SPCSS

Státní pokladna
Centrum sdílených služeb

Poskytovatel služeb datových center

a služeb kybernetické bezpečnosti

pro státní správu

Adversary Emulation
v rámci Šedé zóny aktivní kybernetické obrany

SPCSS – Ondřej Nekovář, Jan Pohl

e-government 20:10, Mikulov

07. - 08. 09. 2021

Státní pokladna Centrum sdílených služeb s. p.

SPCSS

Intro

Stage 1/7

Intro

About Us

- **Ondřej Nekovář**
- **Jan Pohl**

Státní pokladna Centrum sdílených služeb, s. p.

Intro

Our topics

- **DC, Cloud, Hybrid-cloud bezpečnost**

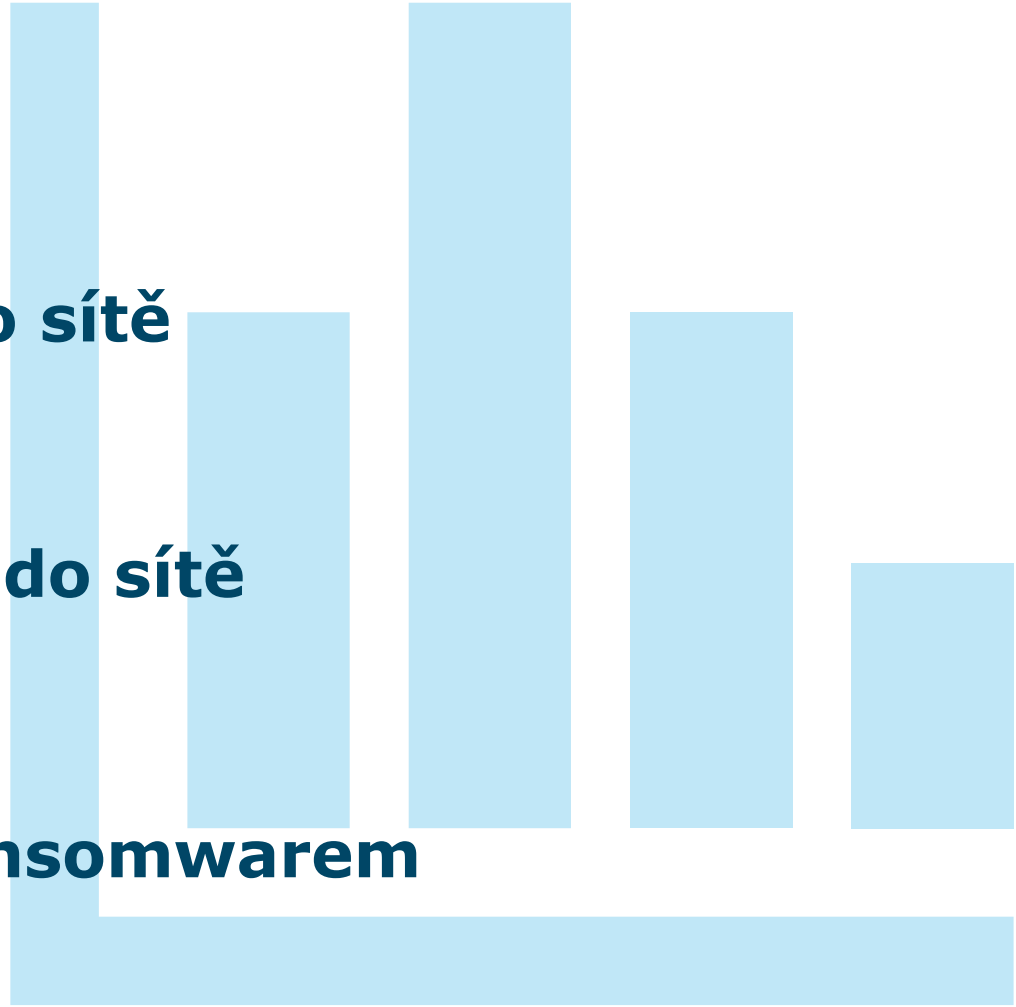
- **Aktivní kybernetická obrana**

Adversary

Stage 2/7

Adversary
Statistiky

- **3950** potvrzených průniků do sítě
- **9** hodin na provedení průniků do sítě
- **20** mld. USD škod pouze ransomwarem



