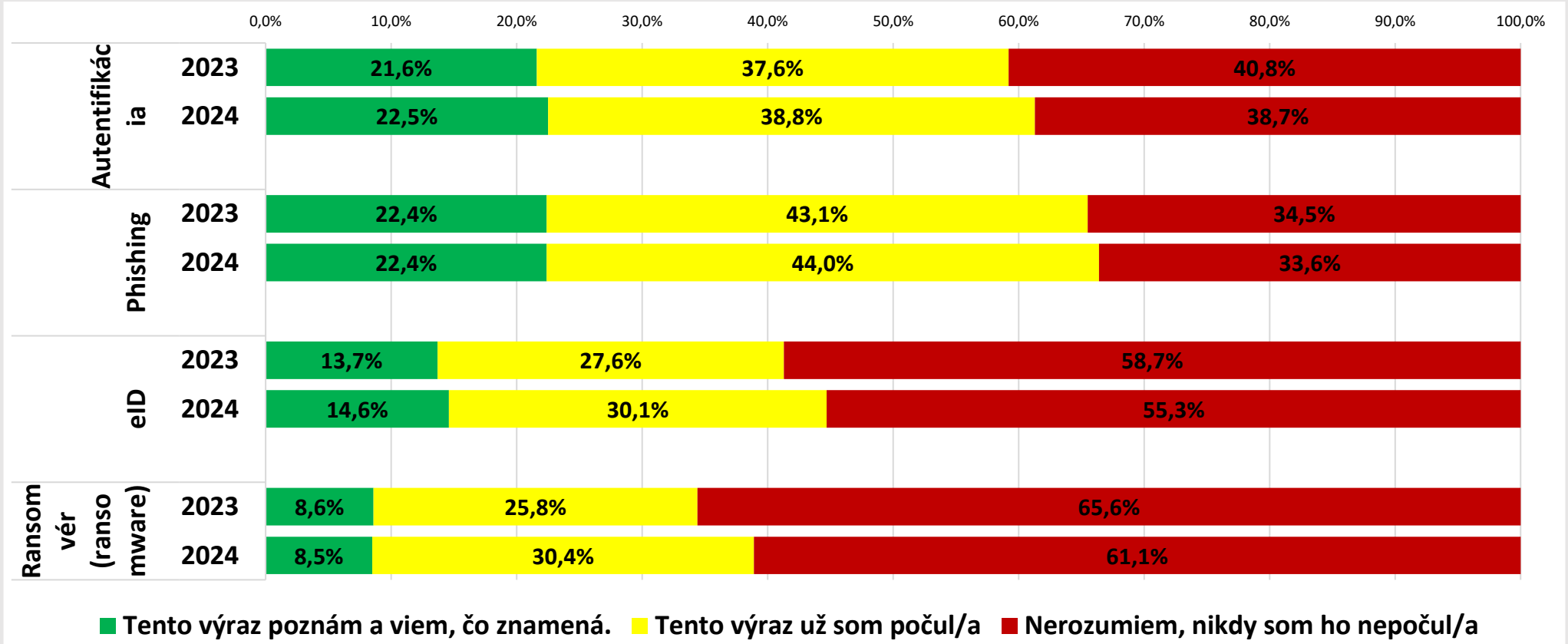
Porovnanie s predchádzajúcim prieskumom



7. ZNALOSŤ HROZIEB KYBERNETICKEJ BEZPEČNOSTI

„Do akej miery ste sa stretli s nasledovnými výrazmi z počítačového prostredia? Ku každému výrazu prosím zaznačte.“

Porovnanie s predchádzajúcim prieskumom



Pozn.: Výraz „Trojan“ nebol v minulom prieskume skúmaný.

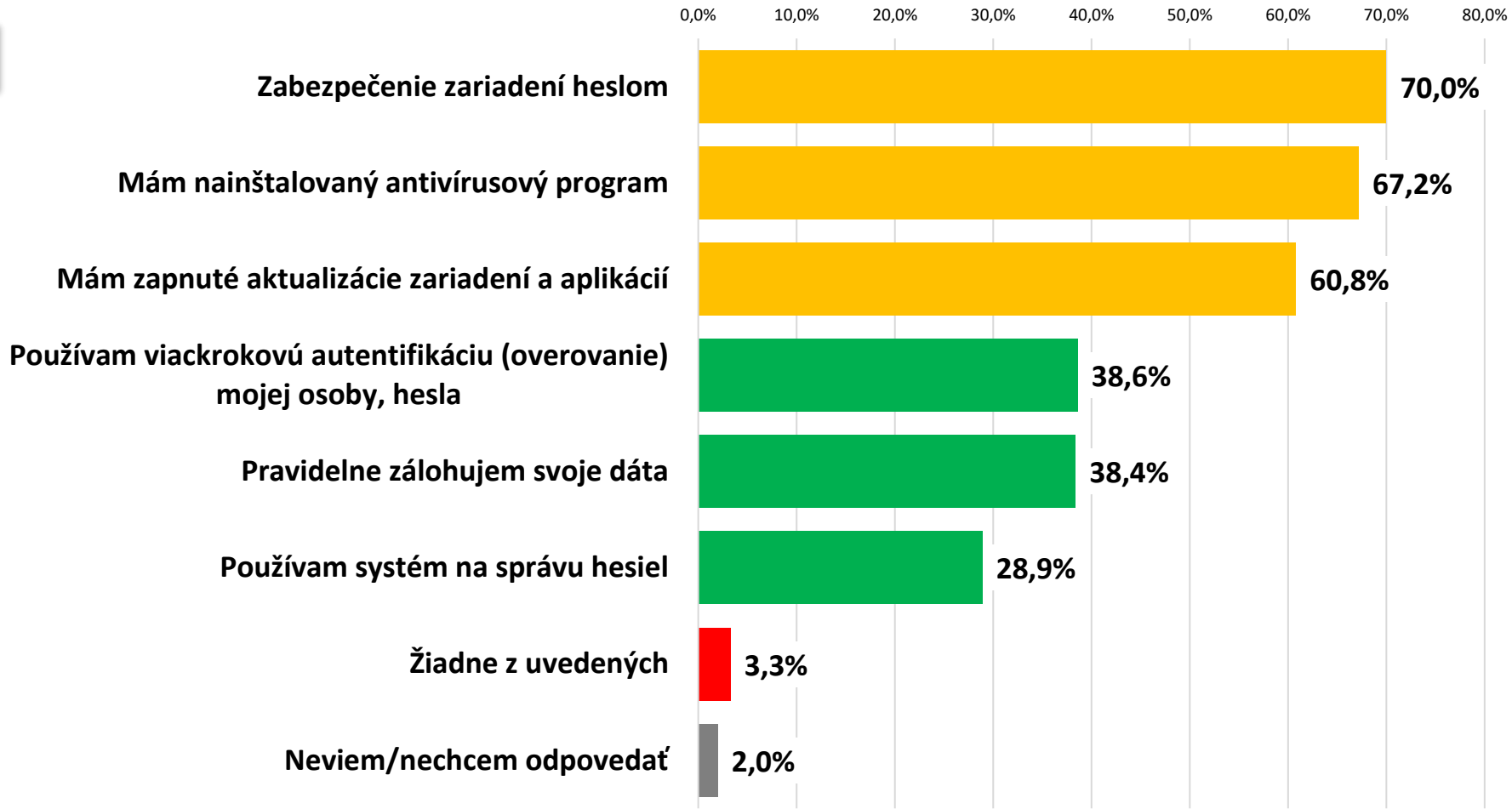
8. POUŽÍVANÉ OPATRENIA KYBERNETICKEJ BEZPEČNOSTI

„Ktoré z nasledujúcich oparení počítačovej bezpečnosti používate?“

8. POUŽÍVANÉ OPATRENIA KYBERNETICKEJ BEZPEČNOSTI

„Ktoré z nasledujúcich oparení počítačovej bezpečnosti používate?“
Odpovede všetkých respondentov

N= 1000



Respondent si mal možnosť vybrať odpovede z vopred preddefinovaných variantov.

Varianty boli respondentom predkladané v rotovanom poradí.

Možnosť viacerých odpovedí, preto súčet presahuje 100%.

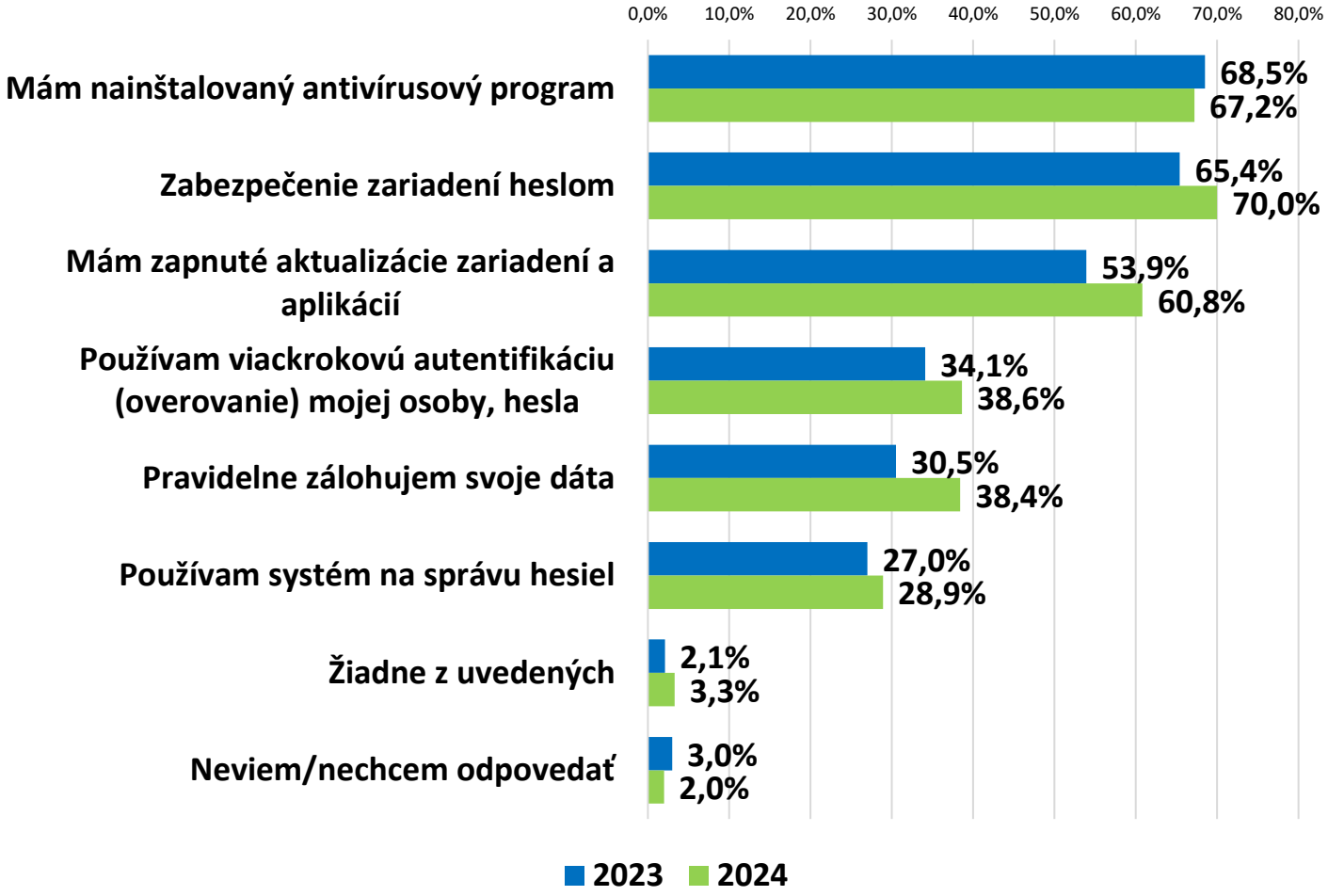
Žiadne opatrenia

Základné opatrenia

Silnejšie opatrenia

8. POUŽÍVANÉ OPATRENIA KYBERNETICKEJ BEZPEČNOSTI

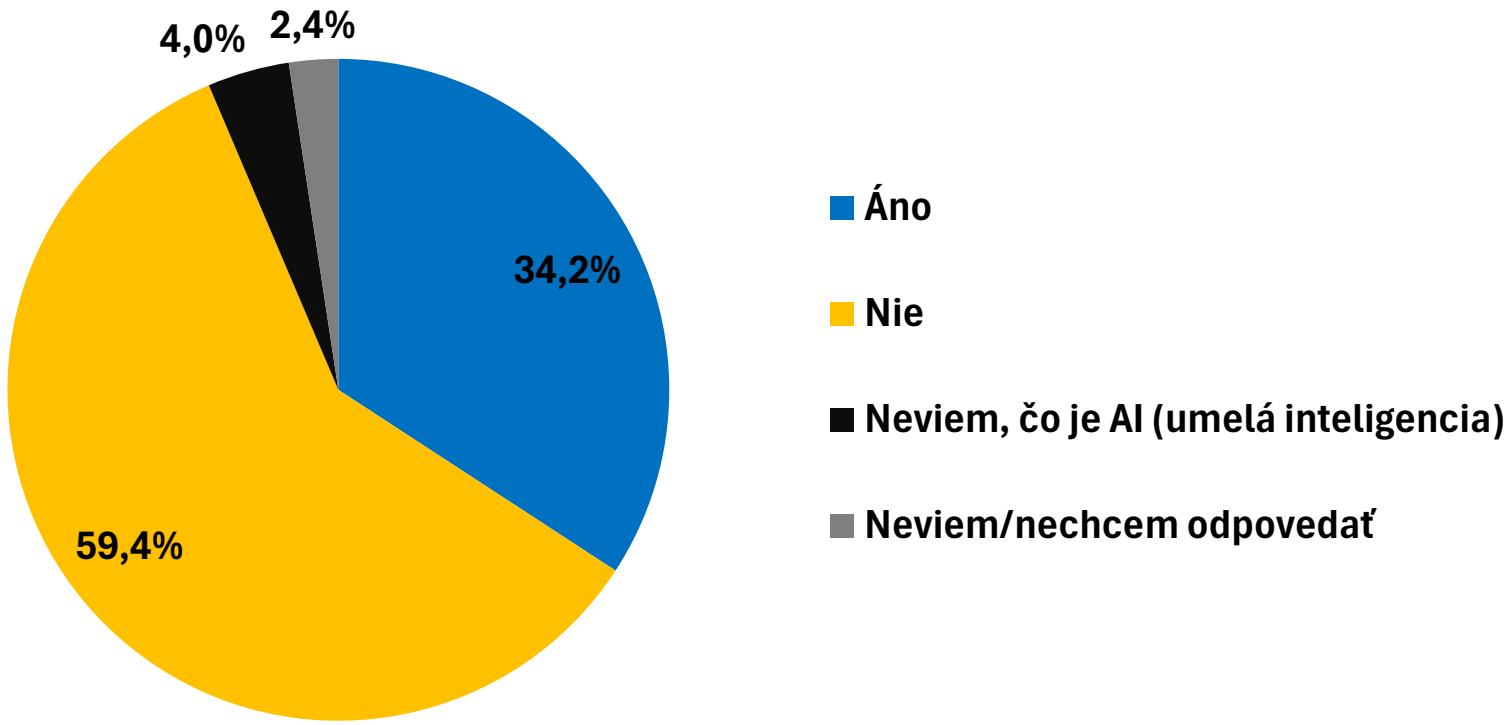
„Ktoré z nasledujúcich oparení počítačovej bezpečnosti používate?“
Porovnanie s predchádzajúcim prieskumom



9. AI – UMELÁ INTELIGENCIA

„Komunikovali ste už s umelou inteligenciou (AI)?“
Odpovede všetkých respondentov

N= 1000



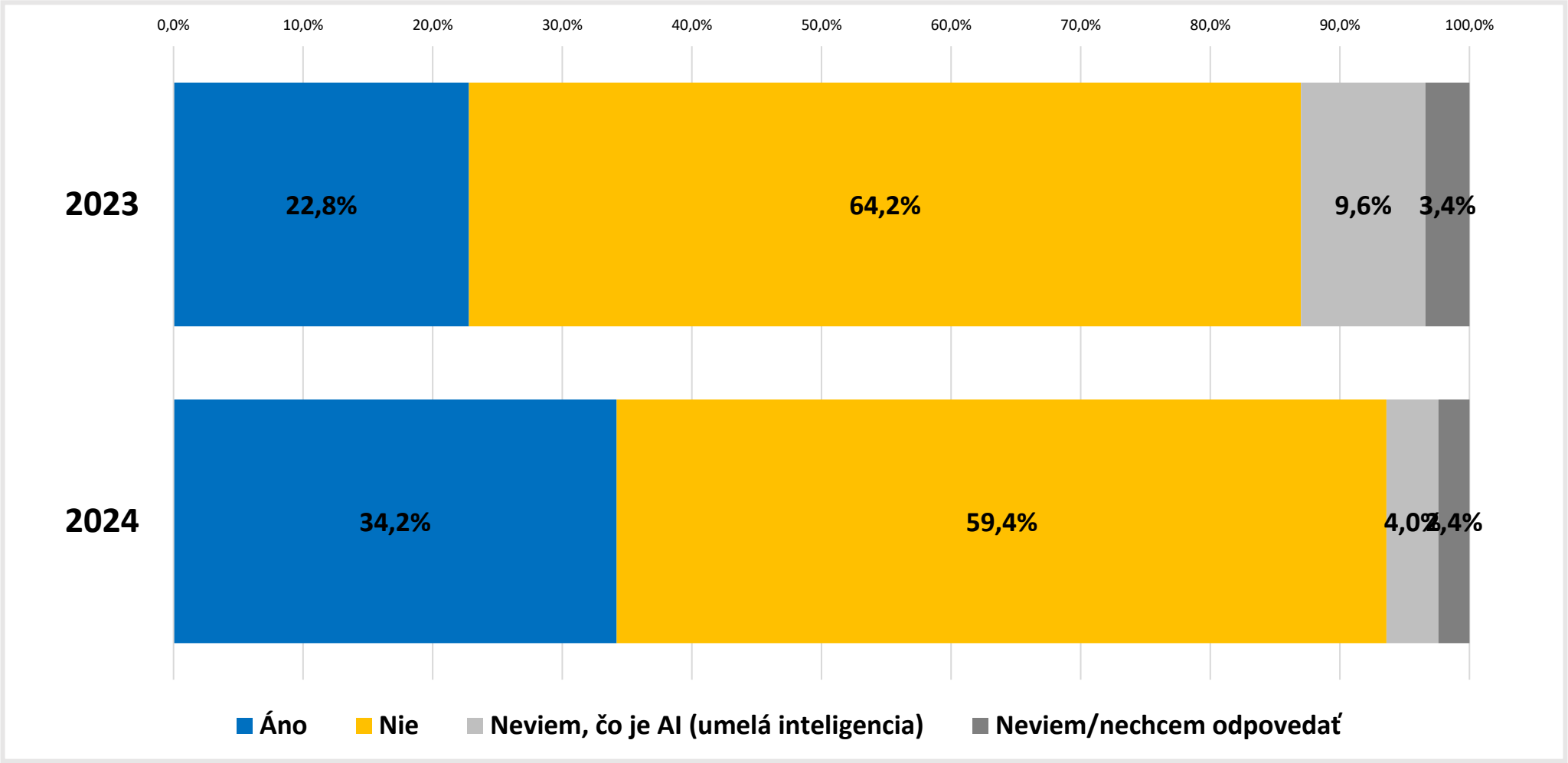
Respondent si mal možnosť vybrať odpovede z vopred preddefinovaných variantov.

Varianty boli respondentom predkladané v rotovanom poradí.

Možnosť 1 odpovede.

