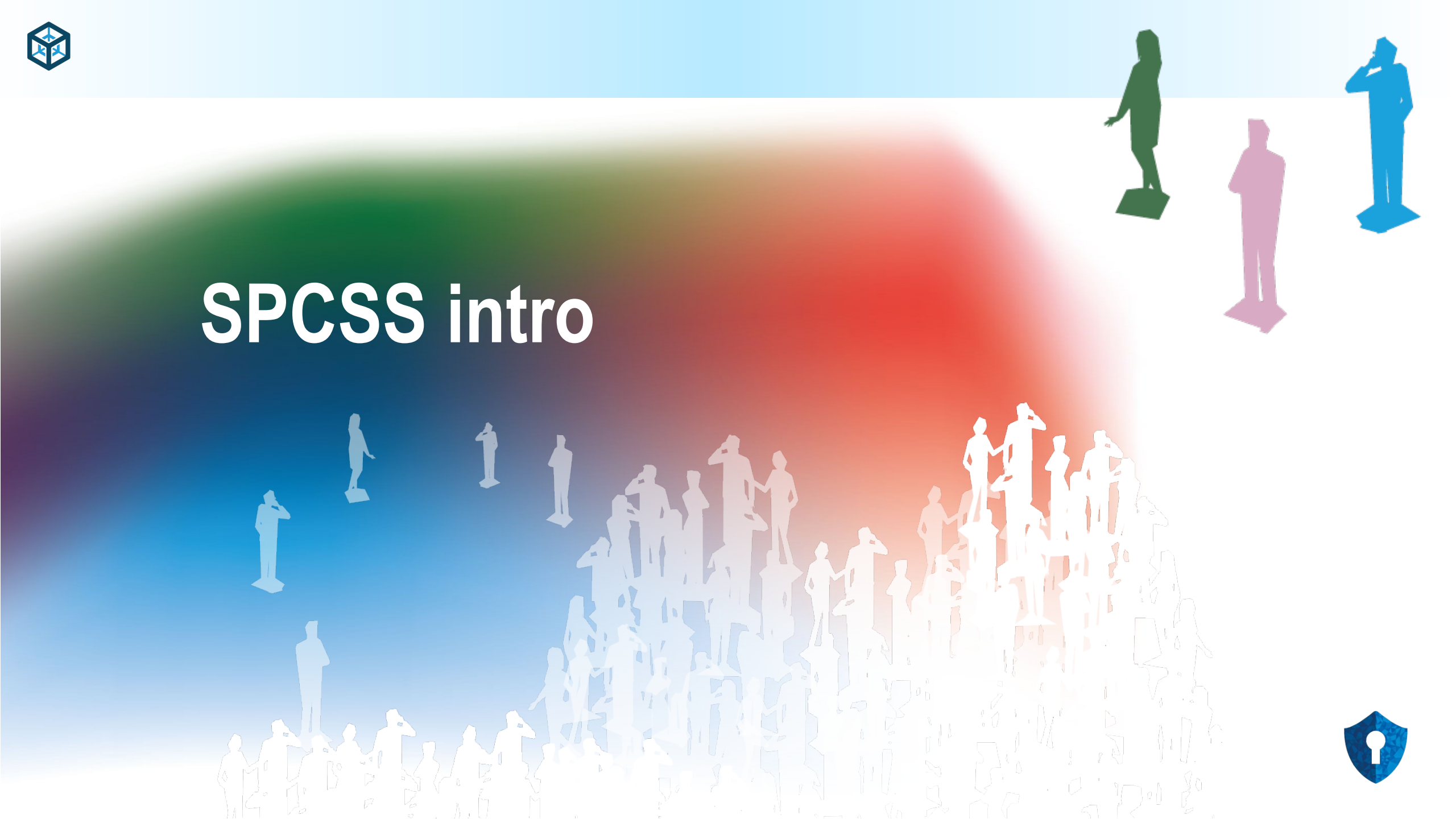
Dva nejdůležitější security koncepty v současnosti a jedna aktivita navíc

SPCSS

Státní pokladna
Centrum sdílených služeb

SPCSS intro



Our topics

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

About US

- **Ondřej Nekovář,** CISO
- **Jan Pohl,** practical CISO advisor

Co v KB v SPCSS děláme

- SOC
- Threat-intel
- Incident response
- Vulnerability
- Threat hunting
- Adversary emulation
- Active defense
- Identity
- Integration
- Risk
- Awareness (internal, external)
- Policy

Aktuální rozvojové projekty

- Deception platform
- Threat-intel platform
- Incident response platform
- Passwordless
- SOCCRATES

No a hledáme zapálené lidi…

Mindset obránce

Mindset

- Přístup k **bezpečnosti**
  - **The Assume Breach Paradigm**
- Přístup k **testování**
  - **Threat-informed Defense**
- Žádoucí **aktivita**
  - **Adversary emulation**