Defender

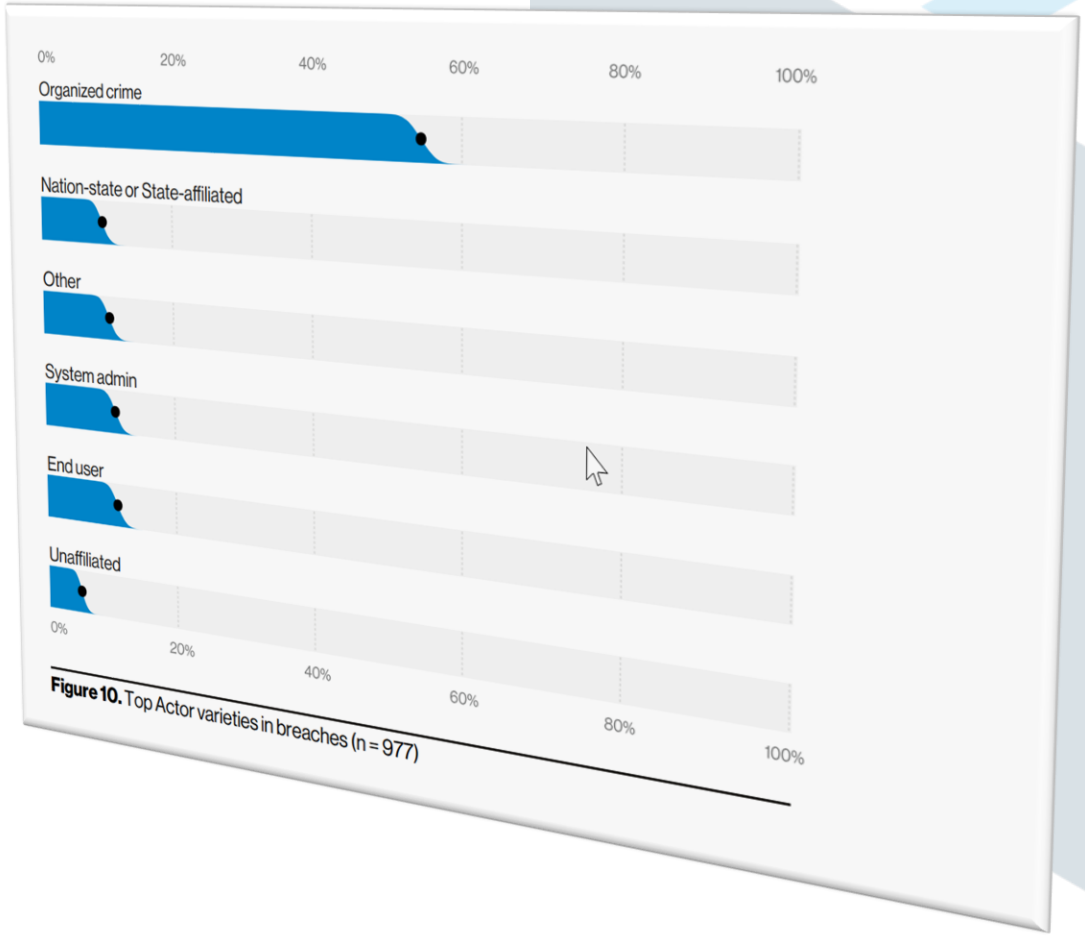
Stage 3/7

Státní pokladna Centrum sdílených služeb s. p.

SPCSS

Defender
Statistiky

- **Pouze reaktivní prvky**
- **Etický kodex**
- **Legislativa**



Verizon Data Breach
Investigations Report 2020

Active Cyber Defense

Stage 4/7

Státní pokladna Centrum sdílených služeb s. p.

SPCSS

Active Cyber Defense

?

Co je aktivní kybernetická obrana?

SPCSS

Active Cyber Defense

Proč aktivní obrana funguje?

- **Pozornost**
- **Energie/zdroje**
- **Nejistota**
- **Získání informací**

Active Cyber Defense

Rozdělení obrany

Reaktivní obrana

Antivirus, Firewall, SIEM, incident response ...

Aktivní obrana – Šedá zóna

Beacons, Botnet, Deception . . .