9. AI – UMELÁ INTELIGENCIA

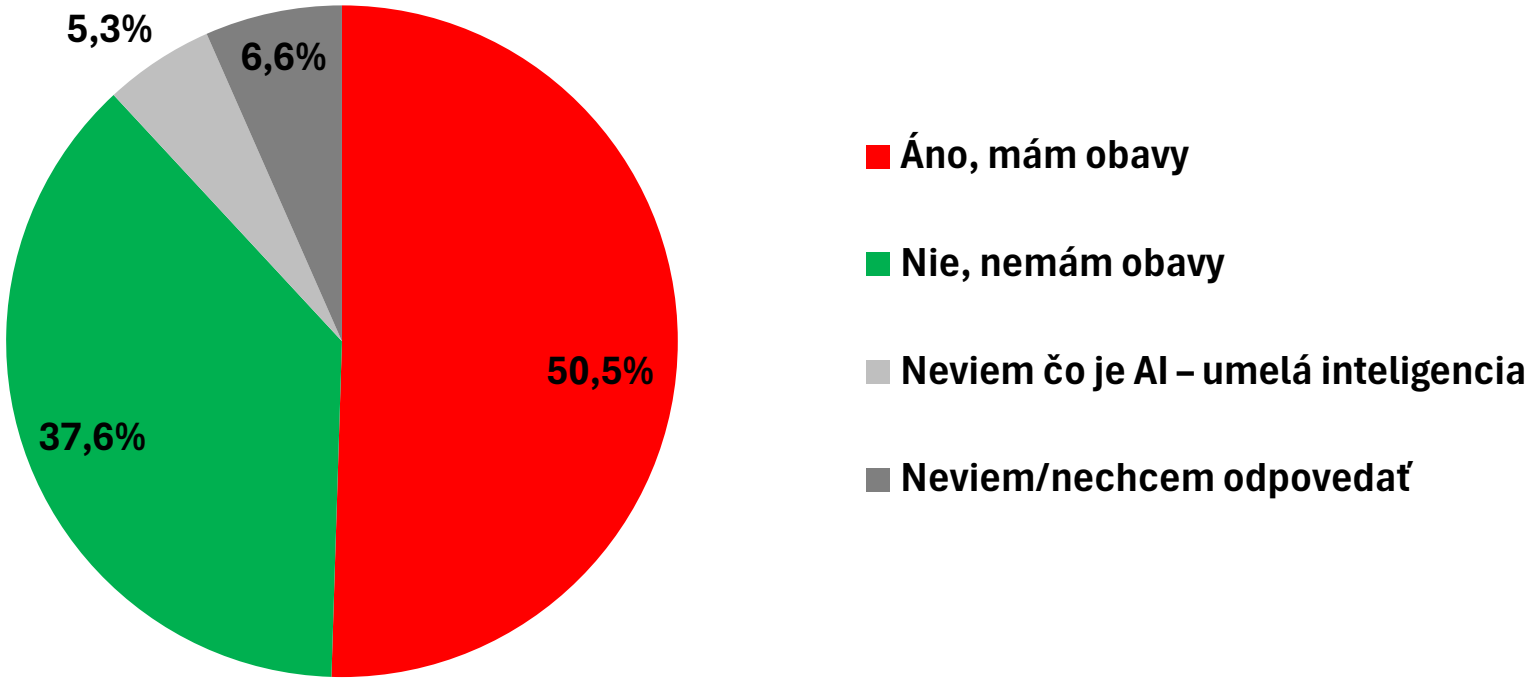
„Komunikovali ste už s umelou inteligenciou (AI)?“
Porovnanie s predchádzajúcim prieskumom



9. AI – UMELÁ INTELIGENCIA

„Máte alebo nemáte obavy z AI – umelej inteligencie?“
Odpovede všetkých respondentov

N= 1000



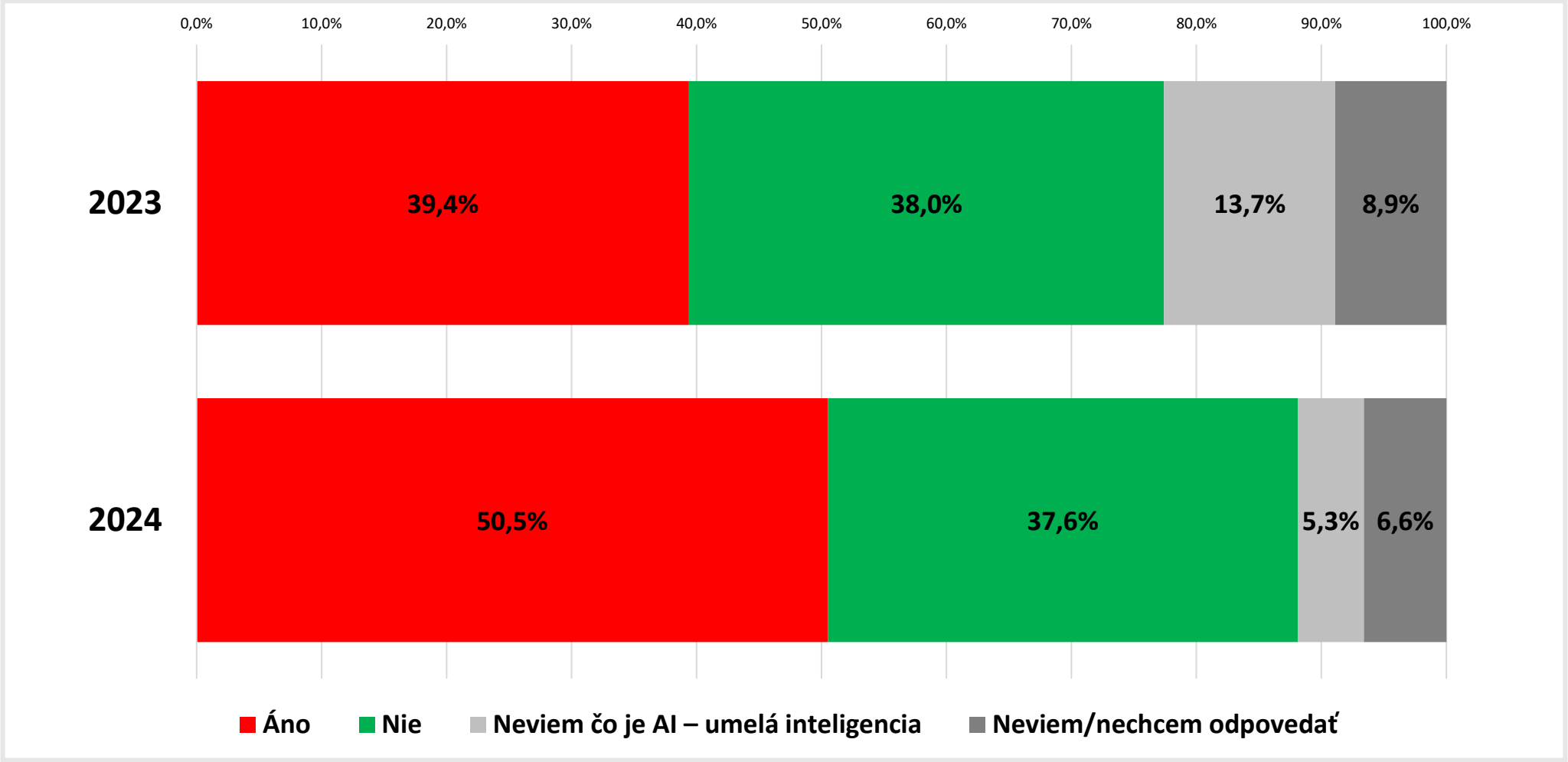
Respondent si mal možnosť vybrať odpovede z vopred preddefinovaných variantov.

Varianty boli respondentom predkladané v rotovanom poradí.

Možnosť 1 odpovede.

9. AI – UMELÁ INTELIGENCIA

„Máte alebo nemáte obavy z AI – umelej inteligencie?“
Porovnanie s predchádzajúcim prieskumom



Je vaša spoločnosť schopná odolať pokročilému útoku?

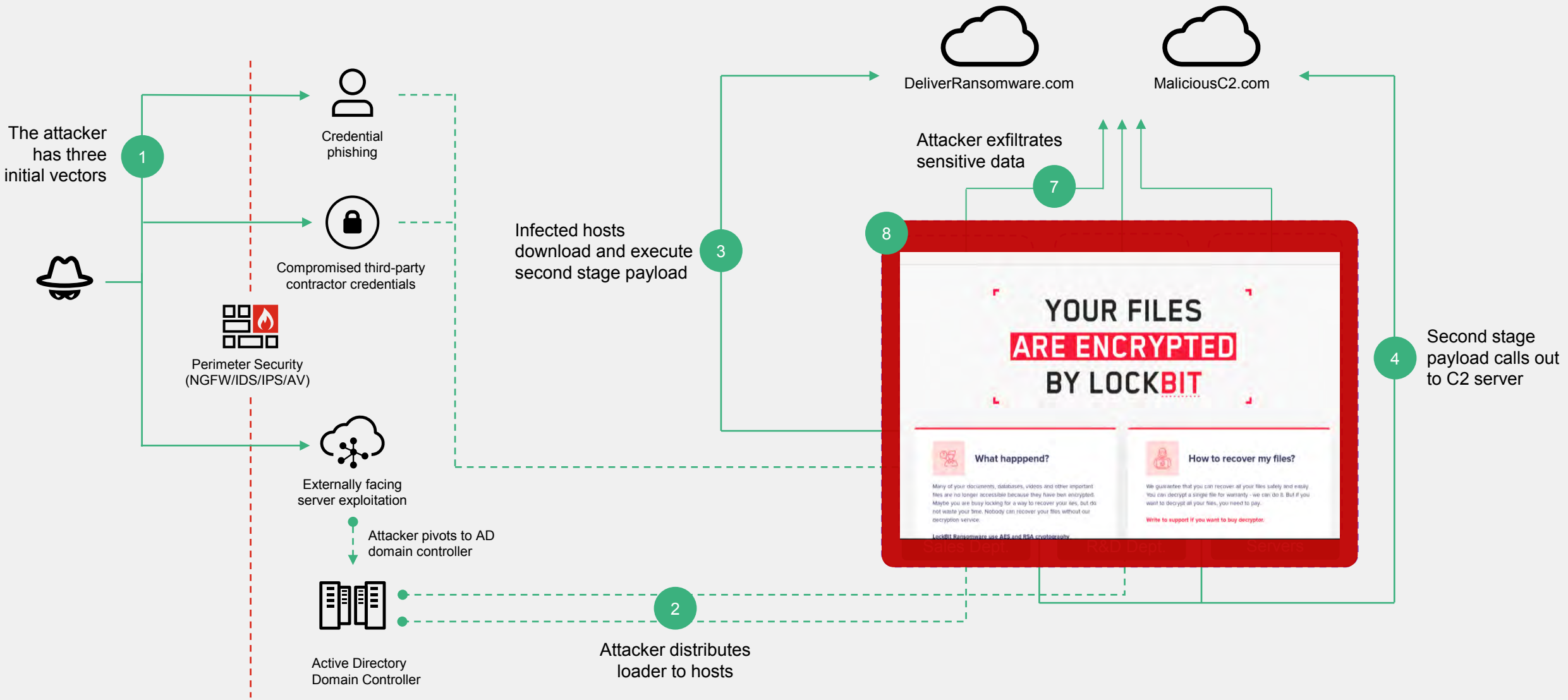
”Viem, že nič neviem.”

Sokrates (iný zápis: Sókrates, Sókratés, starogr. Σωκράτης; * asi 469 pred Kr.)

Juraj Belko

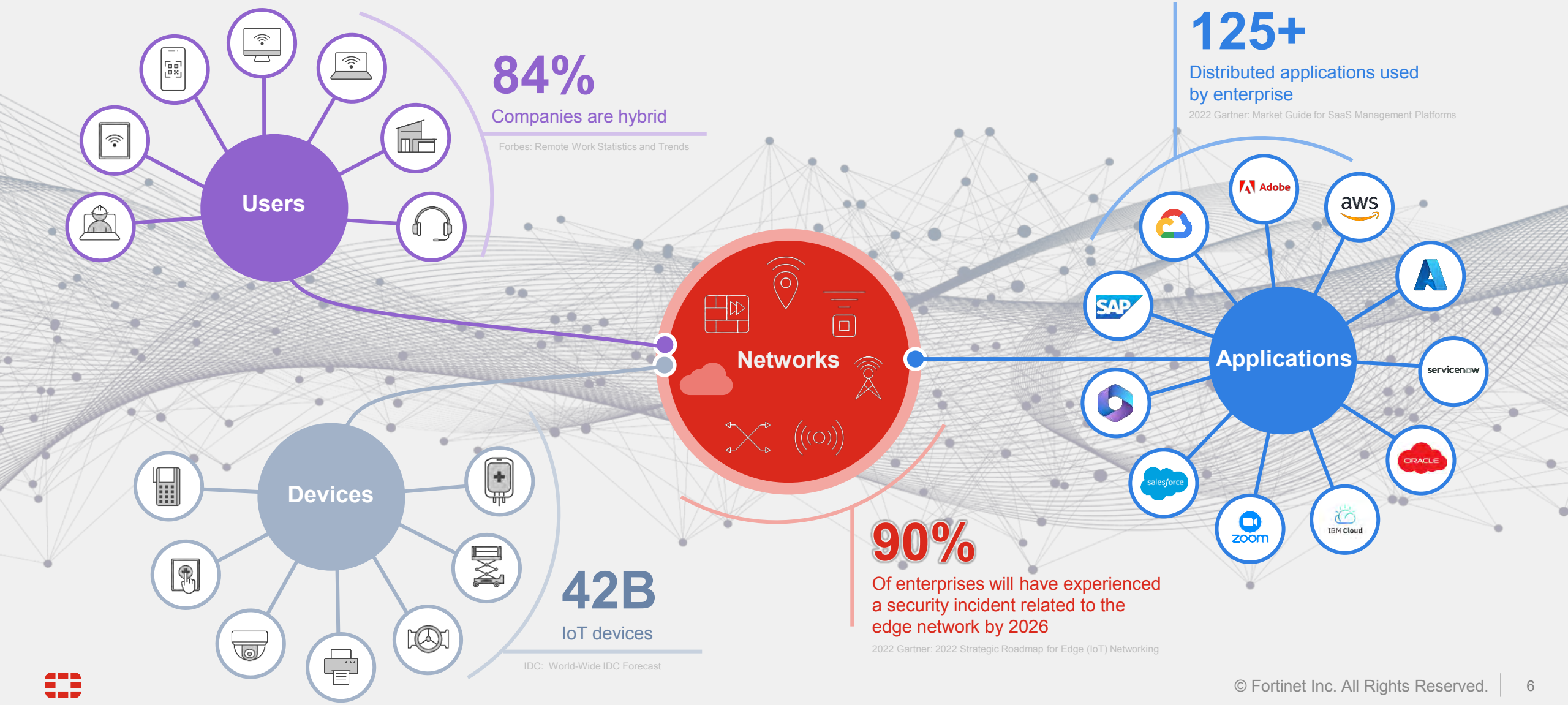
Systems Engineer

Anatomy of a Ransomware Attack



Problém Mačky

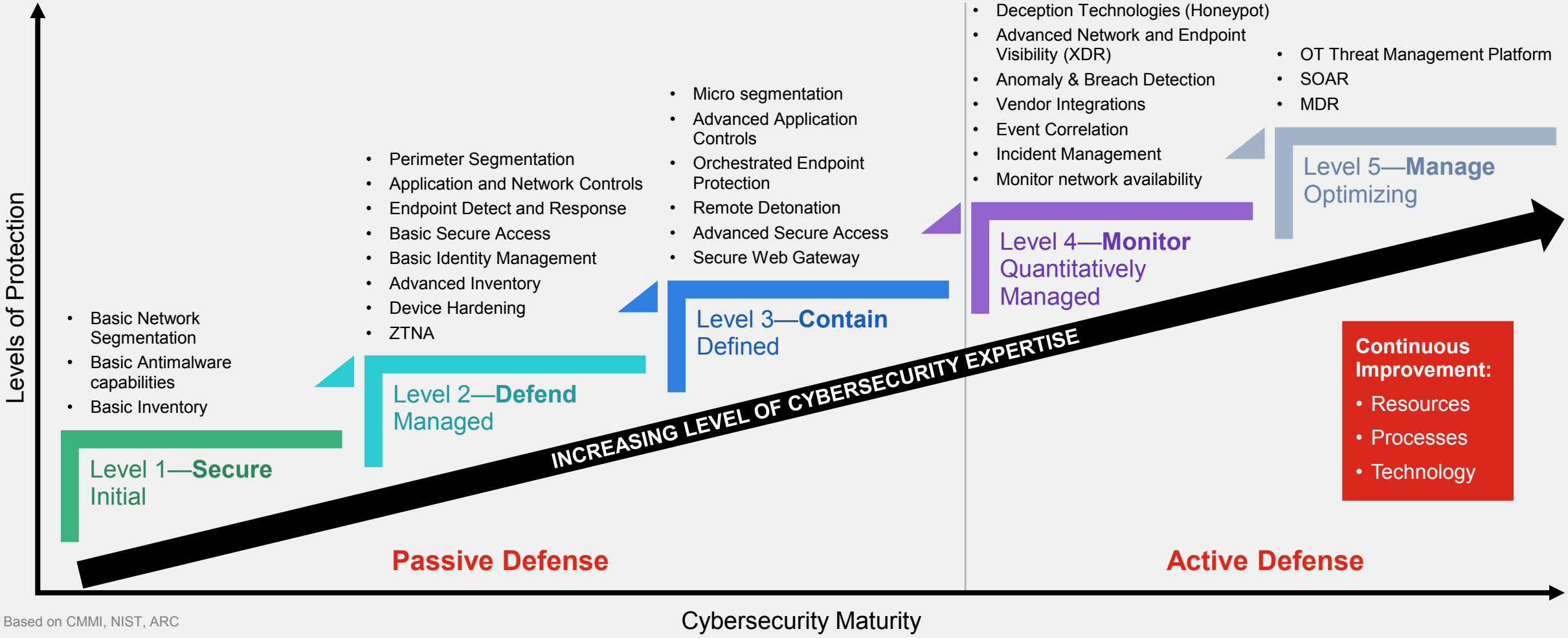
Infrastructure Has Become More Complex and More Vulnerable to Attack



We have Firewall…

Cybersecurity Maturity Scale

Scale breakdown

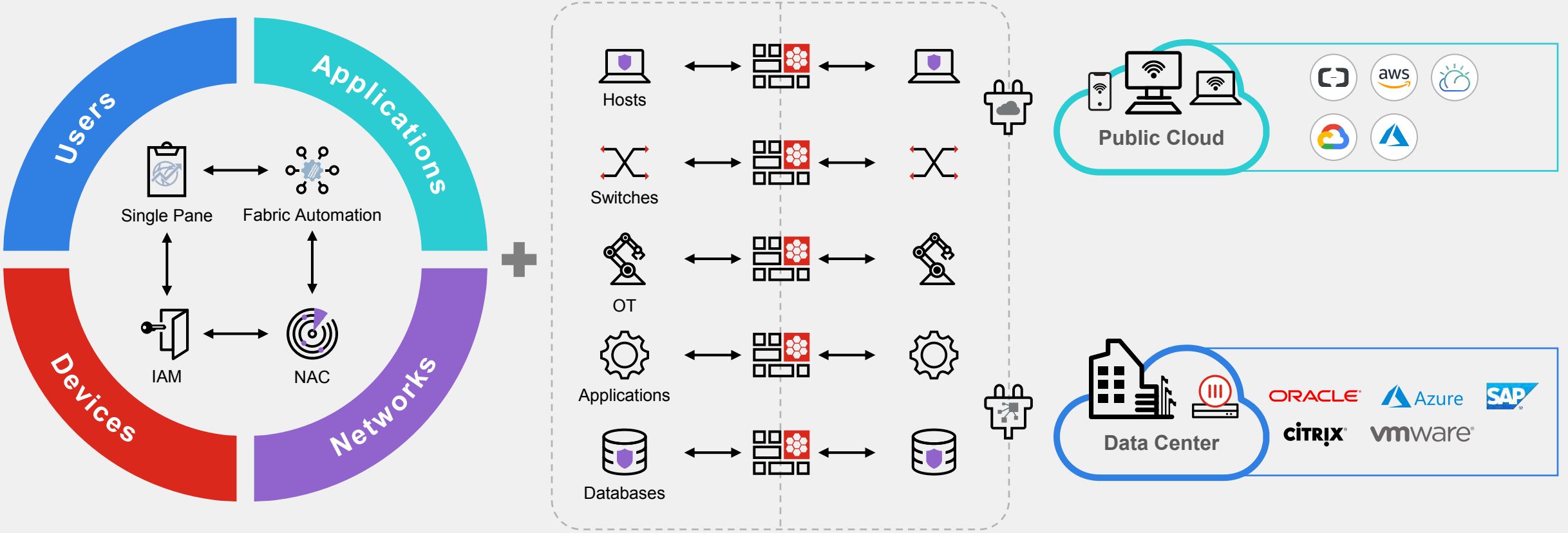


Based on CMMI, NIST, ARC

Ako? Rozdeluj a panuj!