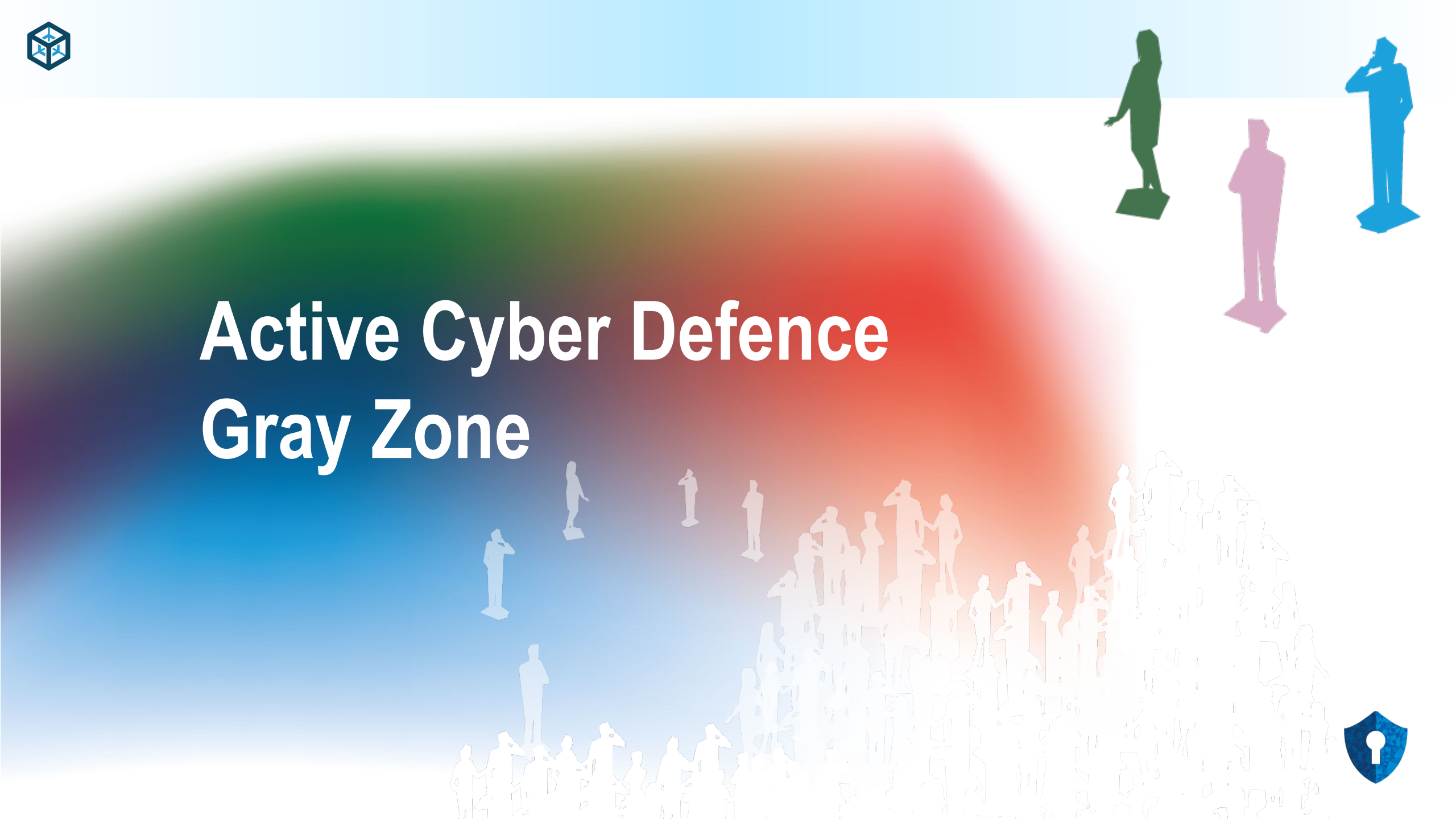
The Assume Breach Paradigm

- Smíření
- Nedostatky reaktivních prvků
- Příprava na zkušené Adversary
- Mindset – nic není bezpečné a je kompromitované
- Emulace, cvičení a metriky
- Efektivní decision making

Threat-Informed Defense

- Porozumění tradecraft a technologie Adversary
- Our Threat landscape
- Systematické používání této znalosti - LOOP
- Umožnění neustálého zlepšování obrany (prevent, detect, response)
- Společný jazyk – „slovník“ - MITRE Att&ck TTP
- Efektivní decision making

Active Cyber Defence
Gray Zone



Active Cyber Defence Gray Zone

Adversary emulation	Adversary Takedowns
Beacons	Ransomware
Deterrence	Rescue Missions
Deception	Sanctions, Indictments & Remedies
Tarpits, Sandboxes & Honeypots	
Threat Intelligence	
Threat Hunting	

Created by DCG420

Adversary Emulation

- Threat modeling
- Purple Teaming
- Blue Teaming
- Red Teaming

Adversary emulation

Use-Case

- **Threat intel** - sběr dat o útočníkovi
- **Scenario –** ATP29 – NOBELIUM, UNC2452, YTTRIUM
- **Adversary emulation** – TTP Adversary, výstupy pro nastavení detekce
- **Detect –** uprava existujících pravidel / vytvoření nových
- ***Monitor***
- ***Alert***
- ***Incident response***

Adversary emulation

Use-Case - Results

- **2Q 2021 - 1Q 2022**
- **Počet testovaných scénářů:** 31 (10-100 testů)
- **Upraveno detekčních pravidel:** 279
- **Nastaveno nových detekčních pravidel:** 63
- **LOOP = Management**

Chyba v MITRixu

Test ověření kvality nezávislou stranou

- **MITRE MAD Evaluations**
- **Nedostatky polo / automatizovaného přístupu**
- **Jiné nástroje, jiné výsledky**
  - Cobalt Strike – BOF
- **Ponaučení**

Díky za pozornost

Stay in touch

- www.spcss.cz/FAKO
- www.spcss.cz/MISP
- www.spcss.cz/CSIRT

- csirt@spcss.cz
- @csirtspcss

Hlasujte pro to, co Vás zajímá

DOTAZNÍK PRO AKCE
k aktivní kybernetické bezpečnosti

SPCSS
Státní pokladna
Centrum sdílených služeb