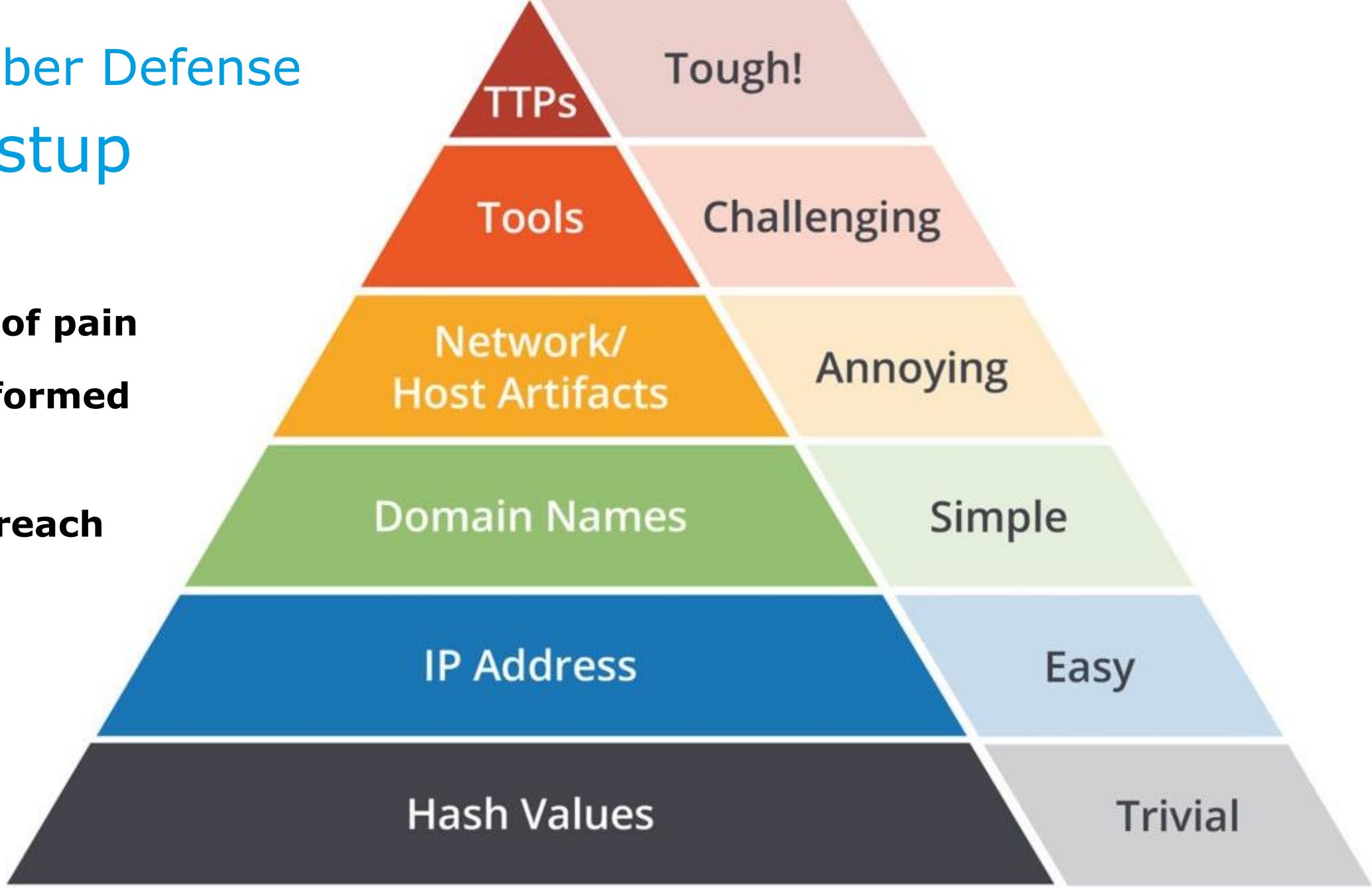
Ofenzivní operace

Hacking back, cyber operations ...

SPCSS

Active Cyber Defense
Náš přístup

- **Pyramide of pain**
- **Threat Informed Defense**
- **Assume breach**



Source: David J. Bianco, personal blog

Gray zone of Active Cyber Defense

Stage 5/7

Státní pokladna Centrum sdílených služeb s. p.

Gray zone of Active Cyber Defense

Deterrence	Botnet Takedowns
Intelligence Sharing	Sanctions, Indictments & Remedies
Deception	Rescue Missions
Threat hunting	Ransomware
Tarpits, Snadboxes & Honeypots	
Red Teaming	
Beacons	