Flexible and Adaptable Segmentation

Reduce attack surface and prevent lateral spread



Border Security

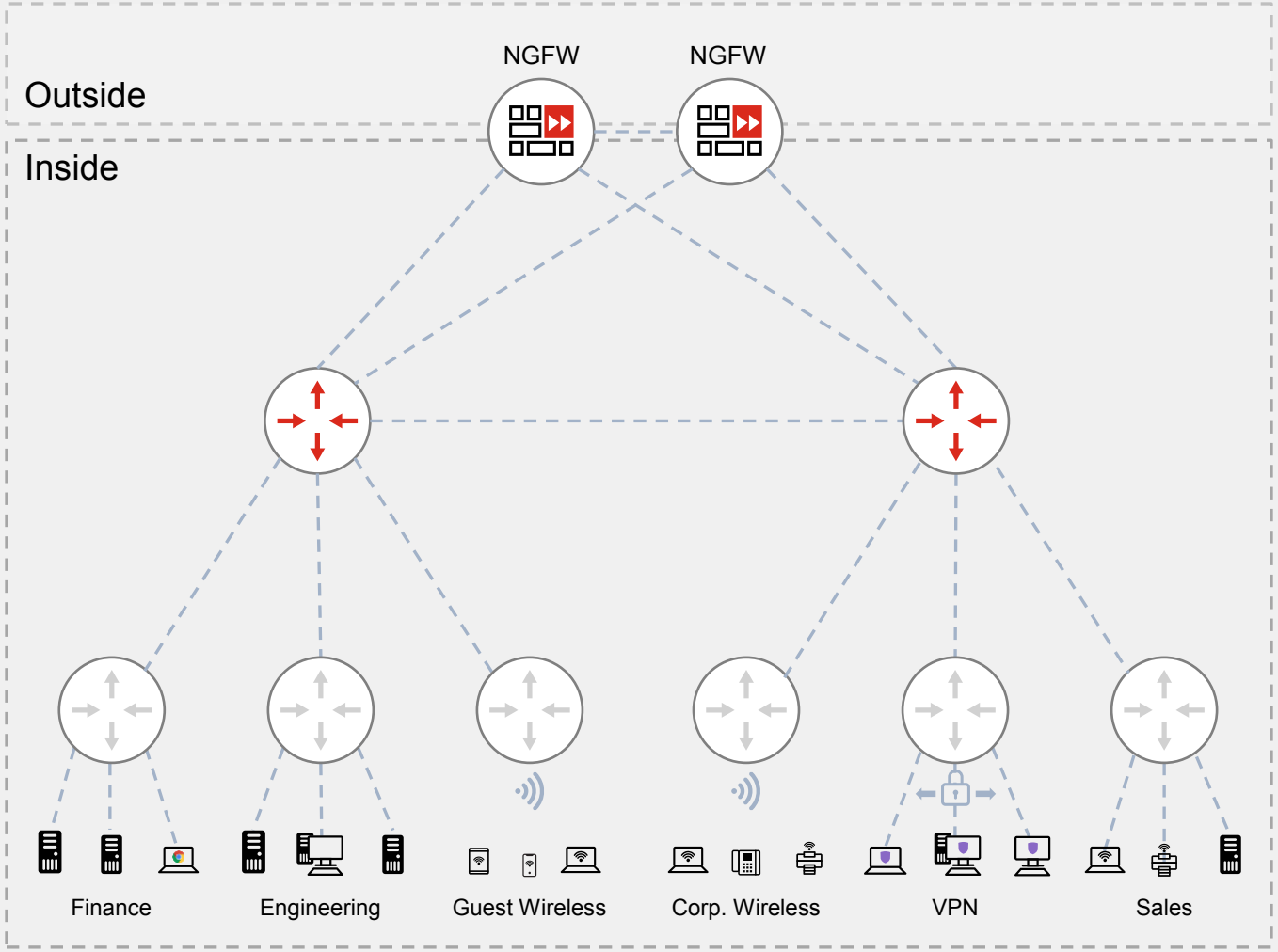
Today

Problem

- **Protect business from outside threats**
- **Protect users from the internet**
- **Keep users productive**

Solution

- **Apply all security at the internet edge**
- **Flat network provides no internal security**
- **Visibility into the network severely limited**
- **Risk of compromise is very high**



Establishing Trust

- **Network Address**
- **User Identity**
- Business Logic
- Fabric Connectors
- **Applications**
- Device Identity

Advanced Security

- SSL Inspection
- **IPS**
- **Antivirus**
- **Application Control**
- **Web Content Filter**
- Data Loss Prevention
- Secure Email Gateway
- Denial of Service Protection
- Web Application Firewall
- Cloud Access Security Broker
- Advanced Threat Protection
- Endpoint Protection

Reducing Attack Surface

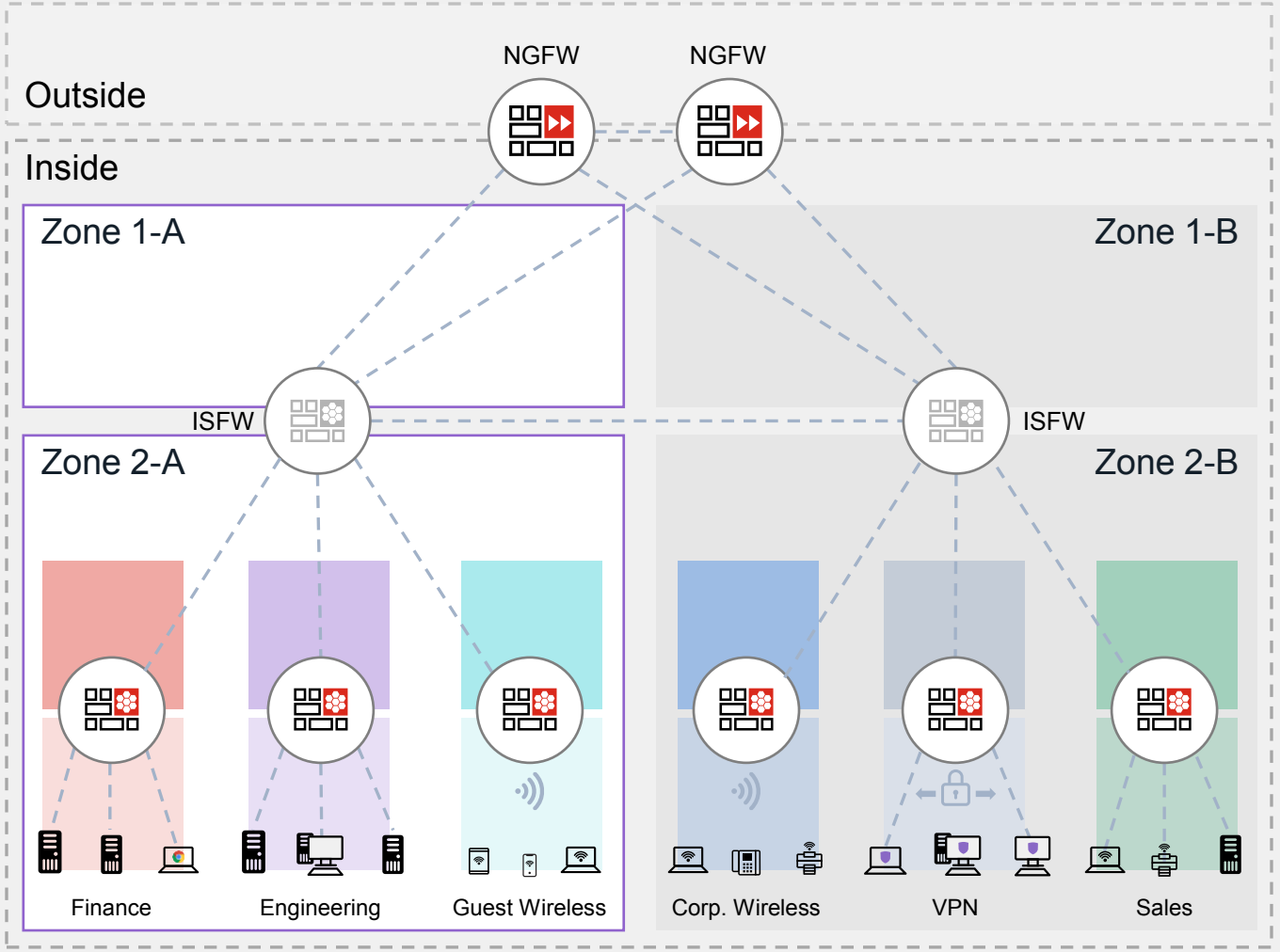
Use case

Problem

- Flat internal network
- No internal visibility
- No internal security

Solution

- Many enforcement points
- Create containment zones
- Inspect SSL
- Inspect Applications
- Check for zero-day malware
- Protect critical assets



Establishing Trust

- **Network Address**
- **User Identity**
- Business Logic
- Fabric Connectors
- Applications
- Device Identity

Advanced Security

- **SSL Inspection**
- **IPS**
- **Antivirus**
- **Application Control**
- Web Content Filter
- Data Loss Prevention
- Secure Email Gateway
- Denial of Service Protection
- Web Application Firewall
- Cloud Access Security Broker
- **Advanced Threat Protection**
- Endpoint Protection

Trusted Application Integrity

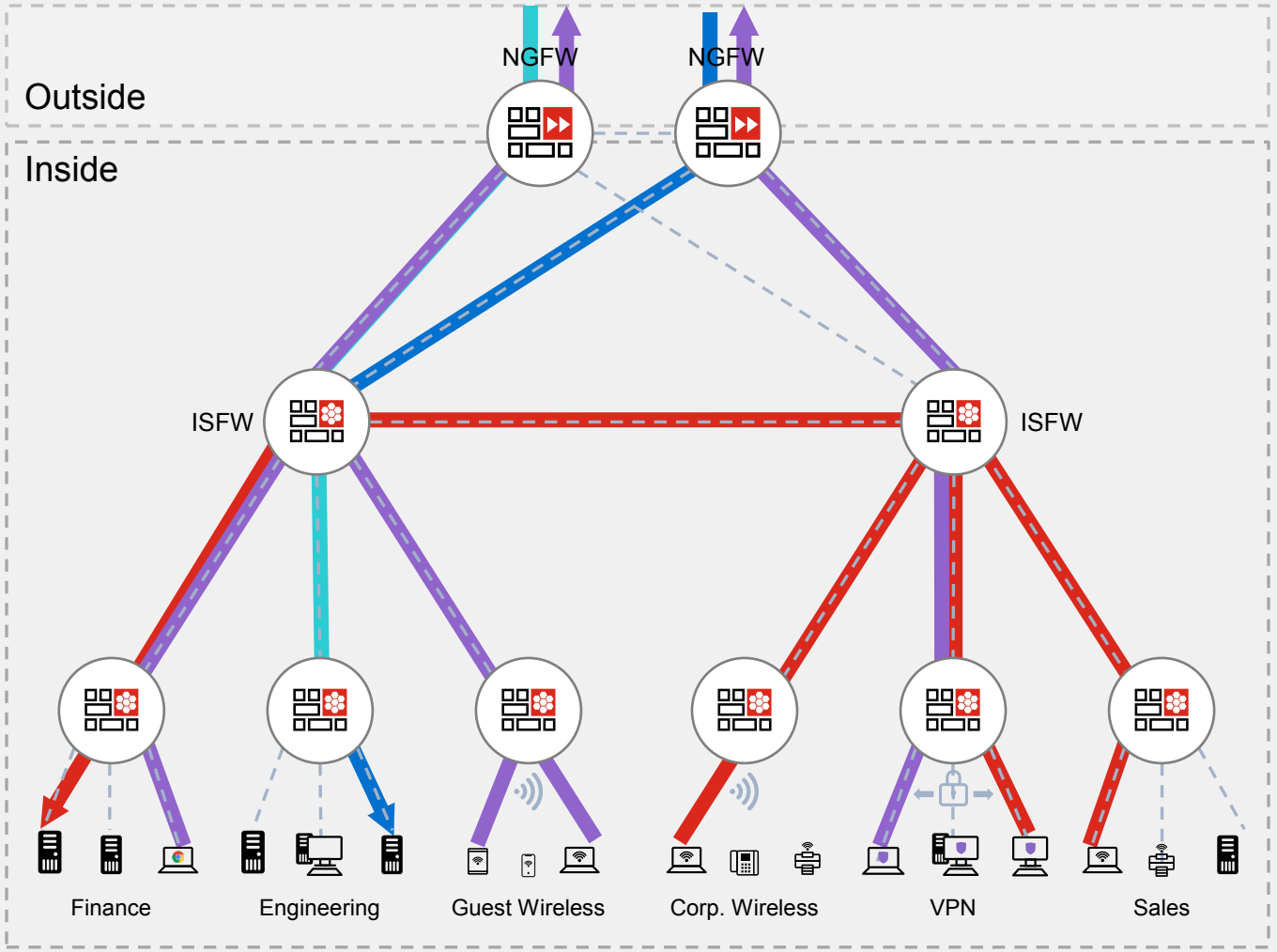
Use case

Problem

- Business critical applications must be secured
- Multiple applications
- Users in many locations

Solution

- Secure applications with solutions that share security intelligence
- Utilize security that will work with mobility and cloud usage
- Inspect SSL to make sure only trusted transactions are taking place
- Establish trust with sources inside and outside the network



Establishing Trust

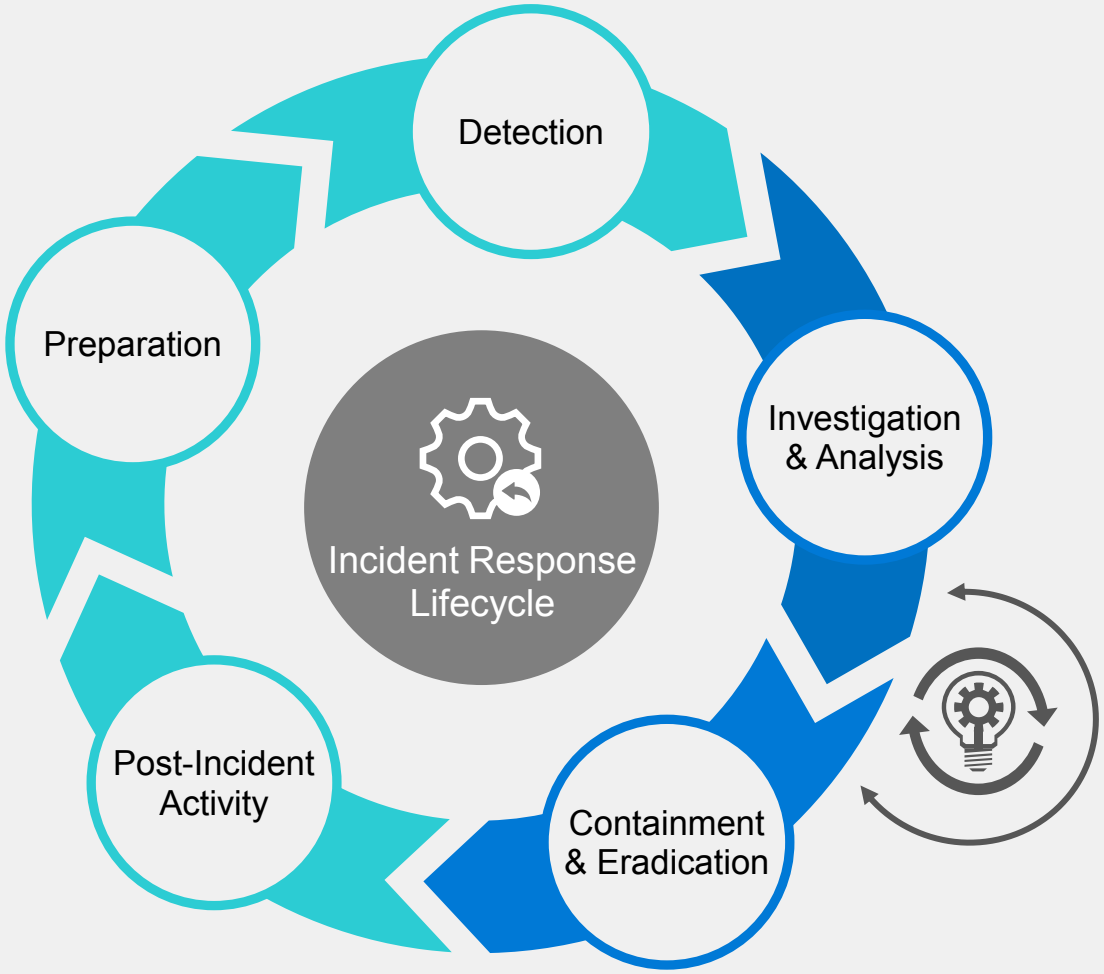
- Network Address
- User Identity
- Business Logic
- Fabric Connectors
- Applications
- Device Identity

