Aktivní kybernetická obrana

Beacon jako nástroj aktivní obrany

- Ondřej Nekovář, Jan Pohl -

Státní pokladna Centrum sdílených služeb, s. p.

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x1

Intro

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x2

Adversary

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x2

Adversary

Statistiky

- **2216** potvrzených průniků do sítě
- **15 hodin** na provedení průniků do sítě
- **817 mld. USD** škod
- **1,7 mld. účtů** bylo prolomeno

Verizon Bread report 2018, Blade Report 2018, Global Affaris 2018, Business insider 2018

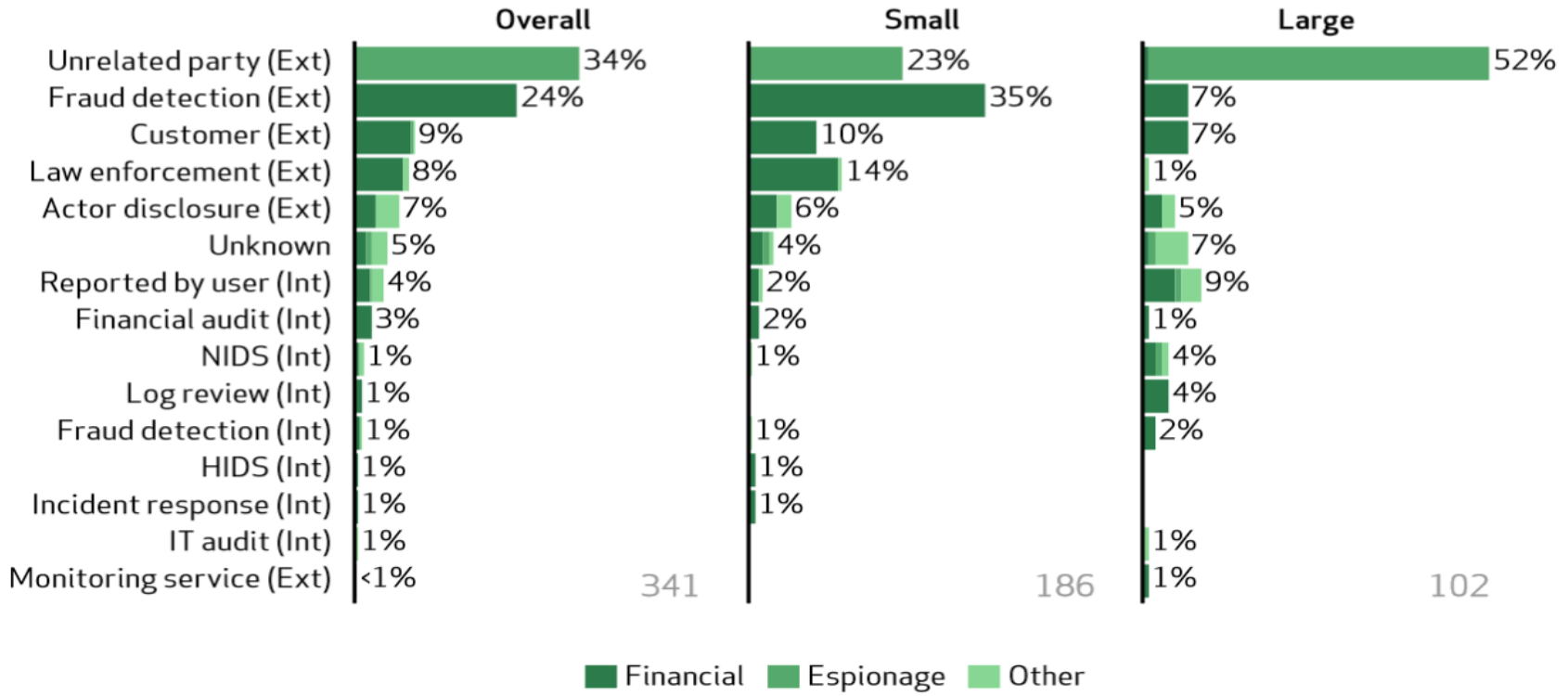
Stage 0x3
Defender

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x3

Defender

Figure 44: Discovery methods



Verizon Data Breach Investigations Report 2013

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x4

Active defense

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x4

Active defense

Co je aktivní obrana?