Gray zone of ACD

Deterrence

- **Zastrašování**
- **Barnes case**
- **FBI warning**

Gray zone of ACD
Intellingence Sharing

Passive

Intelligence

- Threath sharing platforms
- OSINT

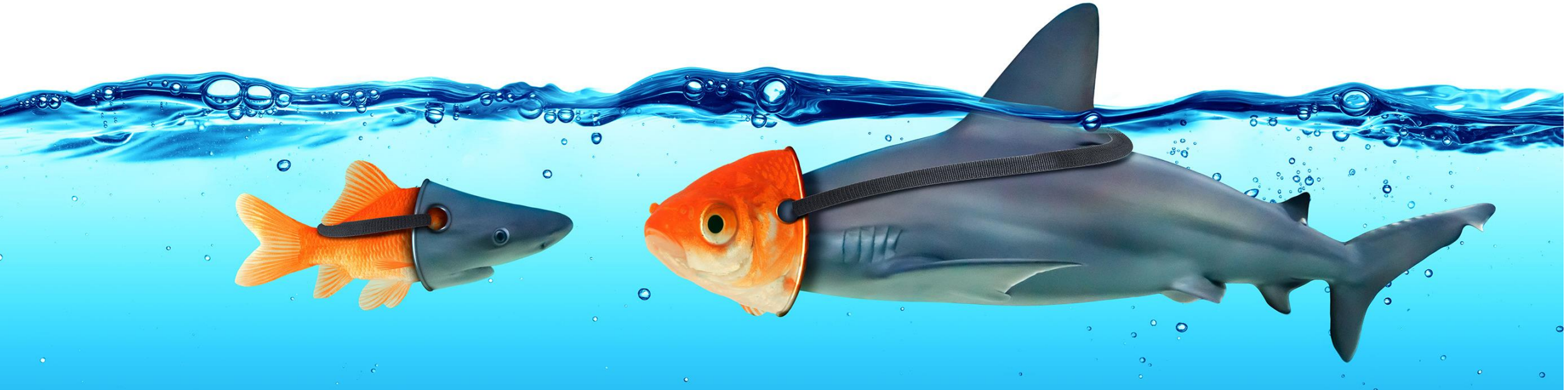
Counter

Intelligence

Gray zone of ACD

Deception

- **Deception**
- **Denial**
- **Counterdeception**
- **Counter-deception**



Gray zone of ACD

Threat hunting

- Proaktivní vyhledávání
- Vytváření hypotéz chování

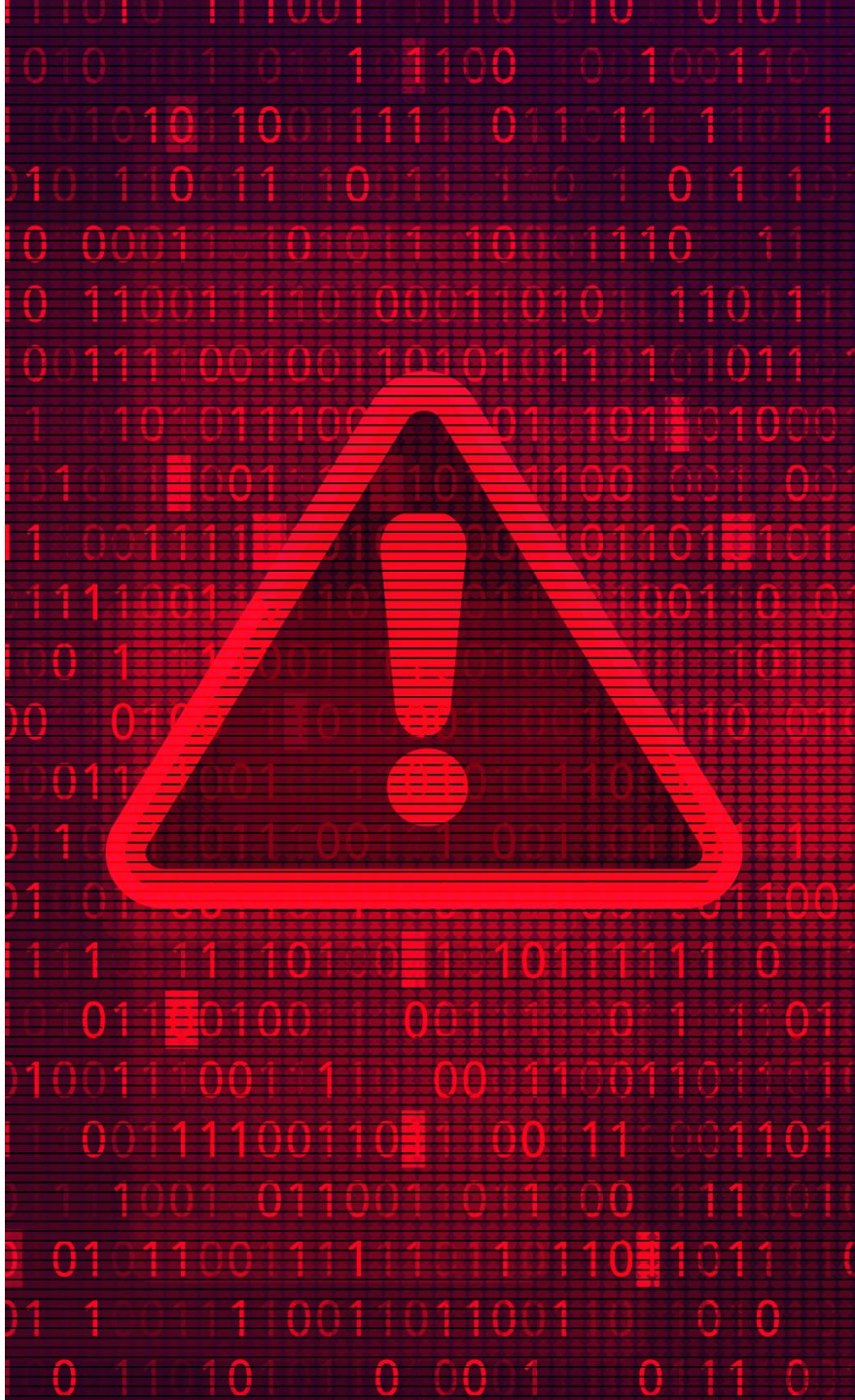
Gray zone of ACD
Tarpits, Sandboxes & Honeypots