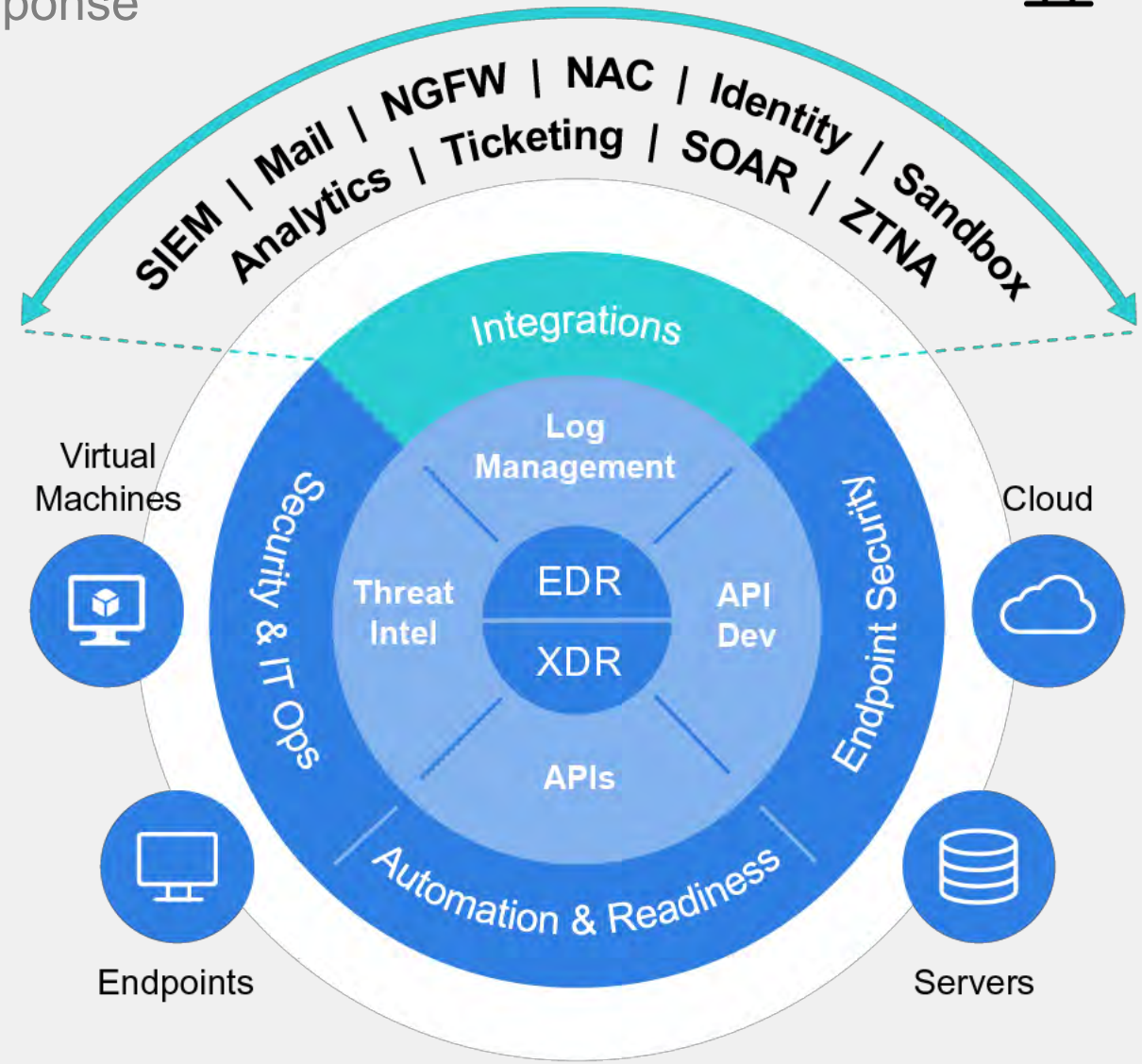
Advanced Security

- SSL Inspection
- IPS
- Antivirus
- Application Control
- Web Content Filter
- Data Loss Prevention
- Secure Email Gateway
- Denial of Service Protection
- Web Application Firewall
- Cloud Access Security Broker
- Advanced Threat Protection
- Endpoint Protection

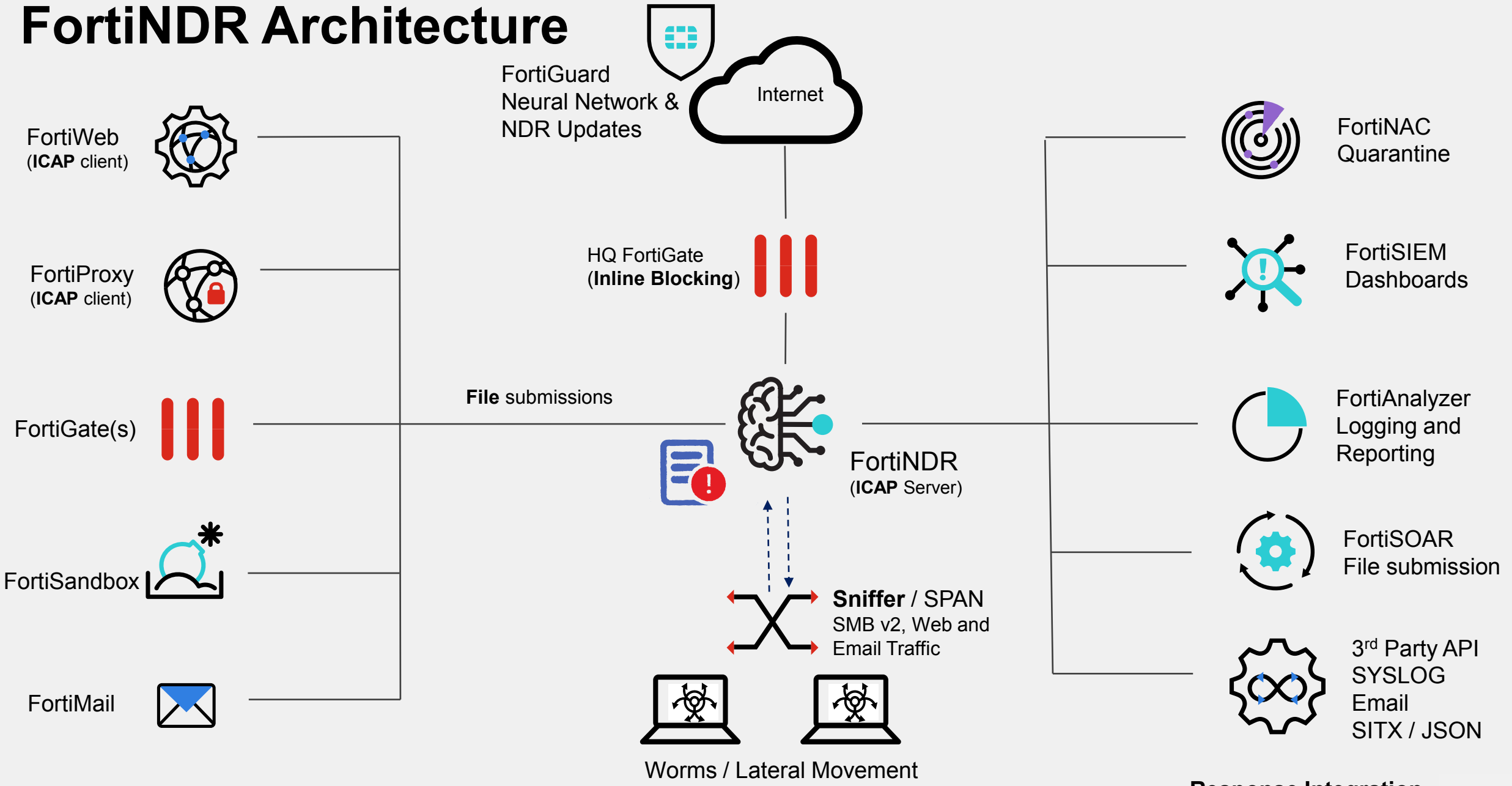
FortiEDR Design Principles

Cloud-native Endpoint Protection, Detection & Response





FortiNDR Architecture



Response Integration

FortiMail - Secure Email Gateway

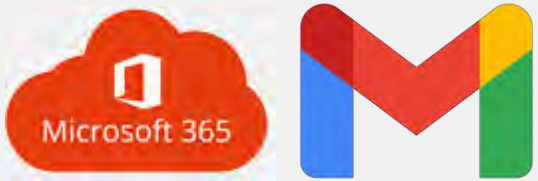
Advanced multi-layer security against:

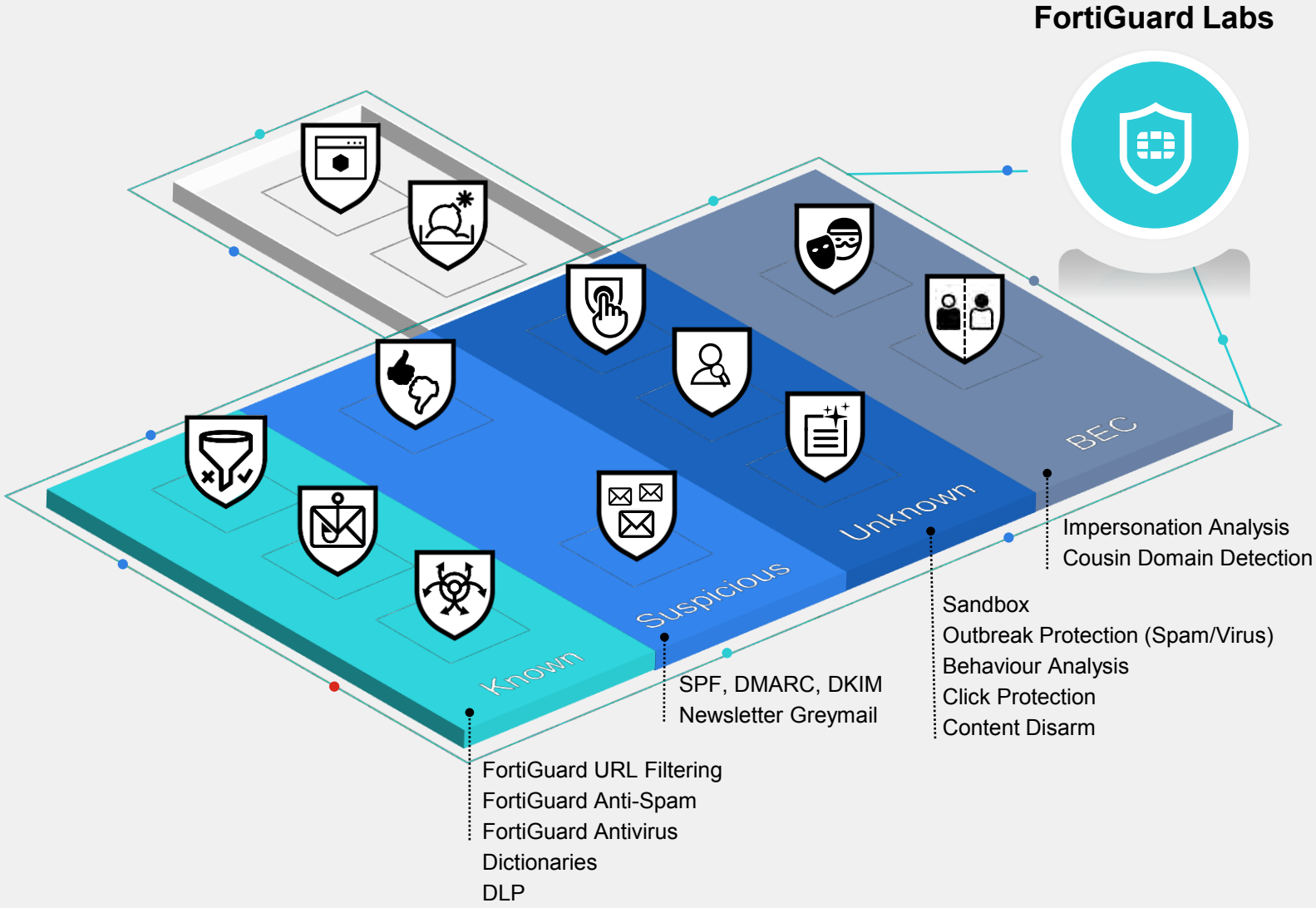
- Known threats
- Suspected threats
- Unknown threats/Zero-days
- Business Email Compromise

Flexible

- Policies
- Profiles

API:



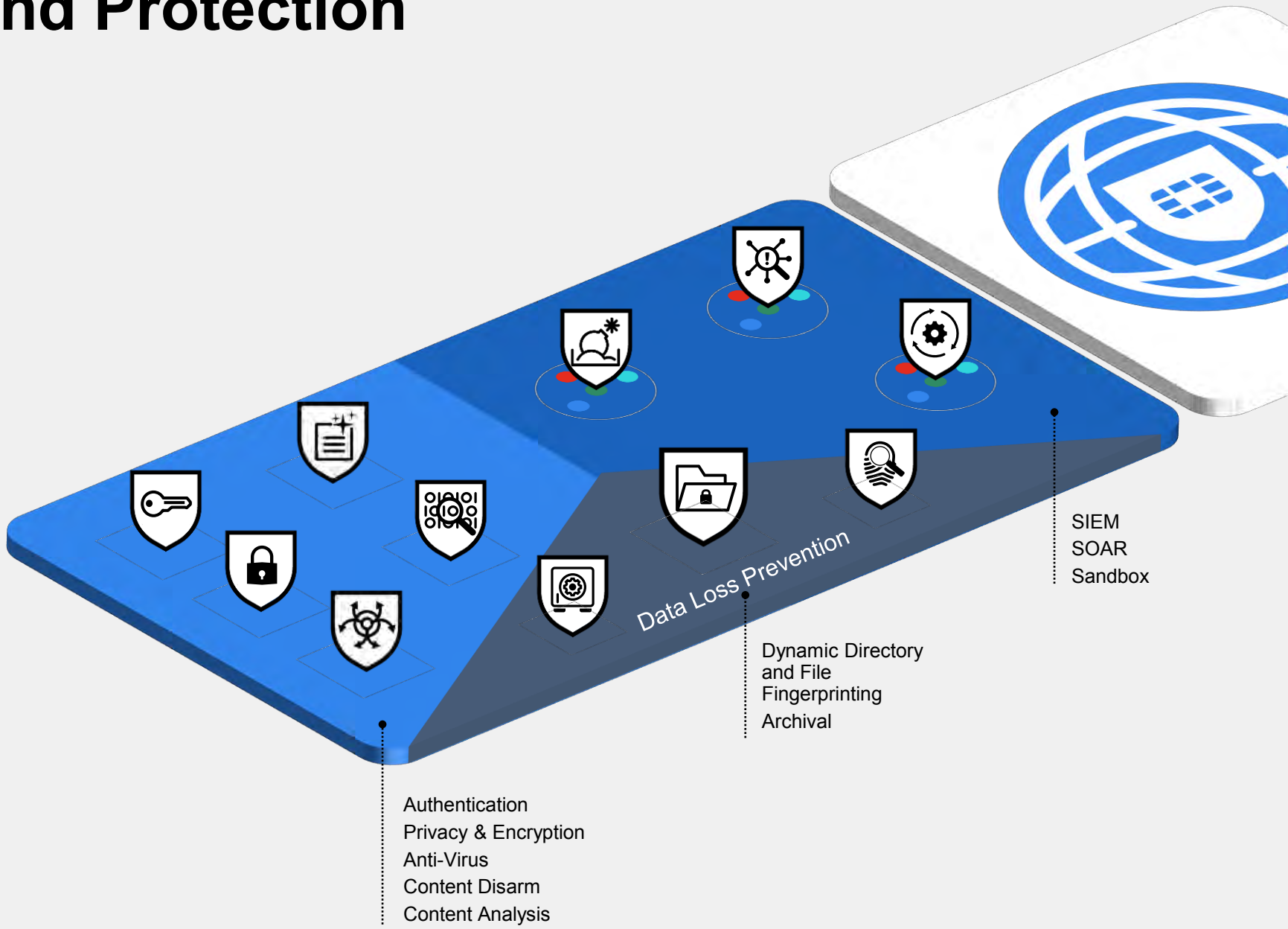


FortiMail - Outbound Protection

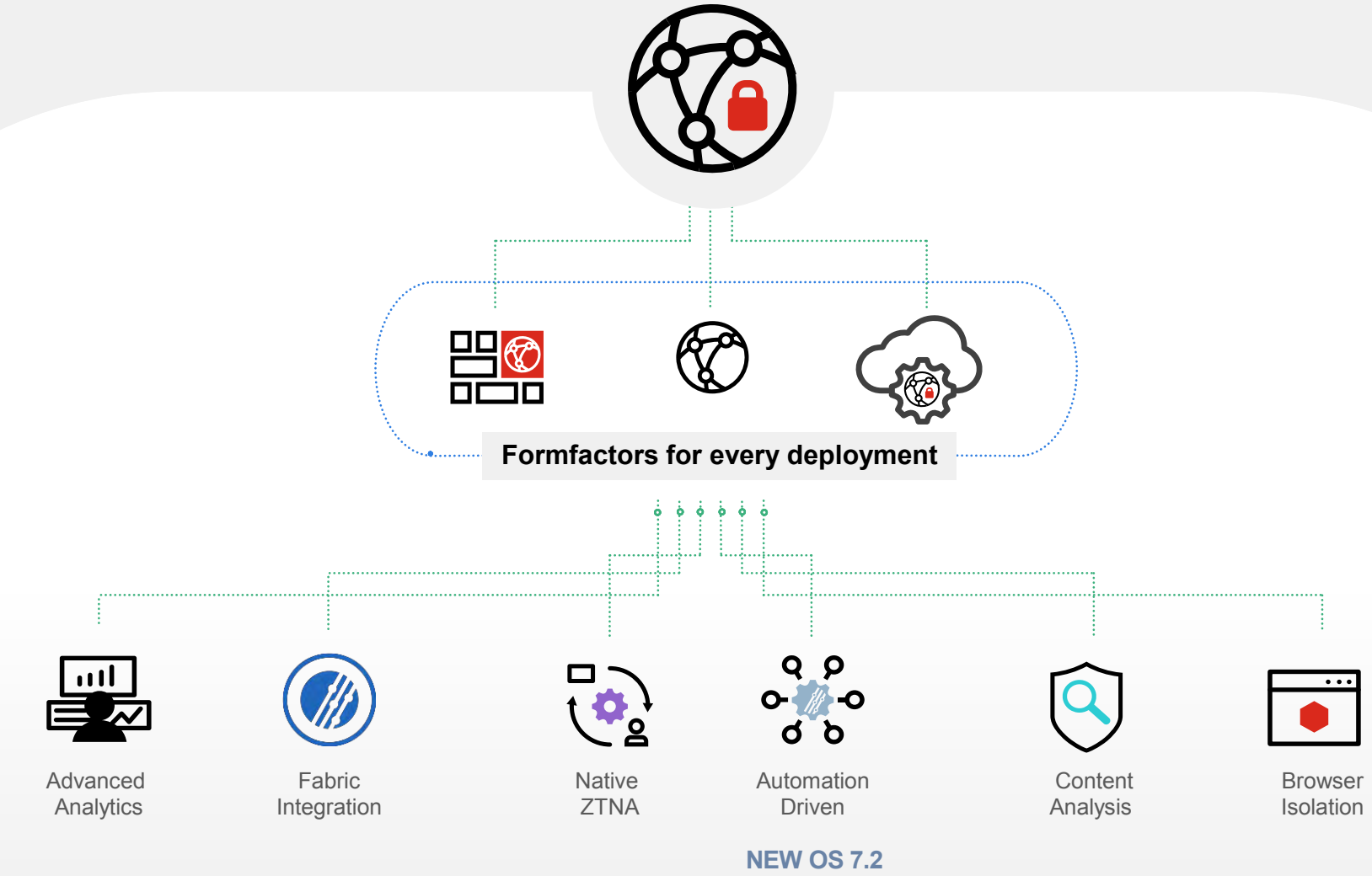
Advanced multi-layer security against:

- Accidental disclosures
- Exfiltration
- Man-in-the-Middle Attacks

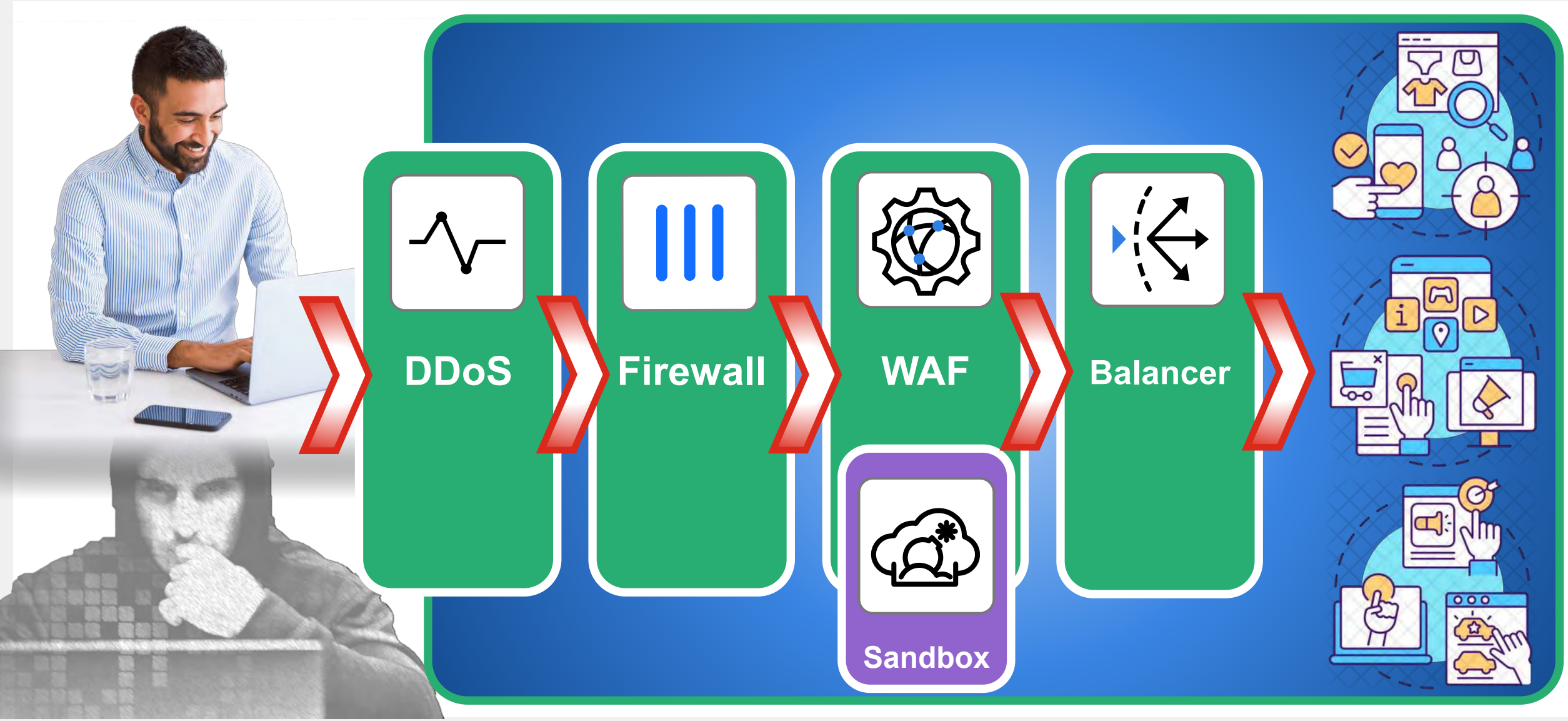
Facilitate automated response workflows.



