



SPCSS

Státní pokladna
Centrum sdílených služeb

**Poskytovatel služeb datových center
a služeb kybernetické bezpečnosti
pro státní správu**

Deterrence v rámci Šedé zóny aktivní kybernetické obrany



SPCSS – Ondřej Nekovář, Jan Pohl
ISSS 2021 – Hradec Králové
20. - 21. 09. 2021

Intro

Stage 0x1

About Us

- **Ondřej Nekovář**
- **Jan Pohl**

- **Státní pokladna Centrum sdílených služeb, s. p.**

Our topics

- **DC, Cloud, Hybrid-cloud bezpečnost**
- **Aktivní kybernetická obrana**



Active Cyber Defense

Stage 0x2

Co je aktivní kybernetická obrana?

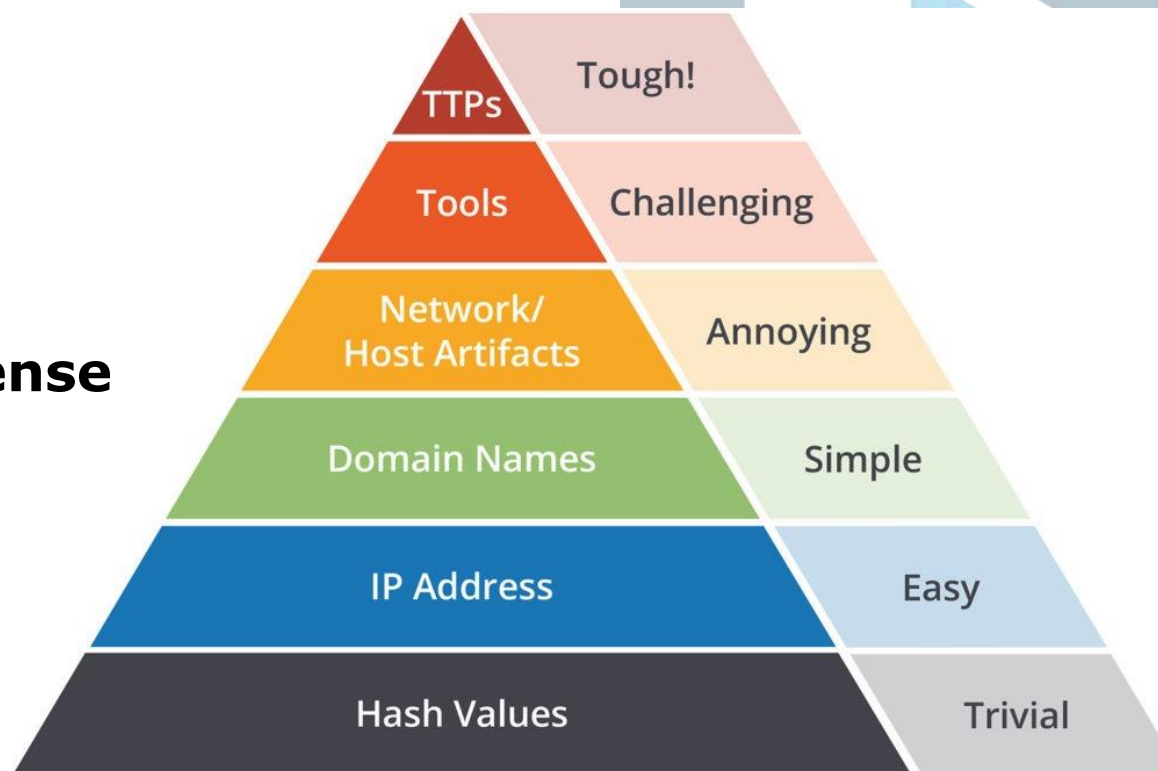


Rozdělení obrany

Reaktivní obrana	Antivirus, Firewall, SIEM, incident response ...
Aktivní obrana – Šedá zóna	Beacons, Botnet, Deception . . .
Ofenzivní operace	Hacking back, cyber operations ...

Náš přístup

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



Source: David J. Bianco, personal blog

Gray zone of Active Cyber Defense

Stage 0x3

Gray zone of ACD

Deterrence

Intelligence Sharing

Deception

Threat hunting

Tarpits, Snadboxes & Honeypots

Red Teaming

Beacons

Botnet Takedowns

Sanctions, Indictments & Remedies

Rescue Missions

Ransomware

Deterrence

Stage 0x4

Deterrence

- **Tradiční pojetí**
- **Výzvy kybernetického prostoru**
- **Možnosti uplatnění deterrence**



How to deter

- **Deterrence by Retaliation**
- **Deterrence by Denial**
- **Deterrence by Entanglement**



Deterrence by Retaliation

- **Obava z odplaty**
- **Sony entertainment**
- **Lze těžko využít**



Deterrence by Denial

- **Nepřiznáme provedený útok**
- **Nepřiznáme skutečný dopad**
- **US Office of Personal Management**



Deterrence by Entanglement

- **Dohoda s útočníkem**
- **Obamova cesta**
- **Je špatné to použít**

Yes, we can

- **Deterrence by Retaliation**
 - Oznámení
- **Deterrence by Denial**
 - Falešné prostředí
- **Deterrence by Entanglement**
 - Ne!



EoF

A person in a futuristic, glowing suit holding a sword in the rain. The scene is illuminated with vibrant blue and green lights, creating a high-tech, cyberpunk atmosphere. The person is wearing a mask with glowing green accents and a suit with various glowing elements. The sword is held across their back, and the rain is falling heavily around them.

Stage 0x5

Our Conference

Fórum aktivní kybernetické obrany 2021

- **2. ročník**
- **Listopad 2021**

Registrace

- **E-mail eventy@spcss.cz**

Conferences of others

V roce 2021 se s námi ještě můžete potkat:

- **CyberCon 2021 – Ransomware**



Keep in touch

- **Web www.spcss.cz/csirt**
- **E-mail csirt@spcss.cz**
- **Twitter [@csirtspcss](https://twitter.com/csirtspcss)**

Děkujeme za pozornost

Q & A