- **Klasické vnímání aktivní obrany**
- **Nástroje**

Gray zone of ACD

Red Teaming

- **Threat Emulation**
- **Adversary Emulation**



Gray zone of ACD

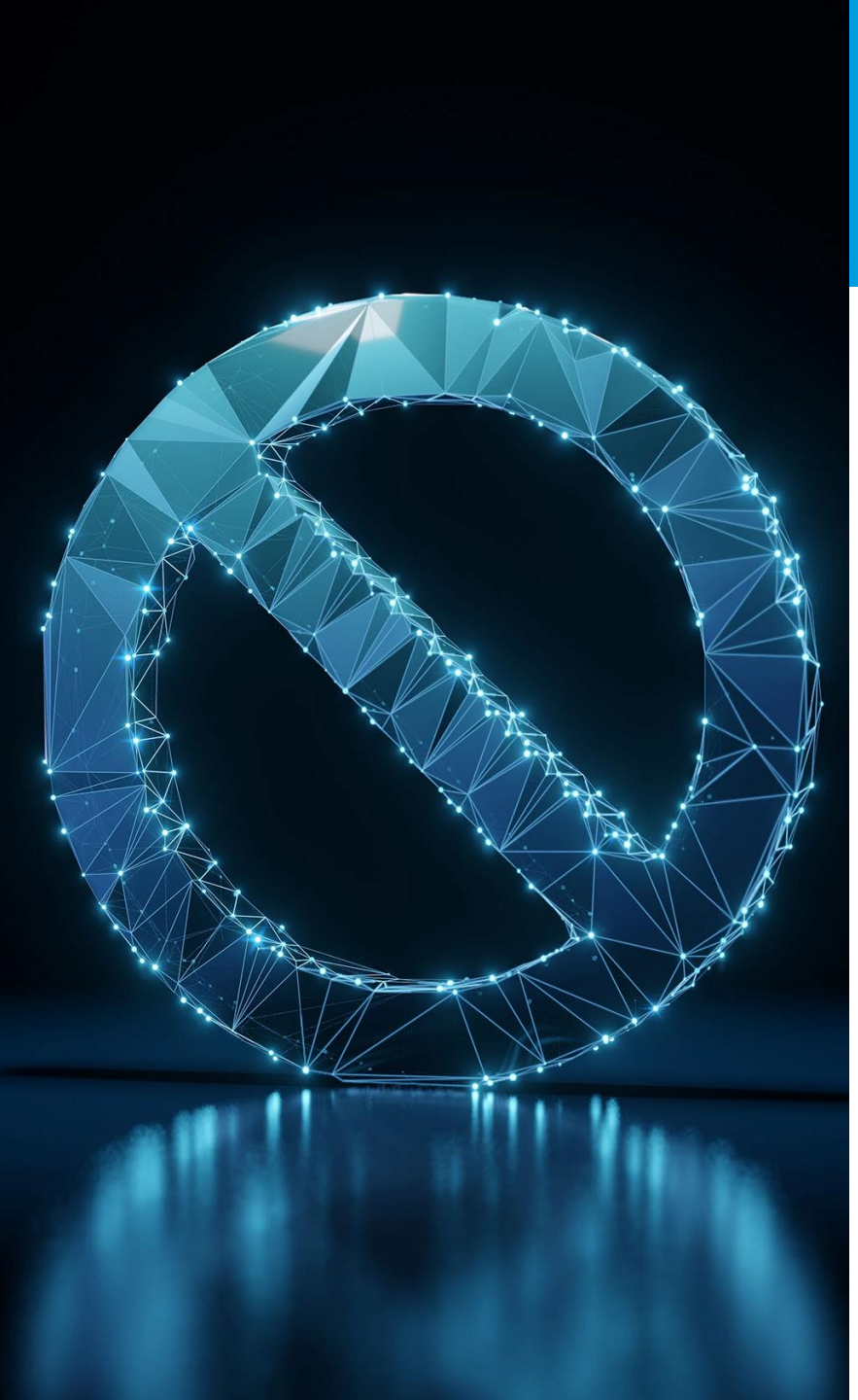
Beacons

- **Notify**
- **Inform**

Gray zone of ACD

*** Botnet Takedowns

- **Nutná legislativní podpora**
- **Malicious behaviour**
- **Ohrožení kritické infrastruktury**