Web Access - FortiProxy

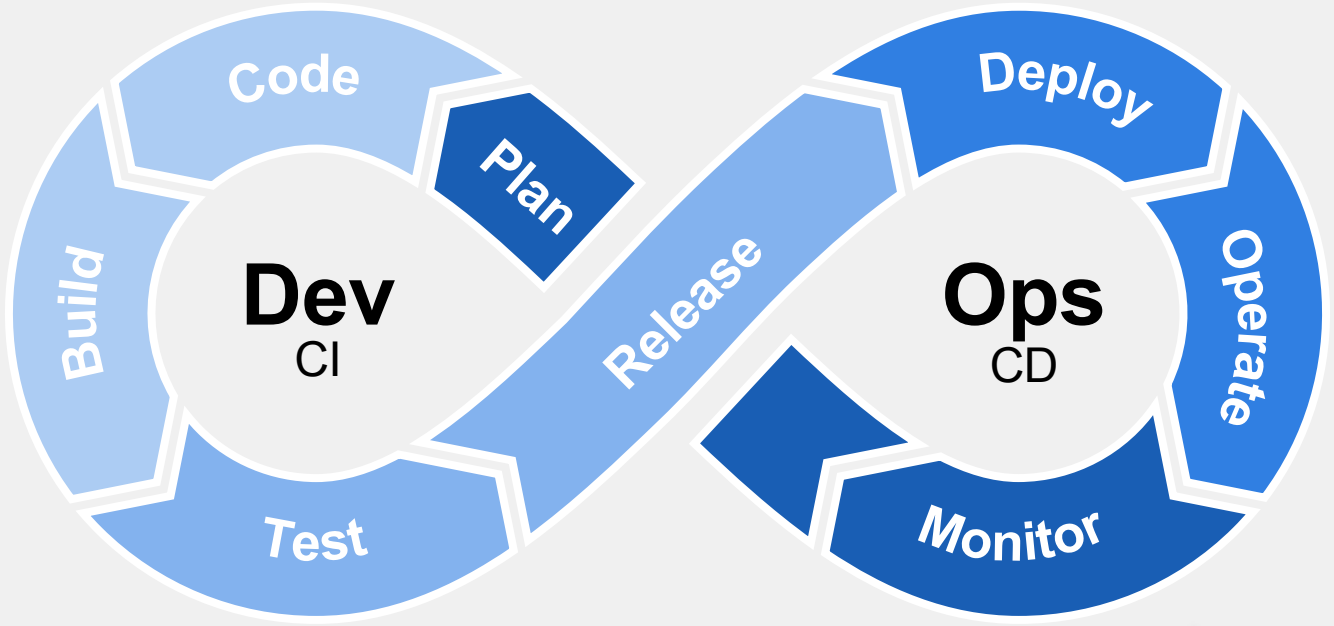


(Web) Application - Security Sandwich



Web App Security at different stages

FortiDAST
Black box vulnerability testing



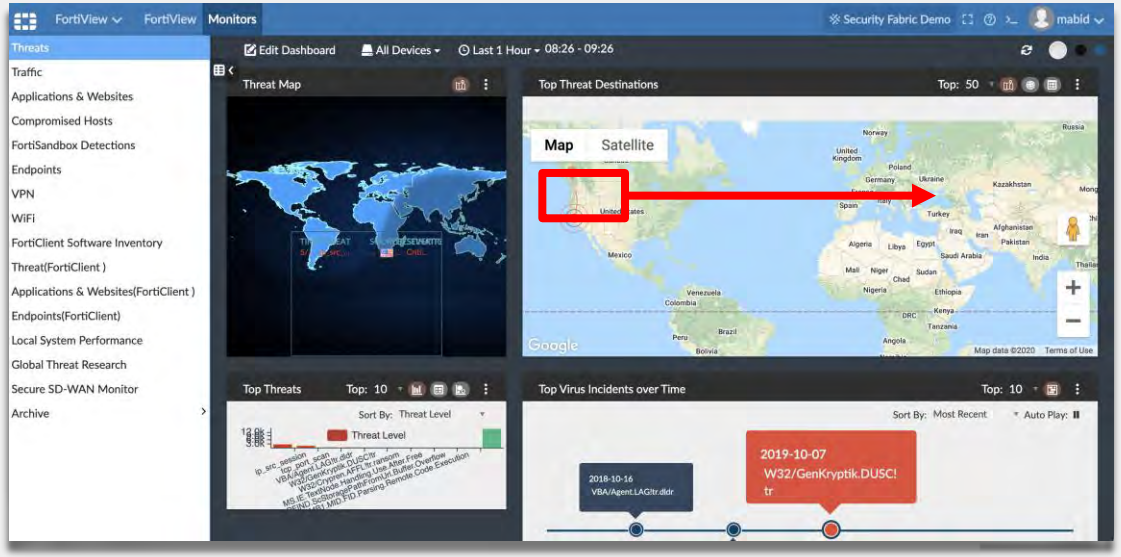
FortiDevSec
SAST, SCA/OSS, Container and IaC scans

FortiDAST
Black box vulnerability testing

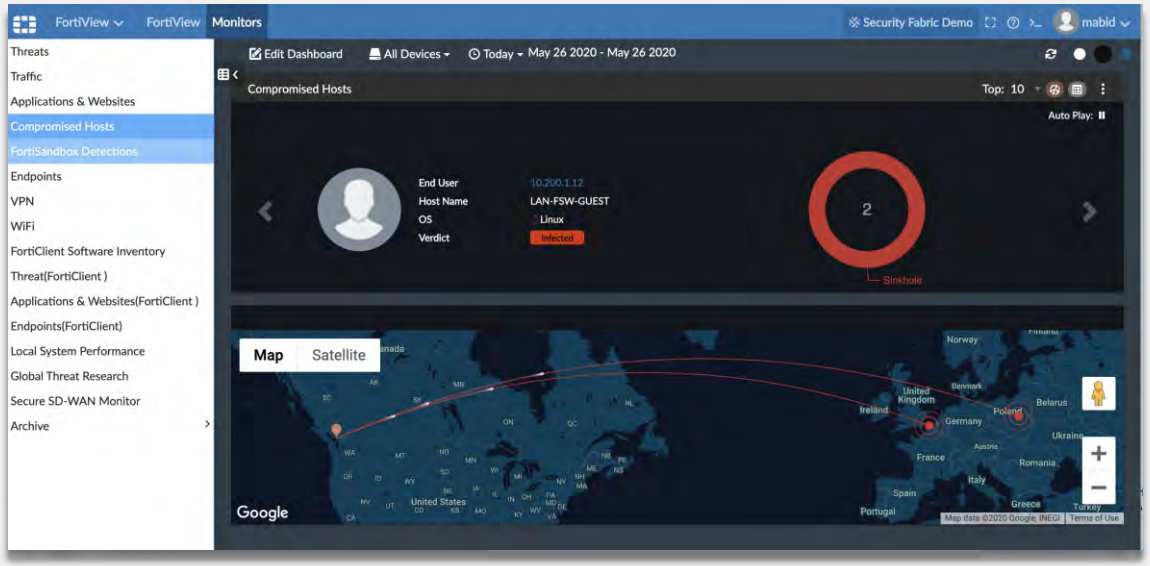
FortiWeb

Protect Web Applications live in Production

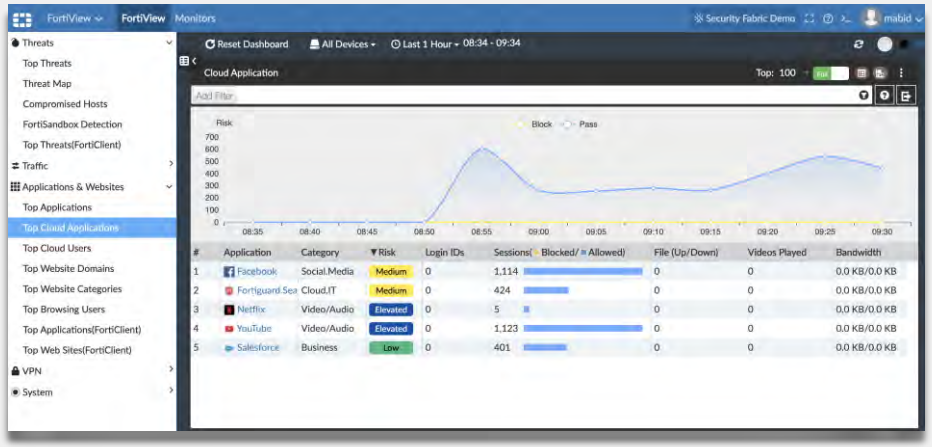
FortiAnalyzer Analytics Increase Visibility



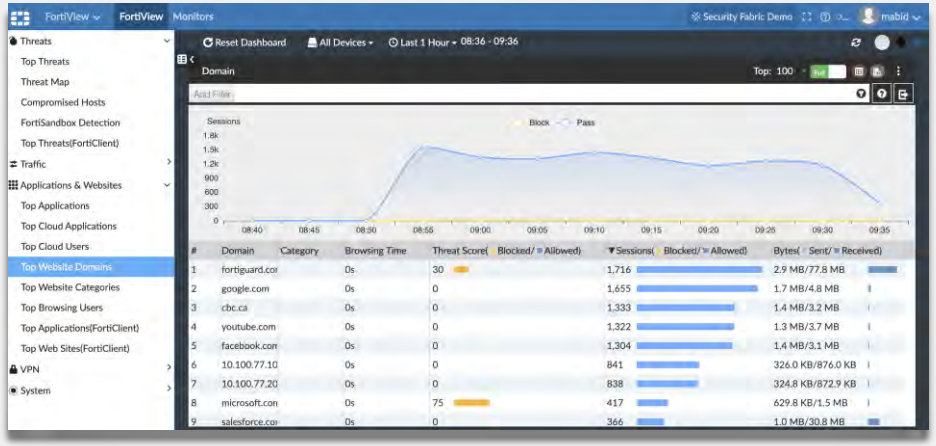
Threat Landscape in last hour



Compromised Host



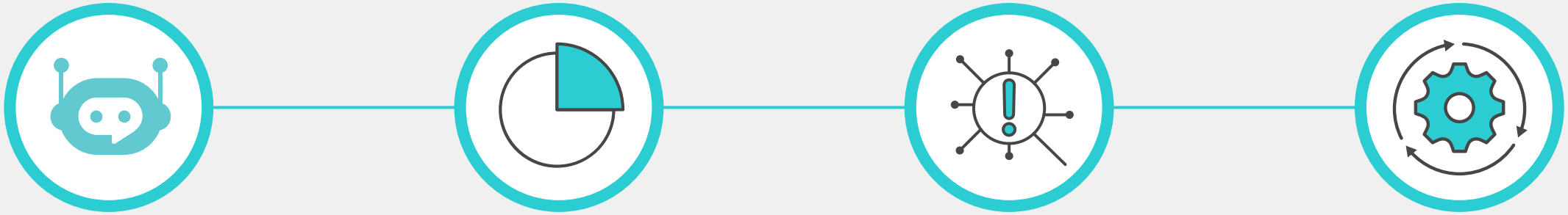
Top Cloud Applications



Top Website Domains

Intuitive AI Assistance

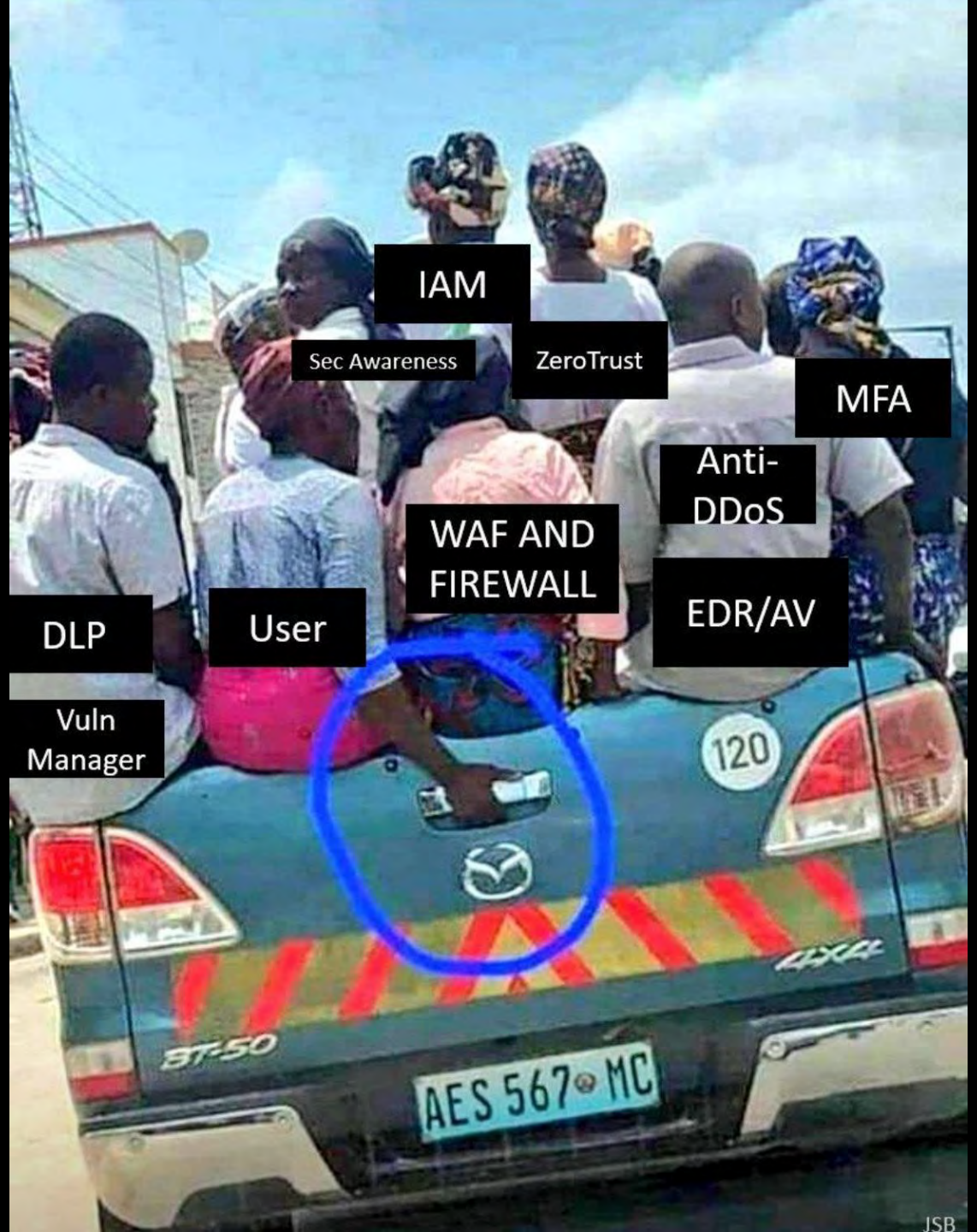
FortiAI: Built-in GenAI capabilities for proactive threat management and automation



- **Assessment:** Utilize FortiAI to evaluate network anomalies within FortiAnalyzer's data streams.
- **Prediction:** Anticipate potential breaches by applying FortiAI's predictive capabilities to analytics.
- **Best Practices:** Continuously receive recommendations and guidance

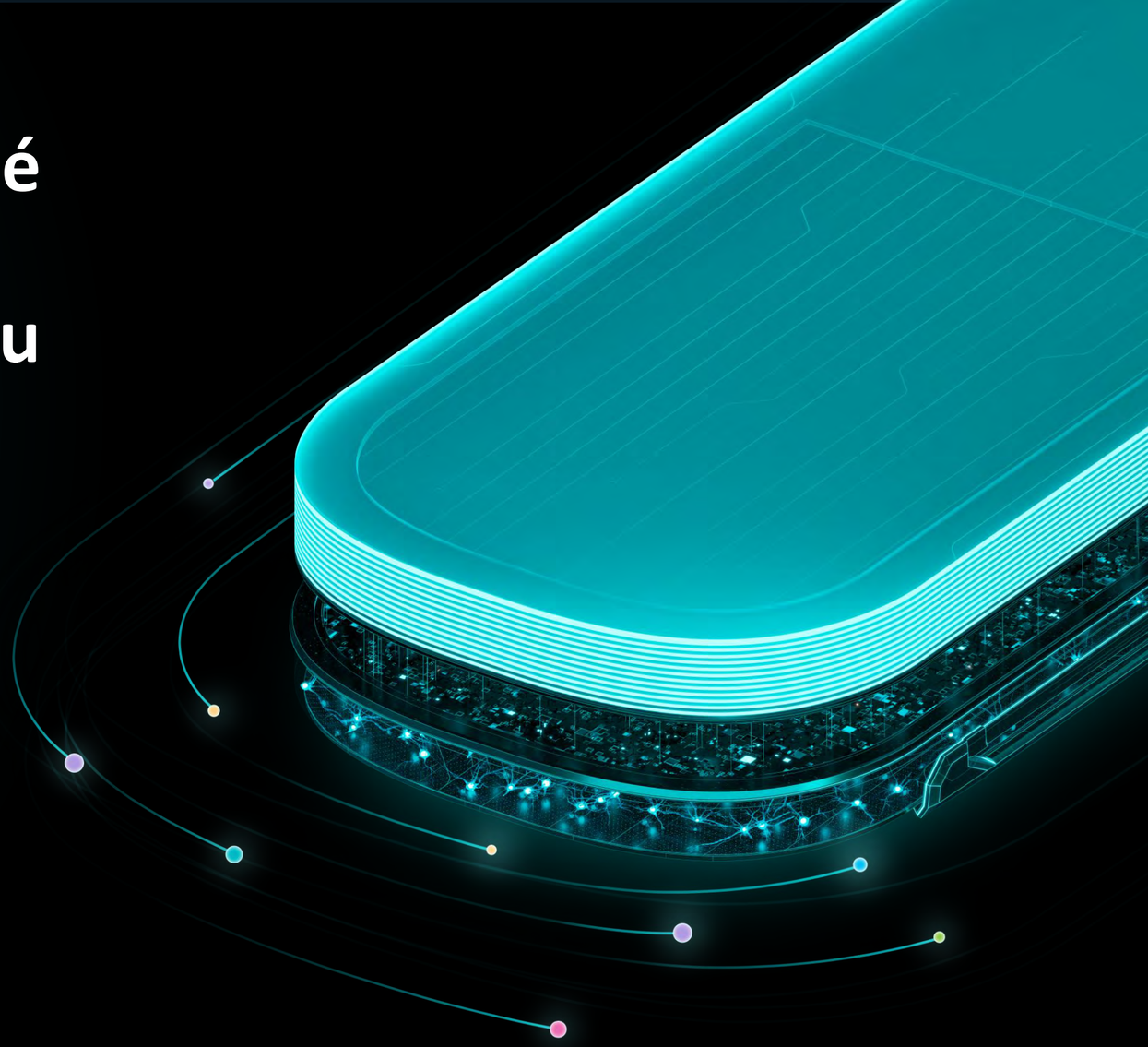
Prompts:

- Analyze this incident and tell me what action to take.
- Tell me about this malware and the attackers who use it.
- What response playbooks do you recommend for this alert?
- Create a report of events per critical incident of the last 30 days.