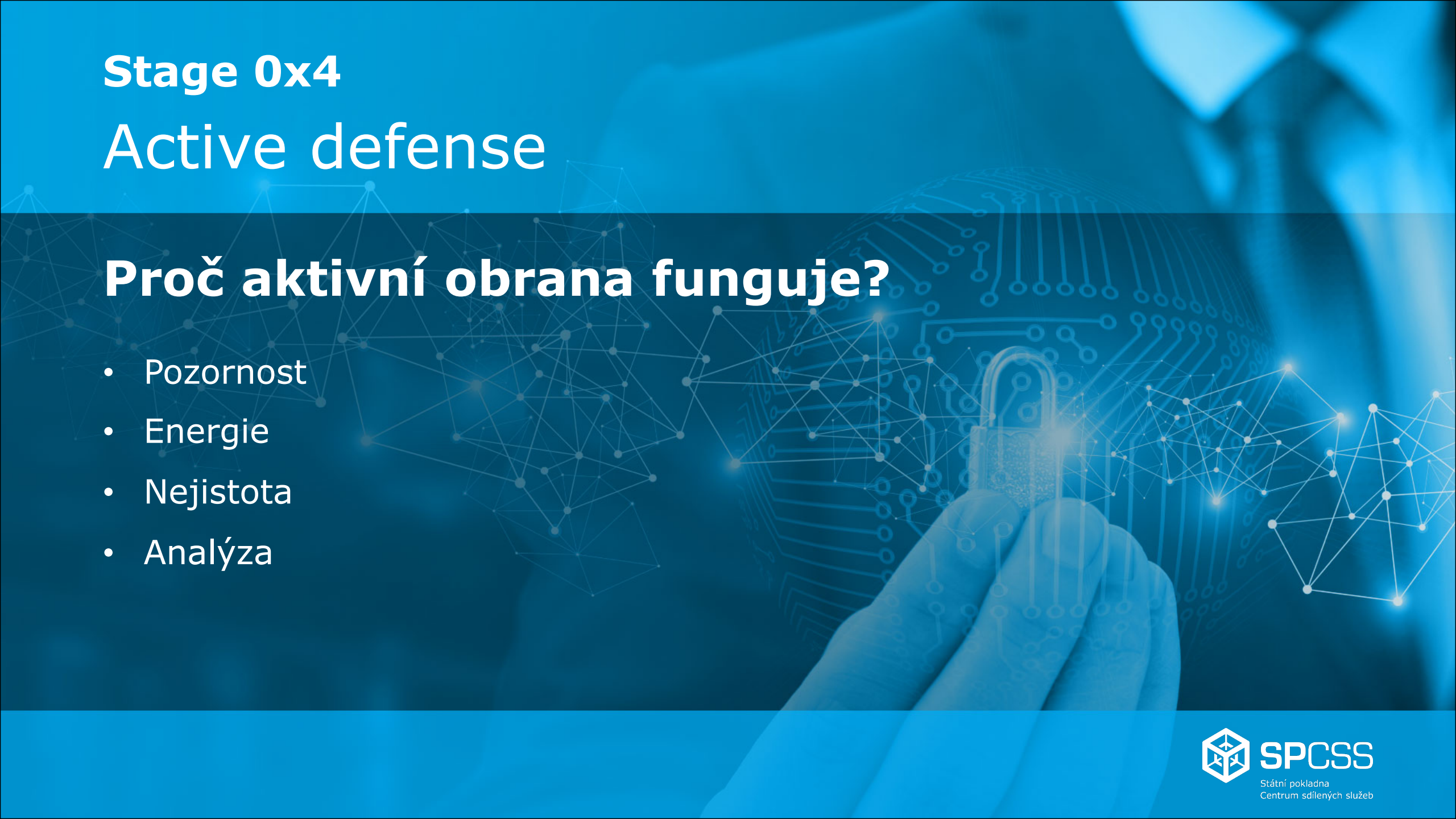
SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x4

Active defense

Proč aktivní obrana funguje?