Gray zone of ACD

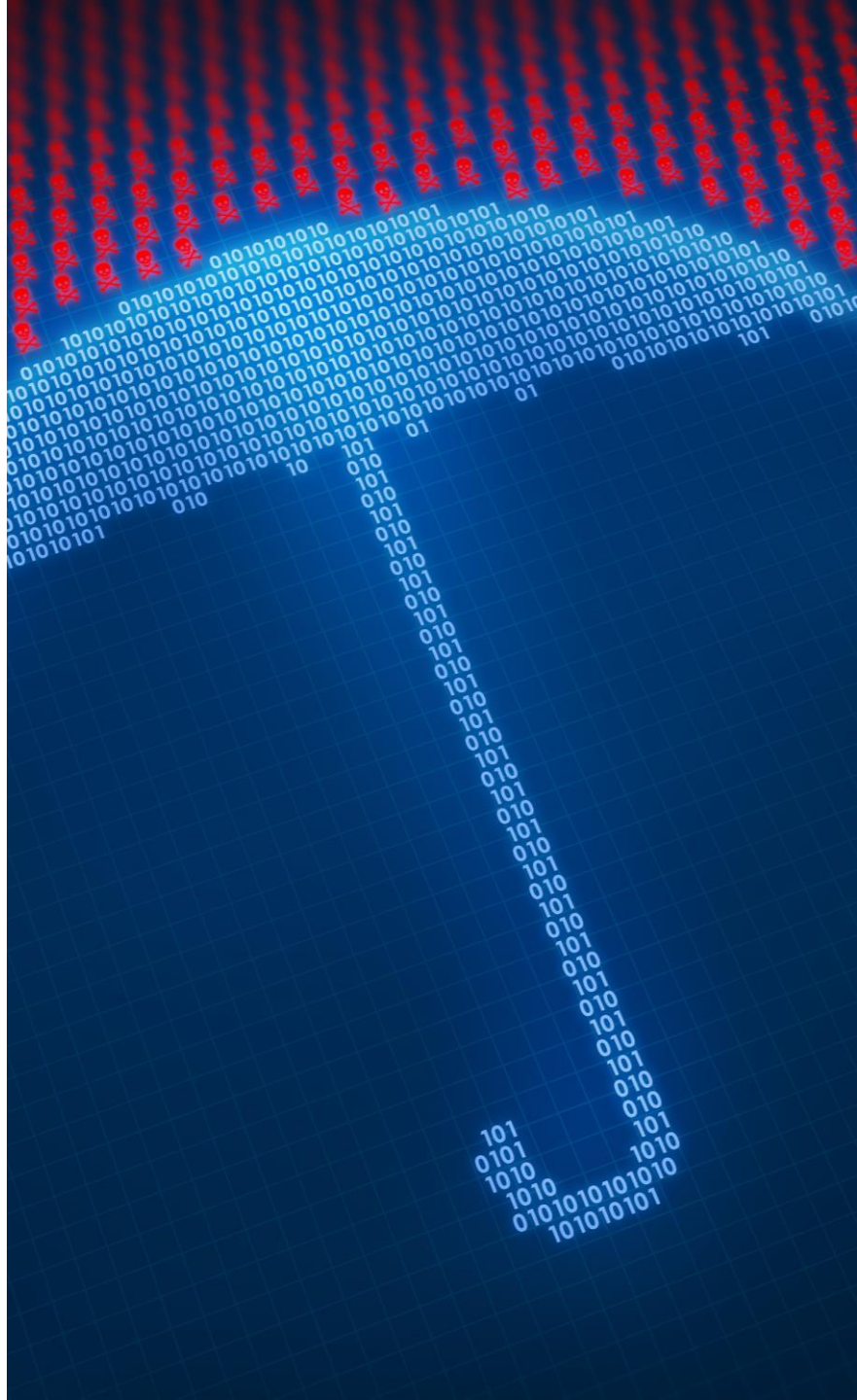
Beacons

- **Nutná legislativní podpora**
- **Sankce**
- **Restrikce**

Gray zone of ACD

*** Rescue Missions

- **Nutná legislativní podpora**
- **Hacking back**
- **Cyber operations**



Gray zone of ACD

*** Ransomware

- **Nutná legislativní podpora**
- **Whitehat ransomware**
- **Humanitární ransomware**