Moderné výzvy si žiadajú moderné riešenia: Bezpečnosť s Managed Detection and Response bez stresu

JÚLIUS SELECKÝ
SENIOR TECHNICAL PRE-SALES REPRESENTATIVE
JULIUS.SELECKY@ESET.COM



Bezpečnostné výzvy pre organizácie

Komplexnosť útokov

2,200

Kyber útokov za deň

Regulácie a ich požiadavky

66%

Očakáva výdaje spojené s reguláciami

Nedostatok IT security odborníkov

49%

Profesionálov priznáva nedostatky v IT štruktúre

Finančná náročnosť

51%

nárast financií v rokoch 2016-2023

Moderný Ransomware

Adversary Gains a Foothold

RDP/RDS Login, Unpatched Service

Examines Network and Users

Living off the land

Downloads other utilities

Escalate Privileges /Steal Credentials

Moves Across Network

Find and Exfiltrate Files

Allows for Extortion

Deploy Encryption

Ransomware

Demand Payment

Extortionware

Adversary Gains a Foothold

RDP/RDS Login, Unpatched Service

Examines Network and Users

Living off the land

Downloads other utilities

Escalate Privileges /Steal Credentials

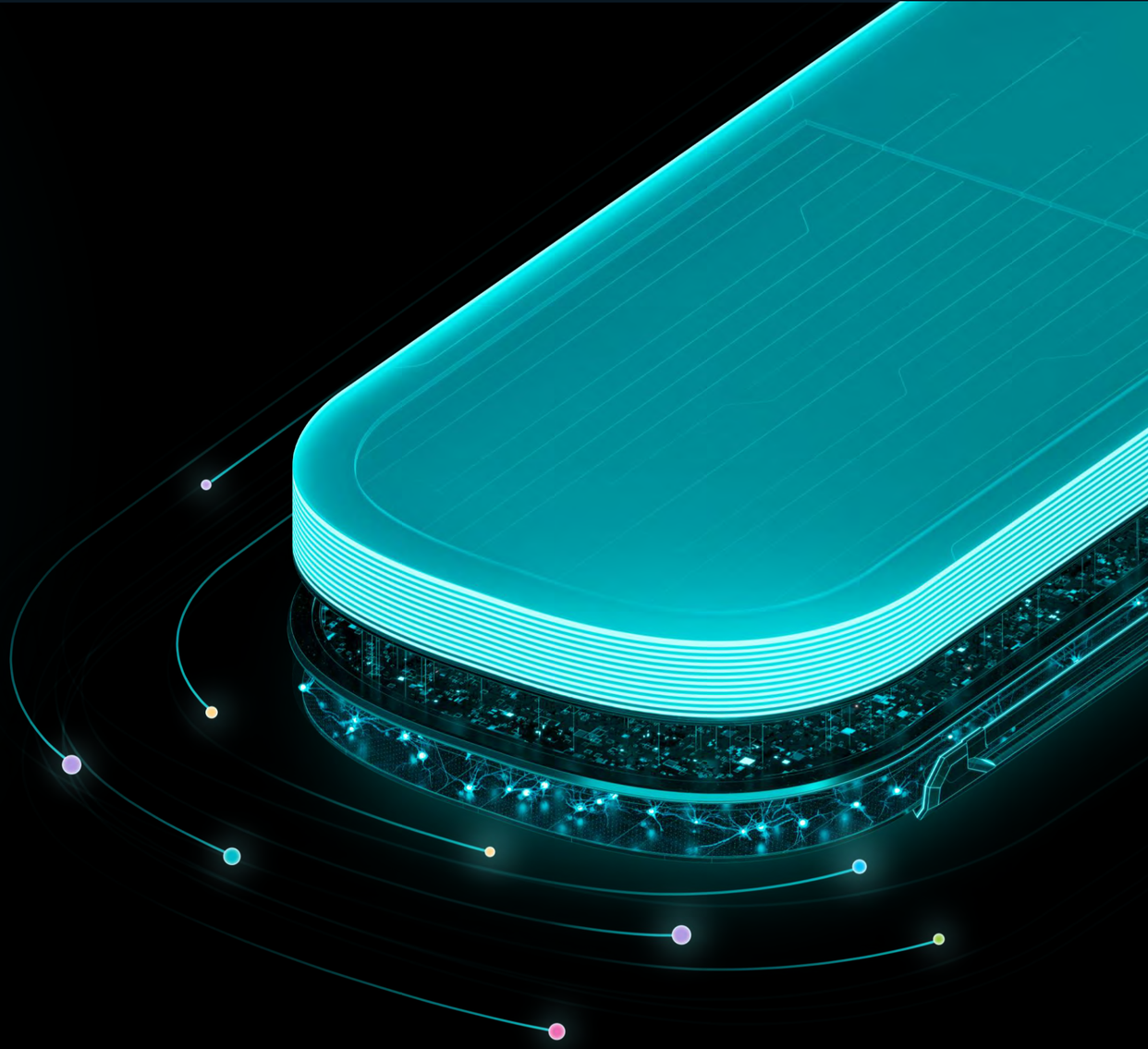
Moves Across Network

Find and Exfiltrate Files

Allows for Extortion

Demand Payment

XDR



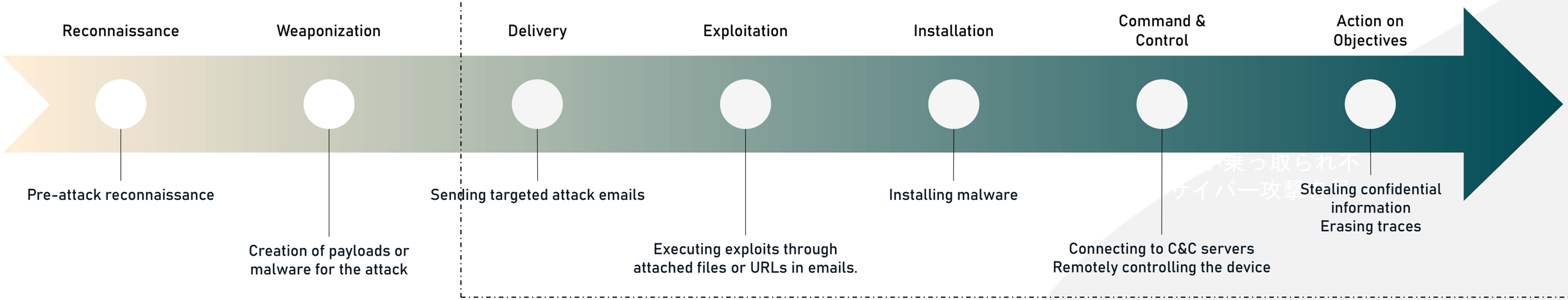
BOJ PROTI RÔZNYM KYBERNETICKÝM ÚTOKOM

10 najväčších hrozieb informačnej bezpečnosti v roku 2024 [Organizácie]	
Rank	**Threats to any organization**
1	Škody spôsobené ransomvérom
2	Útoky využívajúce slabé miesta v dodávateľskom reťazci
3	Incidenty, ako je únik informácií v dôsledku interného podvodu
4	Krádež dôverných informácií prostredníctvom cielených útokov
5	Útoky zamerané na obdobie pred vydaním záplat (Zero-Day útoky)

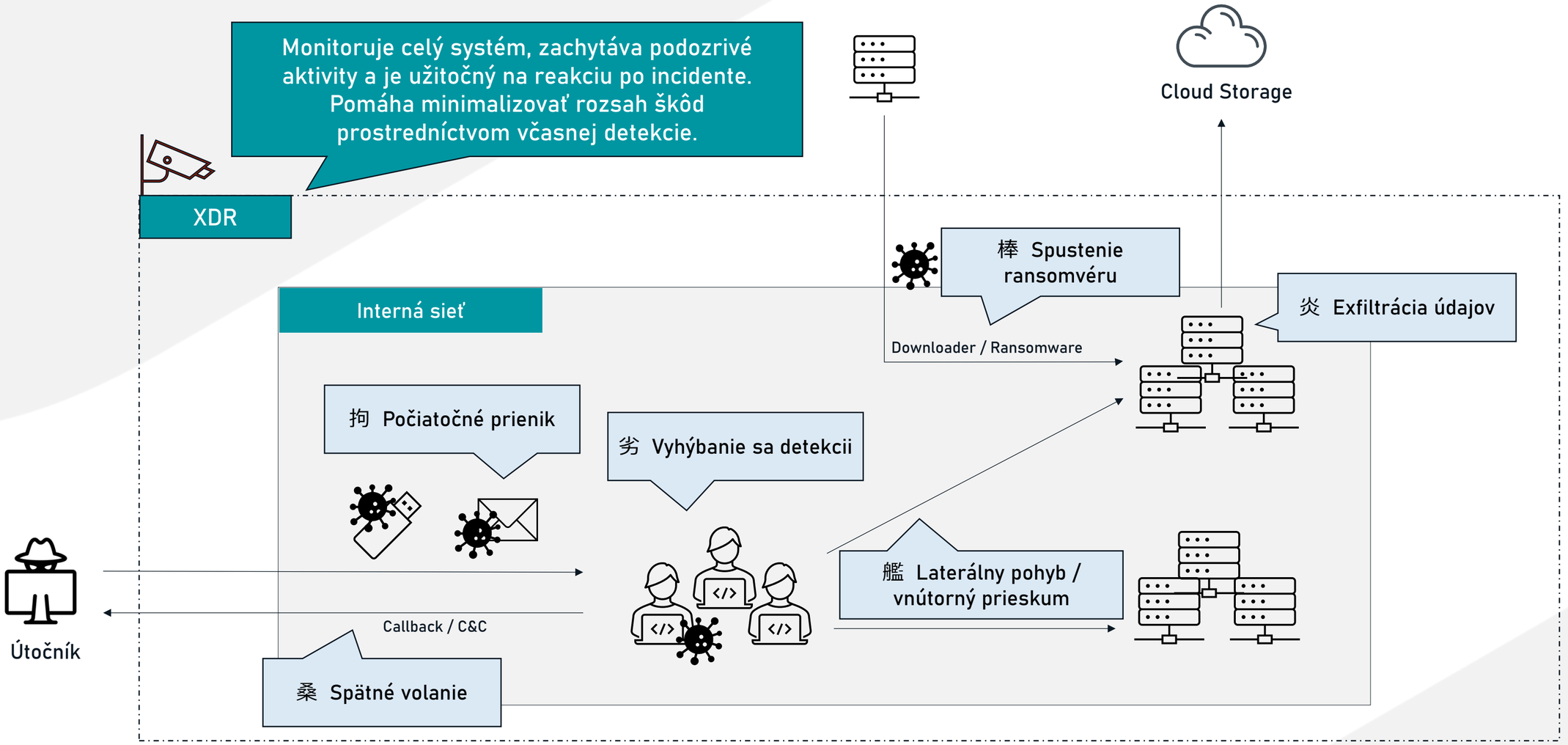
V poslednom čase sa zvýšil počet kybernetických útokov zameraných na zraniteľné miesta, slabiny v dodávateľskom reťazci, interné podvody a iné „slabé miesta“ spoločností.

Útoky často využívajú zraniteľnosti v operačných systémoch a sieťových zariadeniach pomocou veľmi skrytých metód. XDR (Extended Detection and Response - rozšírená detekcia a reakcia) je účinným prostriedkom včasnej detekcie incidentov.

Ukážka útoku



POKRYTIE DETEKCIE A REAKCIE POMOCOU XDR

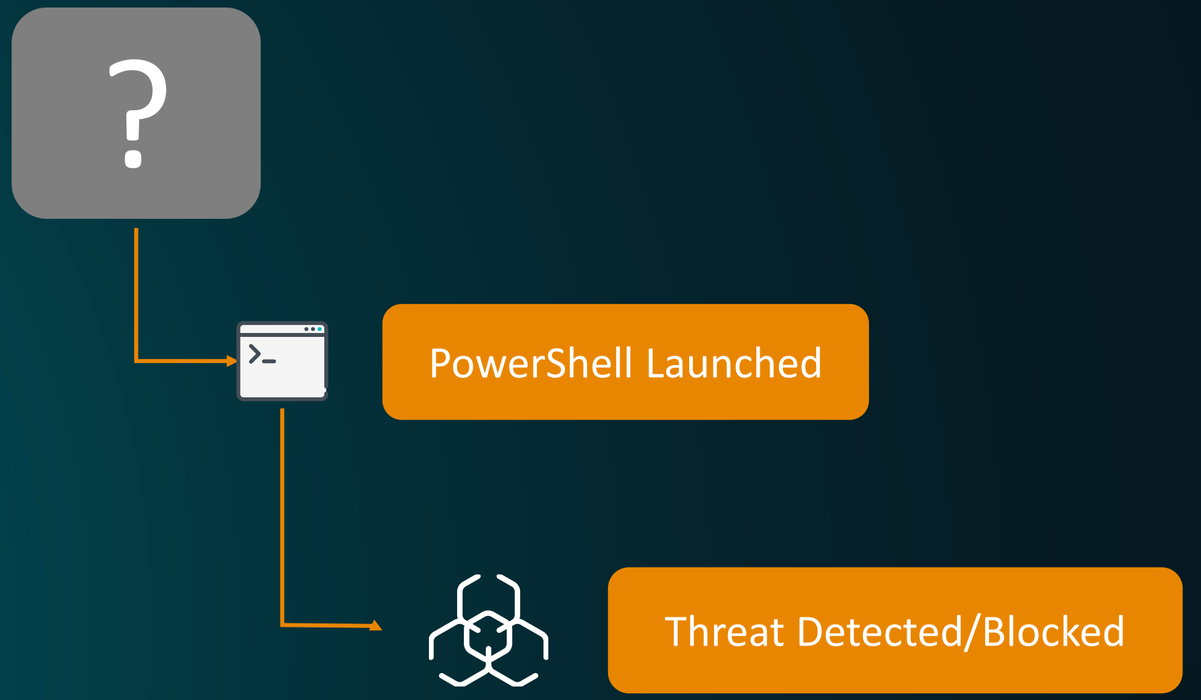


Kybernetické útoky v poslednej dobe dosahujú svoje ciele tak, že prechádzajú viacerými fázami útoku. XDR nepretržite analyzuje logy z každého koncového bodu pomocou modelov umelej inteligencie, aby sa zabránilo šíreniu infekcie a umožnili sa proaktívne reakcie na incidenty.

Bežná viditeľnosť AV ochrany:

minimálna viditeľnosť

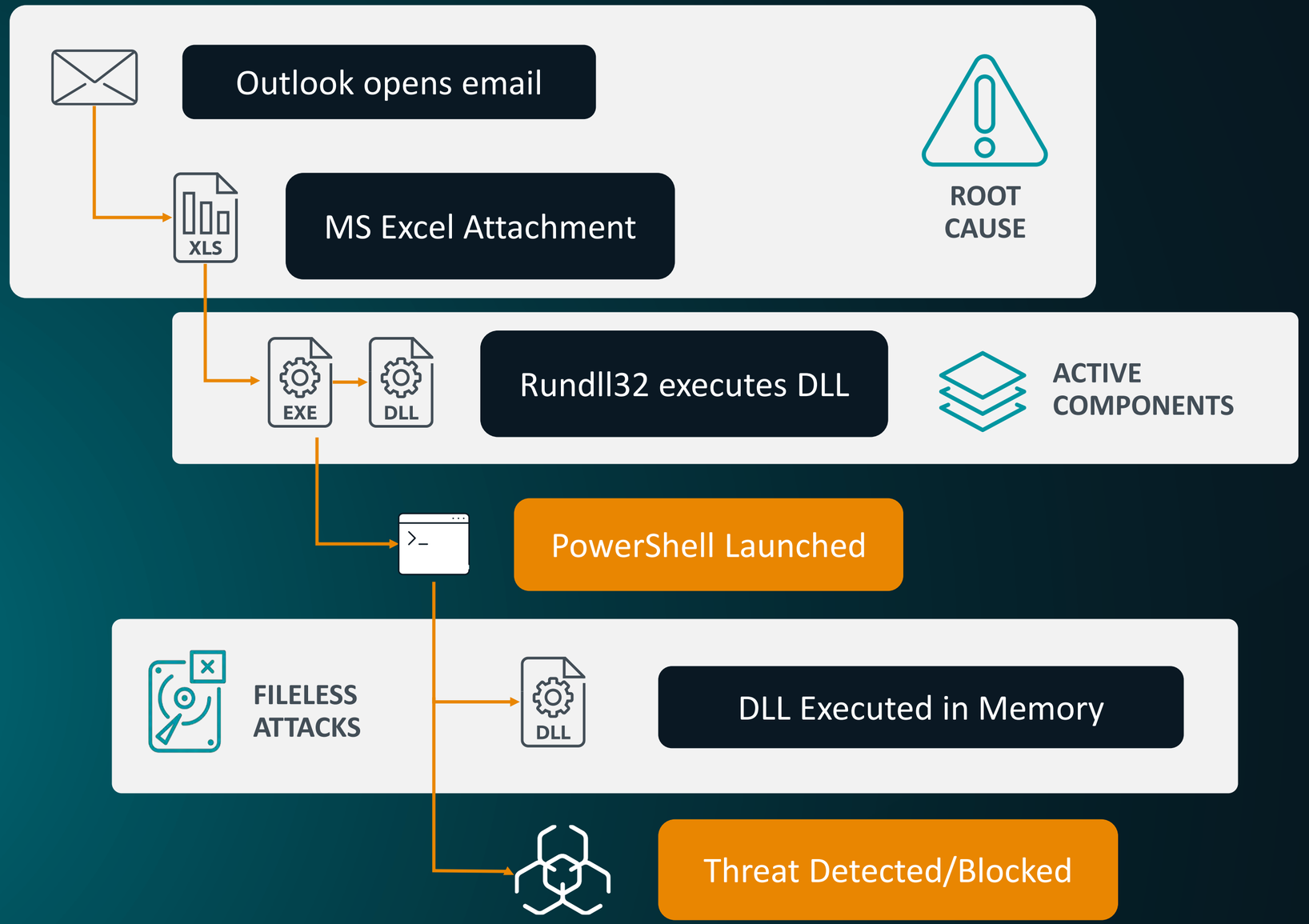
neistota



S XDR riešením:

