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

Státní pokladna Centrum sdílených služeb s. p.

SPCSS

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

Státní pokladna Centrum sdílených služeb s. p.

SPCSS

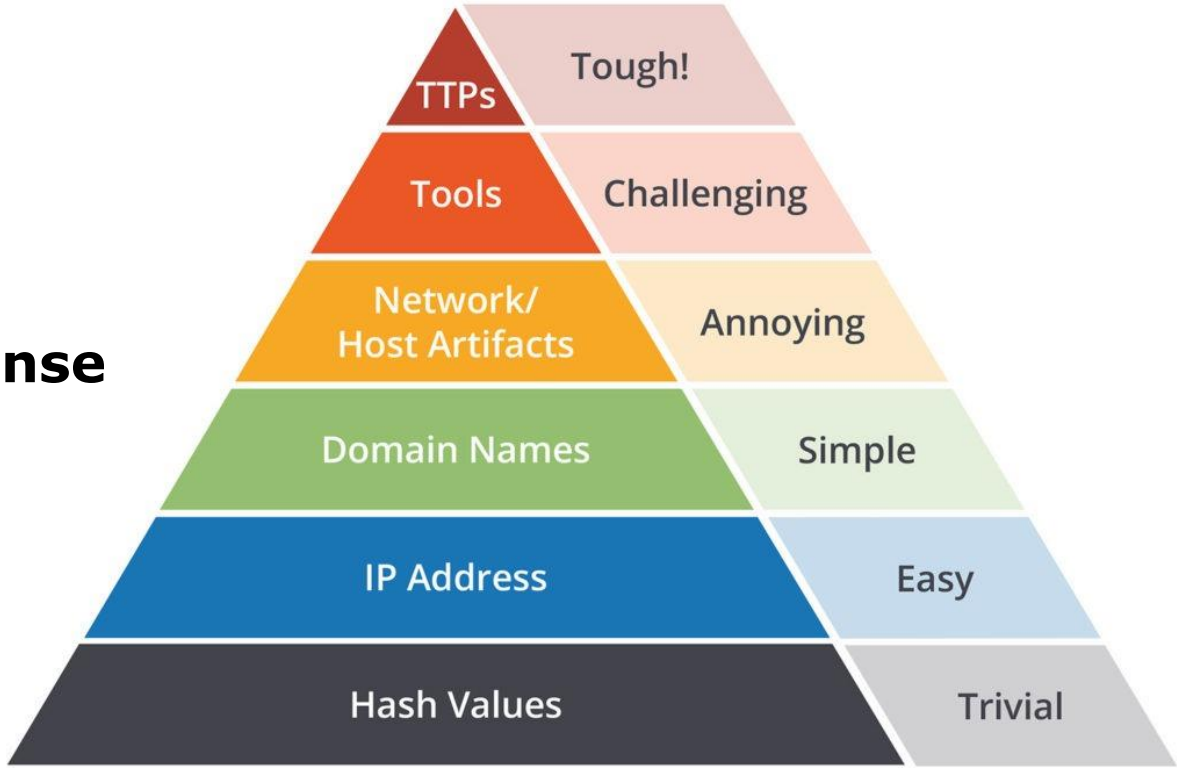
Co je aktivní kybernetická obrana?

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

Státní pokladna Centrum sdílených služeb s. p.

SPCSS

Gray zone of ACD

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

Deterrence

Stage 0x4

Státní pokladna Centrum sdílených služeb s. p.

SPCSS

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

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**

Děkujeme za pozornost

Q & A