Red Teaming

Stage 6/7

Red Teaming

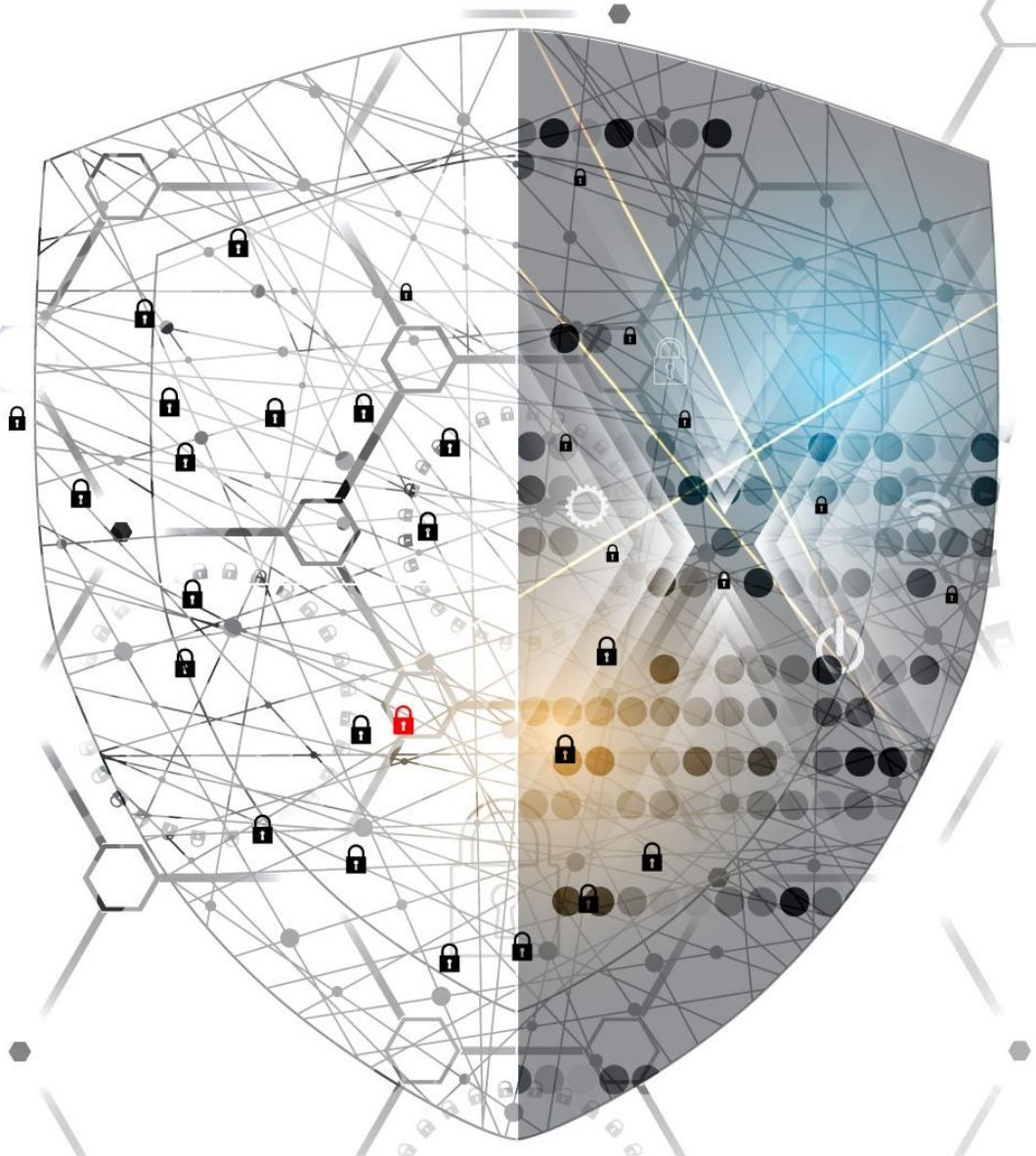
"Nestoupáme k výšinám našich očekávání, ale klesáme s kvalitou našeho tréninku„

Archilochus, 650 BC

Red Teaming

The prostředí

- **Hybrid znamená lateral**
- **Hybrid znamená out of reach**
- **Hybrid znamená cizí**



Red Teaming
High level

- Vulnerability management
- Penetration testing
- Adversary emulation

Red Teaming
Tools of Trade

- **Engage, D3fend, Att&ck Navigator/Workbench**
- **Vectr**
- **CALDERA, C2, Cobalt Strike**

Red Teaming
The analýza

- **Att&ck Framework**
- **DFIR reporty, blogy**
- **MISP**

Red Teaming
The výstup

- **Mindset**
- **Threat informed defense**
- **Pokrytí bílých míst**

Red Teaming

Back to Gray zone of AD

Deterrence	Botnet Takedowns
Intelligence Sharing	Sanctions, Indictments & Remedies
Deception	Rescue Missions
Threat hunting	Ransomware
Tarpits, Snadboxes & Honeypots	
Red Teaming	
Beacons	

EoF

Stage 7/7

EoF

Open sources

- **Mitre.org (Att&ck, CAR, Shield, Caldera)**
- **OSINT framework**

- **CIRCL (MISP, AIL, CyCAT . . .)**
- **HelpSystems (CobaltStrike)**

EoF

Open sources

- https://github.com/mitre
- https://github.com/SecurityRiskAdvisors/VECTR
- https://www.cobaltstrike.com
- https://mitre-attack.github.io/attack-navigator
- https://github.com/yeyintminthuhtut/Awesome-Red-Teaming
- https://github.com/infosecn1nja/Red-Teaming-Toolkit
- https://attack.mitre.org/