zvýšená viditeľnosť

dodatočná kontrola

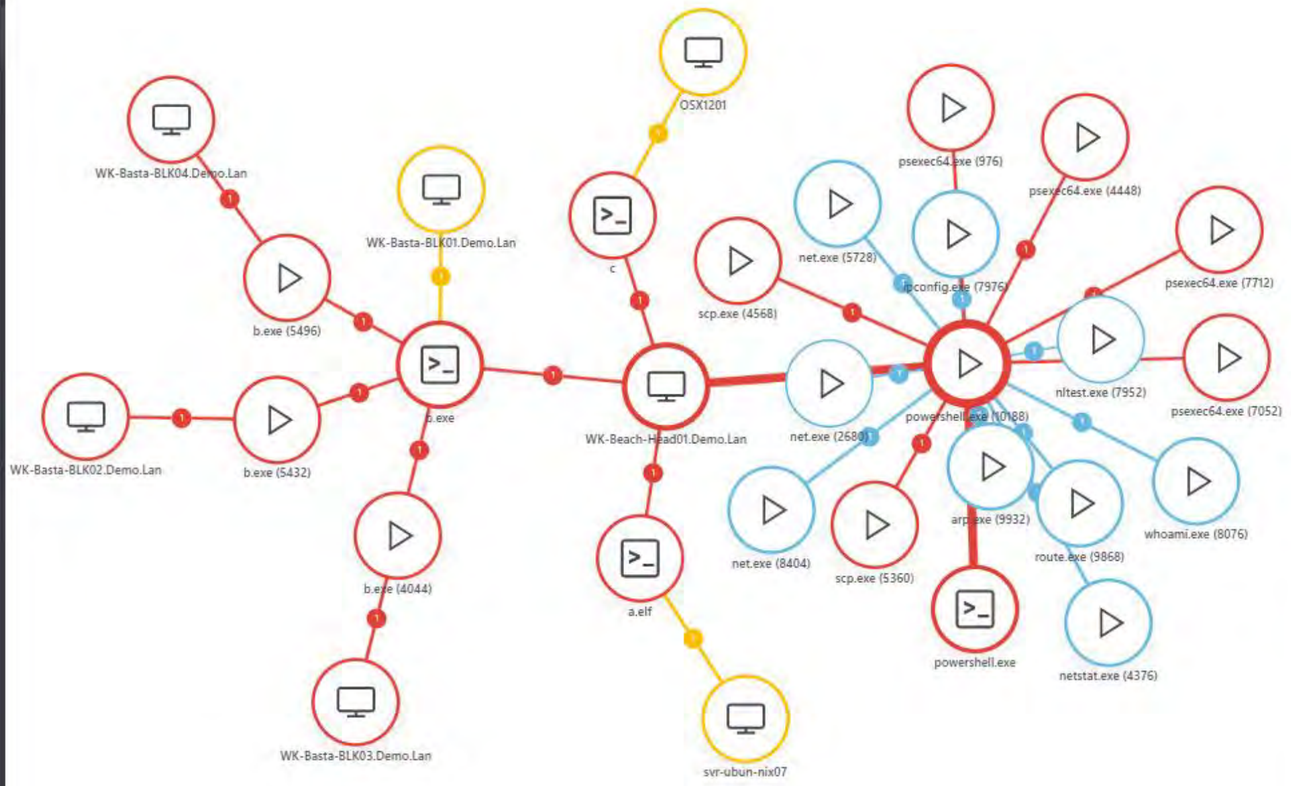


DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Questions
More...
COLLAPSE

BACK

Filecoder activity across multiple endpoints

Timeline | Relation graph | Detections | Computers | Executables | Processes



INCIDENT | REMEDIATION | COMMENT | EDIT | ASSIGN | PROGRESS | GRAPH

Incident | Timeline

Filecoder activity across multiple endpoints

Status Open
Severity High
Assignee Michal Jankech
Tags Gartner Scenario 2 | Ransomware Atta...
Select tags
Description None

Threat indicators (28)

Rule Domain trust discovery [D1102]
Mitre att&ck™ techniques
T1482 - Domain Trust Discovery

Rule Domain trust enumeration via NLTest/ADFind [C1118]
Mitre att&ck™ techniques
T1482 - Domain Trust Discovery

View more

Computers (7)
wk-beach-head01.demo.lan
osx1201
View more

Executables (4)
c
powershell.exe
View more

Processes (19)
powershell.exe (10188)
nltest.exe (7952)
View more

Problémy

Komplexita nástrojov

Únava z veľkého množstva upozornení

Nedostatok kvalifikovaných ľudí

Limitovaný čas na reakciu

MDR

(služby riadenej bezpečnosti)

Čo je MDR?

Managed Detection & Response je služba pod vedením odborníkov monitorujúcich a reagujúcich na škodlivú aktivitu vo vašej infraštruktúre.

Prečo MDR mení pravidlá hry?

je účinné riešenie na zvládnutie výziev spojených s detekciou a reakciou na hrozby pre zákazníkov

Gartner:

kľúčovou hodnotou, ktorú poskytovatelia MDR prinášajú, sú služby, inak príliš zložité a nákladné na to, aby ich klienti vykonávali sami:

- **Analýza rozličných telemetrických údajov**
- **AI/ML a ľudská interpretácia bezpečnostných incidentov**
- **Včasné usmernenie ohrozenia**
- **Rôzne úrovne reakcie/nápravy**

Ako vie MDR pomôcť?

Služba riadenej detekcie a reakcie kombinuje umelú inteligenciu a ľudské odborné znalosti na dosiahnutie bezkonkurenčnej detekcie hrozieb a rýchlej reakcie na incidenty bez potreby udržiavať vlastných bezpečnostných špecialistov..

security | AI | detection | service

expertise | maintain | response

MDR

Posilnenie bezpečnosti

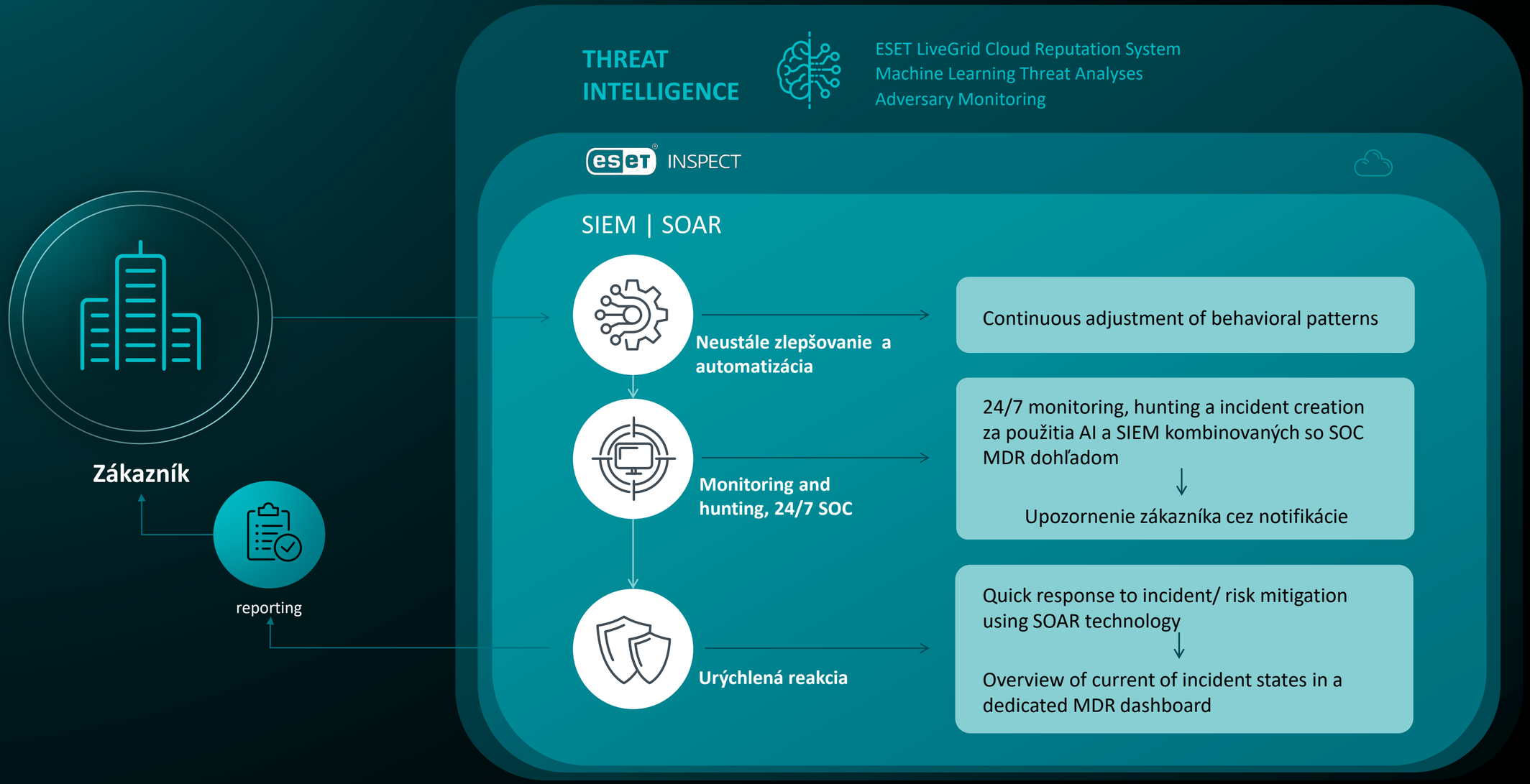
Skúsení ľudia

Cross-industry viditeľnosť

Úspora nákladov

Napĺňanie regulácií

Ako MDR funguje?



Čas na detekciu a reakciu je rozhodujúci

Zraniteľnosti sú často zneužité v priebehu niekoľkých hodín od ich objavenia

Zraniteľnosti sú často zneužité v priebehu niekoľkých hodín od ich objavenia

Záplaty sa reverzne analyzujú a exploity sa objavujú v priebehu dní ako súčasť nástrojov na zneužívanie

Zraniteľnosti sú často zneužité v priebehu niekoľkých hodín od ich objavenia

Záplaty sa reverzne analyzujú a exploity sa objavujú v priebehu dní ako súčasť nástrojov na zneužívanie

Čas od prvého narušenia po spustenie škodlivého softvéru je čoraz kratší

Čím je ESET MDR unikátna:

20 min.
čas potrebný na detekciu a reakciu

600+
R&D expertov v 13 centrách

24/7
threat management

35 rokov
Skúseností v cybersecurity

podpora
39 jazykov

110M+
Po celom svete

Ďakujem za pozornosť

Analýza malvéru pomocou jazykových modelov

EPI Kybernetická bezpečnosť 2024

STU FIIT

epi

SK NBÚ CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Obsah

1. Stav malvéru
2. Stav analýzy a detekcie malvéru
3. Súčasné využitie jazykových modelov
4. Problémy jazykových modelov
5. Možné riešenia

Bio

SK-CERT

Phd na FIIT STU

Malware

Ransomware

Mobile

IoT

Fileless malware

Obchádzanie analýzy a detekcie

Analýza

- statická a dynamická (aj hybridná)

Techniky:

- šifrovanie
- anti-debug
- detekcia sandboxu

Používanie AI na analýzu a detekciu

Najčastejšie algoritmy:

- kNN, NB, DT, RF ale aj CNN

Trénované na dátach

- hlavičky, importy, reťazce, bajty, opcody, systémové volania
- sieťová aktivita, súbory, registry, interakcia so službami, tvorba a ukončenie procesov

Používanie AI na analýzu a detekciu (2)

Je dosahovaná vysoká úspešnosť (skoro 100%) !

- má to ale nedostatky

Modely sú trénované aby mali výsledky aby vznikol článok…

1. malé datasety
2. neodrážajú aktuálny stav
3. žiadna verifikácia robustnosti detekcie

Jazykové modely

najčastejší je BERT

- pred-trénovaný model
- používajú sa aj jeho modifikácie - DistilBERT, RoBERTa, MalBERT, SemalBERT

Vision Transformer

Problémy (nielen) jazykových modelov

Datasety

Veľkosť vstupného kontextu

Problém s obchádzaním analýzy a detekcie

Potenciálne riešenia

Datasety - riešenie je veľmi otázne

Rozšírenie kontextu - LongFormer, Unlimiformer

Transformer trénovaný na špecifickom type dát

Ďakujem za pozornosť

Otázky?

ISACA Slovakia Chapter

Ako prepojiť hodnotenie súladu kybernetickej bezpečnosti, informačnej bezpečnosti a ochrany osobných údajov?

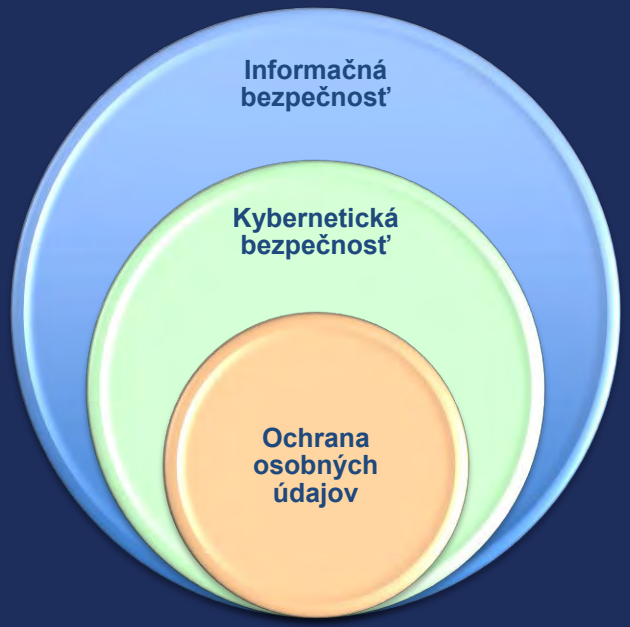
Ing. Eva Hlušková, PhD., audítor KB, Lead audítor ISO/IEC 27001, ISO/IEC 20000-1, ISO 22301, ISO 9001

člen ISACA Slovensko, CEO IQ ideas, s.r.o.

VI. ročník EPI konferencie – Kybernetická bezpečnosť 2024

30. 9. – 1. 10. 2024, Demänovská Dolina, Hotel Grand Jasná

Povinnosť monitorovania súladu



GDPR, čl. 5/Zákon č. 18/2018 Z.z.

- OÚ musia byť spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov ...
- Prevádzkovateľ je zodpovedný za takéto spracúvanie a musí vedieť tento súlad preukázať („zodpovednosť“).

Zákona č. 69/2018 Z.z., §20, ods.3p)

- Bezpečnostné opatrenia sa prijímajú a realizujú najmä pre oblasť: auditu, riadenia súladu a kontrolných činností ...

ISO/IEC 27001:2022

Organizácia musí vykonávať interné audity v plánovaných intervaloch s cieľom poskytnúť informácie o tom, či systém manažérstva informačnej bezpečnosti je v súlade ...

Požiadavky súladu s predpismi/normami

GDPR (Zákon č. 18/2018 Z.z. o OOÚ)

- Ochrana práv a slobôd fyzických osôb pri spracúvaní osobných údajov si vyžaduje, aby sa prijali **primerané technické a organizačné opatrenia** s cieľom zabezpečiť splnenie požiadaviek tohto nariadenia.
- Čl. 5f: Osobné údaje musia byť: spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom **primeraných technických alebo organizačných opatrení** („integrita a dôvernosť“).

Zákon č. 69/2018 Z.z. o KB

- § 19 (1)Povinnosti prevádzkovateľa základnej služby: Prevádzkovateľ základnej služby je povinný do 12 mesiacov odo dňa oznámenia o zaradení do registra prevádzkovateľov základných služieb prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 a sektorové bezpečnostné opatrenia, ak sú prijaté.
- § 20 (1) Bezpečnostnými opatreniami na účely tohto zákona sú úlohy, procesy, role a technológie v **organizačnej, personálnej a technickej oblasti**, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov.

Požiadavky súladu s predpismi/normami

ISO/IEC 27001:2022 – Príloha A (Information security, cybersecurity and privacy protection)

- A.5 Organizačné opatrenia
- A.6 Personálne opatrenia
- A.7 Fyzické opatrenia
- A.8 Technologické opatrenia

ISO/IEC 27018:2019 (protection of personally identifiable information (PII) in public clouds)

- Kap. 5 – 18 organizačné opatrenia, personálne opatrenia, fyzické opatrenia, technologické opatrenia
- Príloha A (A.2-A12) – rozšírené opatrenia OOÚ pre prevádzkovateľa cloud. služieb

ISO/IEC 27701:2019

(privacy information management)

- Kap. 6 – organizačné, personálne, technické opatrenia a opatrenia fyzickej bezpečnosti
- Kap. 7 a Príloha A – požiadavky na prevádzkovateľa
- Kap. 8 a Príloha B – požiadavky na sprostredkovateľa

Zodpovednosti za monitorovanie súladu

- GDPR: Čl. 39, ods. 1b) Úlohy **zodpovednej osoby: monitorovanie súladu** s týmto nariadením, s ostatnými právnymi predpismi Únie alebo členského štátu týkajúcimi sa ochrany osobných údajov a s pravidlami prevádzkovateľa alebo sprostredkovateľa v súvislosti s ochranou osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy personálu, ktorý je zapojený do spracovateľských operácií, a súvisiacich auditov;
- Zákon o KB: § 20, ods. 4: Bezpečnostné opatrenia musia zahŕňať najmenej: **určenie manažéra kybernetickej bezpečnosti**, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti,
- ISO/IEC 27001:2022: kap. 5.3 Vrcholový manažment musí **vymedziť zodpovednosť a právomoc** na: a) zabezpečenie, že systém manažérstva informačnej bezpečnosti spĺňa požiadavky normy (**manažér IB**)

Zodpovednosti za monitorovanie súladu

Manažér IB

ISO/IEC 27001:2022, kap. 7.2
Kompetentnosť

Manažér KB

Príloha č. 5 k Vyhláške č. 492/2022
Z. z. o znalostných štandardoch v oblasti kybernetickej bezpečnosti