- Pozornost
- Energie
- Nejistota
- Analýza



SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x4

Active defense

Příběh ARGO

- Pozor spoiler
- Deception
- Zakryj pravdu, odkryj faleš

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x4

Active defense

Stuxnet

- Deception
- Denial
- Counterdeception
- Counter-Deception

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x4

Active defense

Pasivní obrana	**Reaktivní obrana** • Antivirus, Firewall . . .
Aktivní obrana	**Gray zone of Active Defense** • Beacons, Botnet, Deception . . . • **Ofenzivní obrana** • Hacking back, cyber operations . . .

Stage 0x5

Gray zone of Active Defense

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x5

Gray zone of AD

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

Stage 0x5

Gray zone of AD

Deterrence

- Zastrašování
- Barnes case
- FBI warning

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x5

Gray zone of AD

Intelligence Sharing

- Passive Intelligence
  - Threath sharing platforms
  - OSINT
- Counter-Intelligence

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x5

Gray zone of AD

Deception

- Deception
- Denial
- Counterdeception
- Counter-deception

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x5

Gray zone of AD

Threat hunting

- Proaktivní vyhledávání
- Vytváření hypotéz chování

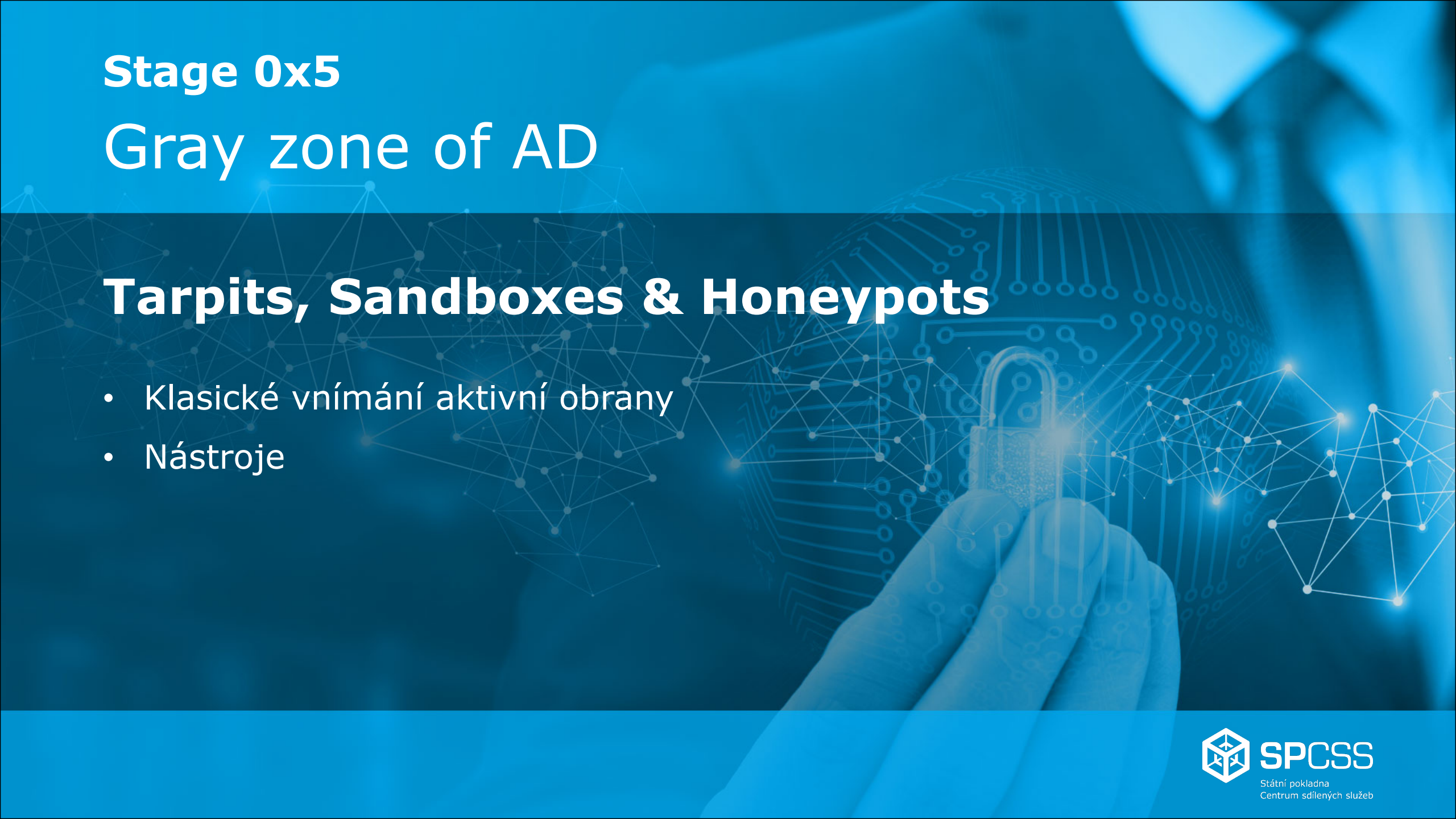
SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x5

Gray zone of AD

Tarpits, Sandboxes & Honeypots

- Klasické vnímání aktivní obrany
- Nástroje



SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x5

Gray zone of AD

Red Teaming

- Threat Emulation
- Adversary Emulation

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x5

Gray zone of AD

Beacons

- Notify
- Inform

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x5

Gray zone of AD

Botnet Takedowns

- Nutná legislativní podpora
- Malicious behaviour
- Ohrožení kritické infrastruktury

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x5

Gray zone of AD

Sanctions, Indictments & Trade Remedies

- Nutná legislativní podpora
- Sankce
- Restrikce

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x5

Gray zone of AD

Rescue Missions

- Nutná legislativní podpora
- Hacking back
- Cyber operations

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x5

Gray zone of AD

Ransomware

- Nutná legislativní podpora
- Whitehat ransomware
- Humanitární ransomware

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x5

Gray zone of AD

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

Stage 0x6a

Mind the Beacons

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x6a

Mind the Beacons

Deskripce

- NOTIFY Beacon
- INFORM Beacon

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x6a

Mind the Beacons

Levelace

- 1. Beacons v cloudu
- 2. Beacons on-premise
- 3. Beacons jako jiné AD

https://adhdproject.github.io

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x6b

Relief with Beacons

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x6b

Relief with Beacons

From zero to hero

- CanaryTokens.org
- Využití existujícího
- Kombinačky
- Generujte till you can
- Advanced – vytvořte vlastní C2
- Drobnohled

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x7

EoF

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x7

EoF

FAQ

- AD není postavena na vysokých nákladech
- GDPR – součást incident response

Stage 0x7

EoF

Open sources

- Mitre.org (Att&ck, CAR, Shield, Caldera)
- SpecterOps.io (blog, Covenant, Ghost . . .)
- Redteam journal
- CIRCL (MISP, AIL . . .)
- HelpSystems (CobaltStrike)

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x7

EoF

Open sources

- https://mitre-attack.github.io/attack-navigator/enterprise/#
- https://github.com/mitre/brawl-public-game-001
- https://github.com/clong/DetectionLab
- https://github.com/redcanaryco/atomic-red-team
- https://car.mitre.org
- https://github.com/OTRF/ThreatHunter-Playbook
- https://github.com/mitre/caldera
- https://github.com/cobbr/Covenant
- https://github.com/infosecn1nja/Red-Teaming-Toolkit
- https://shield.mitre.org/matrix/
- https://canarytokens.org

Stage 0x7

EoF

Community

Defcon Group 420 Czech republic

- www.DCG420.org

MeetUps

- DCG420.eventbrite.com

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x7

EoF

Conference

Fórum aktivní kybernetické obrany 2020

- 2. ročník
- Listopad 2020
- Funny on-line

Keep in touch

- csirt@spcss.cz

SPCSS
Státní pokladna
Centrum sdílených služeb

Stage 0x7

EoF

Děkujeme za pozornost

SPCSS
Státní pokladna
Centrum sdílených služeb