EoF

Community

Defcon Group 420 Czech republic

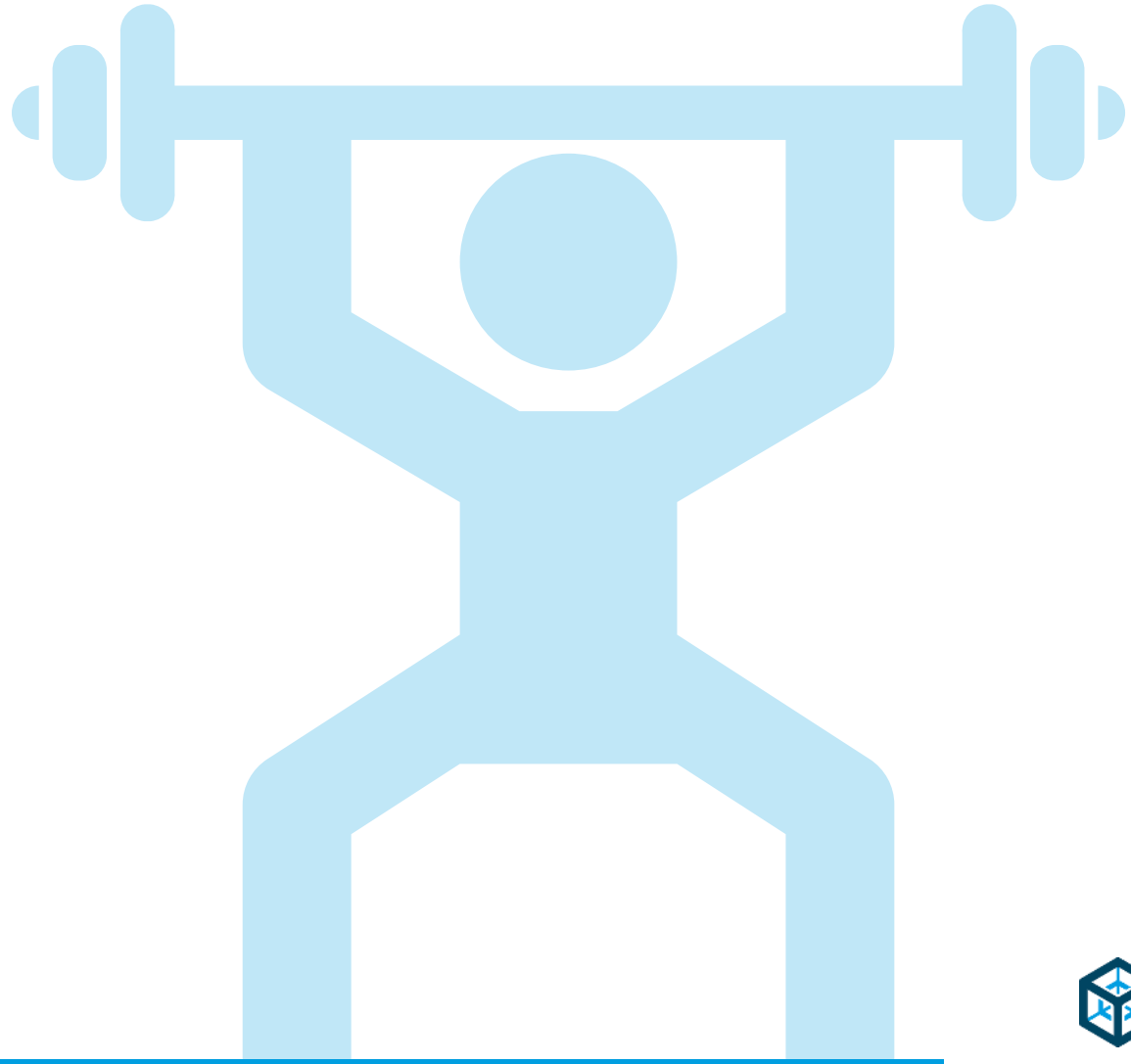
- www.DCG420.org

MeetUps

- DCG420.eventbrite.com

EoF

Our Training



MISP Training 2021

- 4. ročník - MISP, AIL, CyCAT
- Zdarma – On-site/On-line
- 14.-15.9.2021, anglicky

Registrace

- www.spcss.cz/misp

EoF

Our Conference

Fórum aktivní kybernetické obrany 2021

- 2. ročník
- Listopad 2021, česky

Registrace

- E-mail csirt@spcss.cz

EoF

Conferences of others

V roce 2021 se s námi ještě můžete potkat:

- ISSS 2021 – Detterence
- CyberCon 2021 – Ransomware

EoF

Keep in touch

- **Web www.spcss.cz/csirt**
- **E-mail csirt@spcss.cz**
- **Twitter @csirtspcss**

Děkujeme za pozornost

Q & A