Zodpovedná osoba za OOÚ

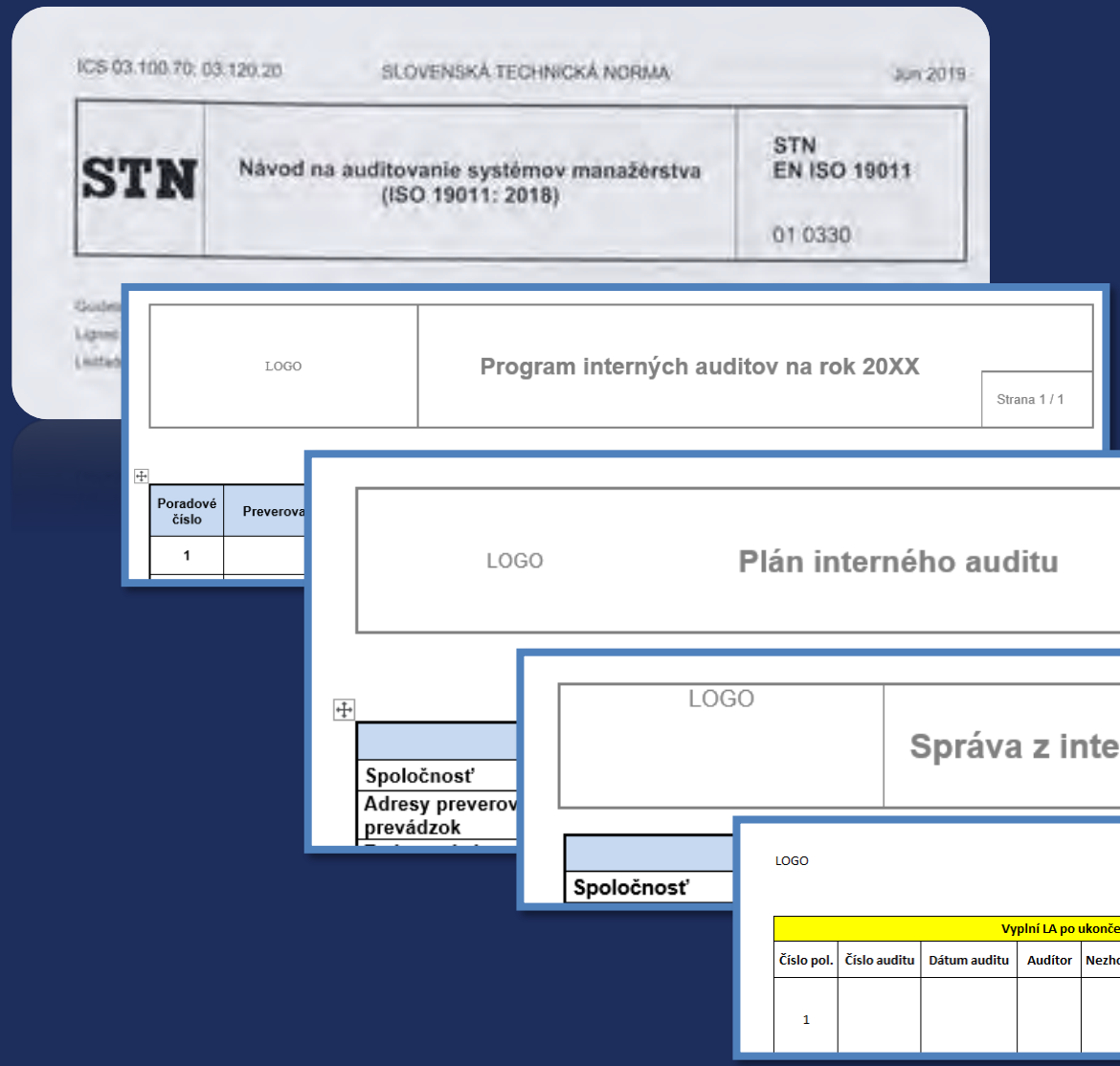
Zákon č. 18/2018, § 44
Určenie zodpovednej osoby, ods. 6

Môže to byť jedna osoba?

- Nezávislosť
- Nestrannosť
- Odbornosť
- Kvalifikácia (požiadavky GDPR, KB, ISO/IEC 27001)

Fórum informačnej bezpečnosti/Rada IB

Hodnotenie súladu = interný audit



Plánovanie integrovaného interného auditu KB / GDPR / ISO/IEC 27001:

- identifikovanie zistení z interných auditov
- sledovanie progresu zistení z interných auditov, dodržiavanie súladu s prepismi/normami

Výkon integrovaného interného auditu

	ISO/IEC 27001:2022	Zákon č. 69/2018 Z.z. (Vyhláška č. 362/2018)	Zákon č. 18/2018 Z.z.	ISO/IEC 27701:2019
Riadenie dodávateľov	5.19 Informačná bezpečnosť vo vzťahoch s dodávateľmi 5.20 Riešenie informačnej bezpečnosti v rámci dodávateľských dohôd 5.21 Riadenie informačnej bezpečnosti v dodávateľskom reťazci IKT 5.22 Monitorovanie, preskúmanie a riadenie zmien dodávateľských služieb 5.23 Informačná bezpečnosť pri používaní cloudových služieb	§ 20 ods. 3 písm. e) zákona – riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami § 19 ods. 2 zákona - analýza rizík dodávateľských služieb spôsobom podľa § 6 Vyhláška: § 9 Riadenie dodávateľských služieb	§ 33 Spoloční prevádzkovatelia § 34 Sprostredkovateľ § 35 Zástupca prevádzkovateľa alebo zástupca sprostredkovateľa § 36 Spracúvanie osobných údajov pod dohľadom prevádzkovateľa alebo sprostredkovateľa § 37 Záznamy o spracovateľských činnostiach, ods. 2 § 38 Právo na náhradu škody a zodpovednosť	6.12 Riadenie dodávateľov 6.12.1 1 Informačná bezpečnosť vo vzťahoch s dodávateľmi 6.12.2 Riadenie dodávateľských služieb A.7.2.6 Zmluvy so sprostredkovateľmi A.7.2.7 Spoločný prevádzkovateľ

Výkon integrovaného interného auditu

	ISO/IEC 27001:2022	Zákon č. 69/2018 Z.z. (Vyhláška č. 362/2018)	Zákon č. 18/2018 Z.z.	ISO/IEC 27701:2019
Riadenie incidentov	5.24 Plánovanie a príprava riadenia incidentov informačnej bezpečnosti 5.25 Posudzovanie a rozhodovanie o udalostiach informačnej bezpečnosti 5.26 Reakcia na incidenty informačnej bezpečnosti 5.27 Poučenie z incidentov informačnej bezpečnosti 5.28 Zhromažďovanie dôkazov 6.8 Hlásenie udalostí informačnej bezpečnosti	§ 20 ods. 3 písm. m) zákona – Riešenie kybernetických bezpečnostných incidentov § 24 Hlásenie kybernetických bezpečnostných incidentov prevádzkovateľom základnej služby Vyhláška: § 17 Riešenie kybernetických bezpečnostných incidentov Vyhláška č. 165 /2018 Z. z. - identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov	§ 39 c) Bezpečnosť spracúvania: proces obnovy dostupnosti osobných údajov a prístup k nim v prípade fyzického incidentu alebo technického incidentu § 40 Oznámenie porušenia ochrany osobných údajov úradu § 41 Oznámenie porušenia ochrany osobných údajov dotknutej osobe	6.13 Riadenie incidentov informačnej bezpečnosti 6.13.1.1 Zodpovednosť a postupy 6.13.1.2 Informovanie o udalostiach informačnej bezpečnosti 6.13.1.3 Informovanie o slabinách informačnej bezpečnosti 6.13.1.4 Posúdenie udalostí informačnej bezpečnosti a rozhodnutia o nich 6.13.1.5 Odpoveď na incidenty informačnej bezpečnosti 6.13.1.6 Poučenie z incidentov informačnej bezpečnosti 6.13.1.7 Zber dôkazov

Výkon integrovaného interného auditu

	ISO/IEC 27001:2022	Zákon č. 69/2018 Z.z. (Vyhláška č. 362/2018)	Zákon č. 18/2018 Z.z.	ISO/IEC 27701:2019
Riadenie technických zraniteľností	5.7 Spravodajstvo o hrozbách 8.8 Riadenie technických zraniteľností 8.19 Inštalácia softvéru na prevádzkové systémy	§ 20 ods. 3 písm. g) zákona – Technické zraniteľnosti informačných systémov Vyhláška: § 11 Technické zraniteľnosti informačných systémov	§ 11 Zásada integrity a dôvernosti § 31 Prevádzkovateľ - prevádzkovateľ je povinný prijať vhodné technické a organizačné opatrenia § 32 Špecificky navrhnutá a štandardná ochrana osobných údajov § 39 Bezpečnosť spracúvania, ods. 1	6.9.6 Riadenie technických zraniteľností 6.9.6.1 Riadenie technickej zraniteľnosti 6.9.6.2 Obmedzenia pri inštalácii softvéru

ISACA
Slovakia Chapter

Ďakujem za pozornosť

Ing. Eva Hlušková, PhD., hluskova@iqideas.sk

cyllium

LEAD YOUR BUSINESS PROTECTED

VI. ročník EPI KONFERENCIE Kybernetická bezpečnosť 2024

Nie je audit ako audit

30.9-1.10. 2024

Michal Ďorda, Audítor kybernetickej bezpečnosti, Partner pre expertné služby, Cyllium

MICHAL ĎORDA

IT a bezpečnostný audítor a konzultant

(1) **Audítorská spoločnosť** je organizácia zastrešujúca a zoskupujúca jednotlivcov vykonávajúcich audity.

(2) **Audítor** je jednotlivec so:

- > Vzdelaním a dokladom o ukončení štúdia
- > Praxou a skúsenosťami v oblasti auditu
- > Znalosťami v oblasti auditu, doložené medzinárodne platným certifikátom
- > Nezávislý
- > Objektívny a bezúhonný

Audítori nehryzú !

LEAD YOUR BUSINESS PROTECTED

OTÁZKY DO PUBLIKA

Koľkí z Vás sú audítori?

Koľkí z Vás sú auditovaní?

Koľkí z Vás sa zúčastnia na max. 1 audite za rok?

Koľkí z Vás sa zúčastnia na viac 1 audite za rok?

Koľko FTE sa venuje auditom?

LEAD YOUR BUSINESS PROTECTED

NIE JE AUDIT AKO AUDIT (OBSAH)

01 Od posúdenia až po certifikáciu

- Posúdenie
- Testovanie
- Audit
- Certifikácia

02 Rôzne typy auditov

- Procesné
- Technické
- Personálne

03 Prieniky a rozdiely medzi auditmi

- Najčastejšie testovania a audity
- Praktické skúsenosti audítora

LEAD YOUR BUSINESS PROTECTED

01/ METÓDY OVERENIA ÚROVNE BEZPEČNOSTI

Štyri základné prístupy ako sa môže subjekt uistiť o požadovanej úrovni bezpečnosti:

> **Posudzovanie** – Dokazovanie, že sa splnili určené požiadavky týkajúce sa objektu posudzovania.

> **Testovanie** – Proces, v ktorom je jeden alebo viac objektov posudzovania vystavených podľa opakovateľného postupu určitým podmienkam, s cieľom porovnať ich aktuálne a očakávané charakteristiky.

> **Audit** – Systematický, nezávislý a zdokumentovaný proces získavania záznamov, konštatovaní faktov alebo iných dôležitých informácií a ich objektívneho posudzovanie s cieľom určiť rozsah, v akom sa splnili určené požiadavky.

> **Certifikácia (Posudzovanie zhody)** – Atestácia nezávislým akreditovaným orgánom posudzovanie zhody, týkajúca sa charakteristík objektu posudzovania.

LEAD
YOUR
BUSINESS
PROTECTED

02/ TYPY OVERENÍ A AUDITOV BEZPEČNOSTI

Procesné:

> Efektívnosť a implementáciu procesov a postupov (COBIT, a iné)
> Audit systému riadenia informačnej bezpečnosti (ISO 27001, a iné)
> Audit súladu s legislatívou (zákony, vyhlášky, smernice, a iné)
> Audit projektu implementácie systému (KPI, riziká, požiadavky)

Technické:

> Audit fyzickej bezpečnosti
> Analýza bezpečnostnej architektúry
> Konfiguračné previerky systémov, aplikácií, sieťových prvkov
> Audit bezpečnosti aplikácie
> Penetračné testovanie (OSSTMM, OWASP, a iné)
> Audit zdrojového kódu

Personálne:

> Personálna previerka osôb
> Popis charakteru a kvality práce
> Sociálne inžinierstvo

LEAD
YOUR
BUSINESS
PROTECTED

03/ Najčastejšie testovanie a audity

AUDIT KYBERNETICKEJ BEZPEČNOSTI

Prevádzkovateľ základnej služby je povinný **preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených Zákonom o Kybernetickej Bezpečnosti** vykonaním auditu kybernetickej bezpečnosti v rozsahu stanovenom podľa Vyhlášky o audite kybernetickej bezpečnosti.

Audit kybernetickej bezpečnosti vykonáva certifikovaný audítor kybernetickej bezpečnosti.
-> cca. 51 za KCCKB + cca. 34 za TÜV-SÚD + 53 právnických osôb na webe NBÚ

1. Žiadosť o audit kybernetickej bezpečnosti
2. Výkon auditu Kybernetickej bezpečnosti podľa ZoKB
3. Záverečná správa o výsledkoch auditu

LEAD YOUR BUSINESS PROTECTED

LIMITOVANÁ IT PREVIERKA AKO SÚČASŤ ŠTATUTÁRNEHO AUDITU (1/2)

Zákon č. 431/2002 o účtovníctve požaduje **riadnu alebo mimoriadnu individuálnu účtovnú závierku** overenú **štatutárnym audítorom** pre rôzne účtovné jednotky.

Štatutárny audítor je fyzická osoba, ktorá je zapísaná v zozname štatutárnych audítorov, ktorý vedie úrad, a má oprávnenie na vykonávanie štatutárneho auditu (ďalej len „licencia“).

> Člen auditného tímu - IT expert

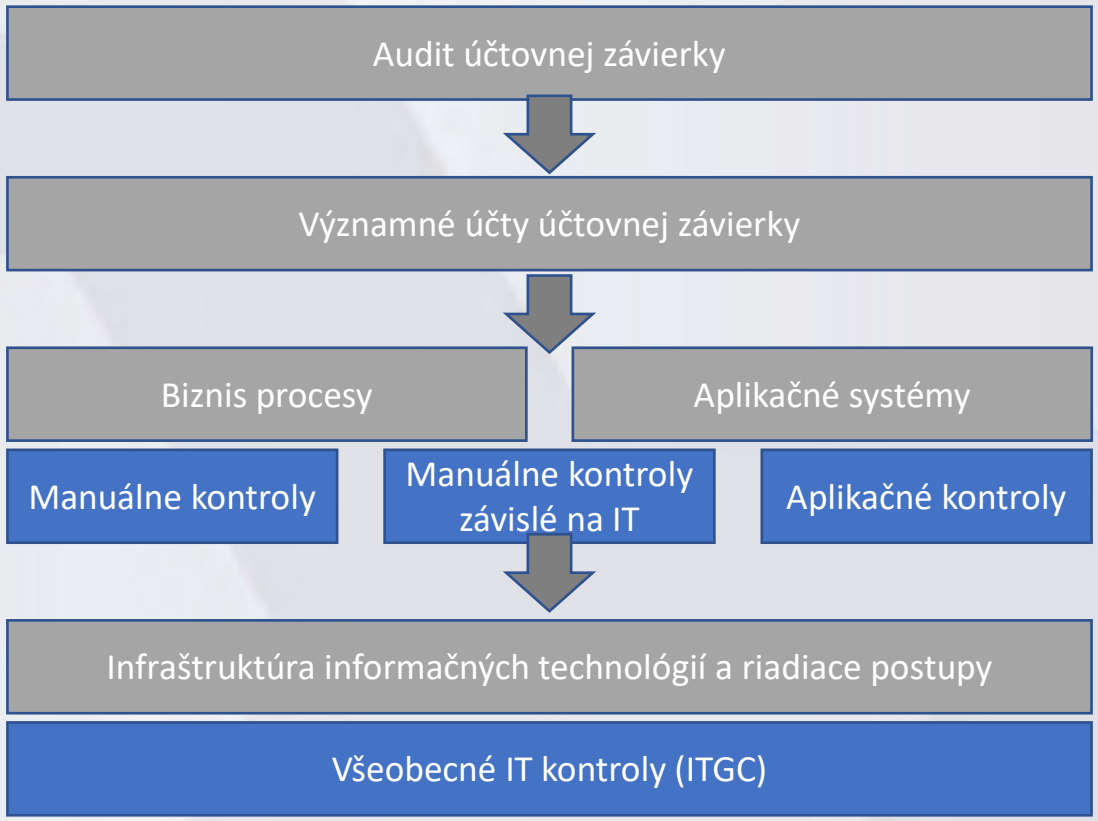
Medzinárodný audítorský štandard 315 (revidované znenie 2019),
Identifikácia a posúdenie rizika významných nesprávností:

> **Príloha 5:** Aspekty dôležité pri oboznámení sa s informačnými technológiami používanými účtovnou jednotkou (IT)

> **Príloha 6:** Aspekty dôležité pri oboznámení sa so všeobecnými IT kontrolami

LEAD YOUR BUSINESS PROTECTED

LIMITOVANÁ IT PREVIERKA AKO SÚČASŤ ŠTATUTÁRNEHO AUDITU (2/2)



Substantívne procedúry

Postupy testovania kontrol

LEAD YOUR BUSINESS PROTECTED

CERTIFIKAČNÝ AUDIT PODĽA TECH. NORIEM

Norma ISO/IEC 27001:2022 špecifikuje požiadavky na zostavenie, implementáciu, prevádzku, monitorovanie, preskúmanie a zlepšovanie systému manažérstva informačnej bezpečnosti. Cieľom auditu je deklarovať **zavedenie systematického prístupu v oblasti bezpečnosti informácií v organizácií a plnenie požiadaviek medzinárodnej normy**.

Certifikačný audit ISMS vykonávajú akreditované certifikačné orgány.

-> 12 za SNAS pre ISO 27k, 4 za SNAS pre ISO 22301, 2 za SNAS pre ISO 20000-1 a ďalšie v iných krajinách

Priebeh certifikácie:

- Certifikačný audit 1. stupeň: Posúdenie dokumentácie + 2. stupeň: Posúdenie procesov -> Získanie certifikátu
- 1. Dozorný audit
- 2. Dozorný audit
- Recertifikačný audit

LEAD YOUR BUSINESS PROTECTED

INÉ IT A BEZPEČNOSTNÉ AUDITY

Napríklad:

- **Overenie bezpečnosti IS**
- **Audit bezpečnostných opatrení podľa RTS SCA (PSD2)**
- **SWIFT nezávislé hodnotenie SWIFT Customer Security Program (Customer Security Controls Framework)**
- **PCI audit**
- **Testovanie digitálnej prevádzkovej odolnosti (DORA)**
- **TISAX audit**
- **a rôzne iné ...**

LEAD
YOUR
BUSINESS
PROTECTED

IT A BEZPEČNOSTNÝ AUDIT

STU FEI I-ITBA

Študijný predmet poskytuje študentom komplexné a aktuálne znalosti v oblasti **informačných technológií a auditov bezpečnosti**. V priebehu dvanástich prednášok budú študenti uvedení do kľúčových tém, ako sú základy bezpečnosti informačných systémov, normy a regulácie, bezpečnostné politiky a postupy, identifikácia a autentifikácia, a testovanie bezpečnosti. Špeciálne prednášky budú venované aj konkrétnym oblastiam, ako sú sieťová bezpečnosť, audit cloudu a legislatíva v oblasti IT a bezpečnostného auditu.

LEAD
YOUR
BUSINESS
PROTECTED

cyllium

LEAD YOUR BUSINESS PROTECTED

Ďakujem za pozornosť

www.cyllium.eu

Zborník z konferencie EPI Kybernetická bezpečnosť 2024

Dátum konania: 30. 9. - 1. 10. 2024, Hotel Grand Jasná****

Vydavateľ: Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Rok vydania: 2024

Editori: Miroslav Havelka, Ivan Makatura

ISBN: 978-80-69011-43-4

EAN: 9788069011434

Vzor citácie:

Zborník z konferencie. In *EPI Kybernetická bezpečnosť 2024* [online]. Bratislava: KCCKB, 2024. 418. ISBN 978-80-690-1143-4. Dostupné na internete: <https://cybercompetence.sk>.

Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti