



**SPCSS**

Státní pokladna  
Centrum sdílených služeb

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

# Validace detekce a Aktivní obrana v cloudu



**SPCSS – Ondřej Nekovář, Jan Pohl**  
**e-government 20:10, Mikulov**  
06. - 07. 09. 2022

# Intro

## Stage 1/4

Intro

About Us

- **Ondřej Nekovář**
- **Jan Pohl**

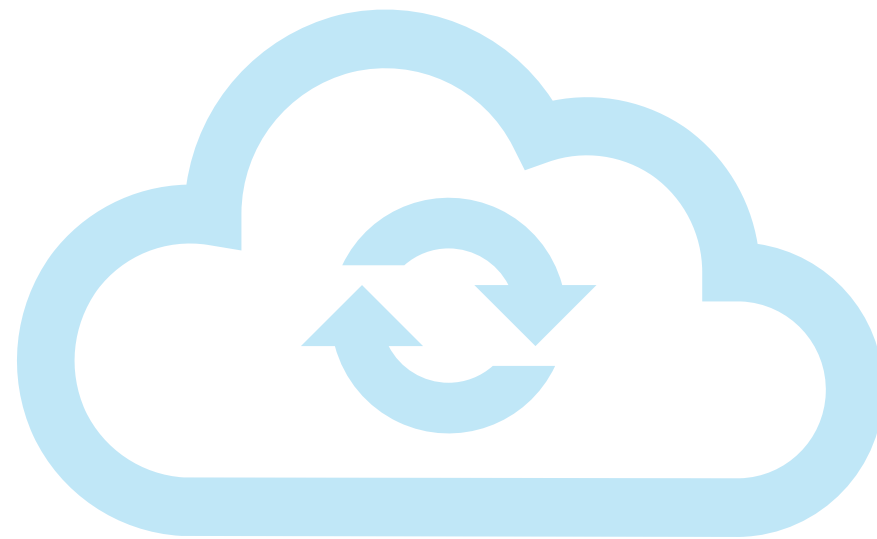
**Státní pokladna Centrum sdílených služeb, s. p.**



Intro

Our topics

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

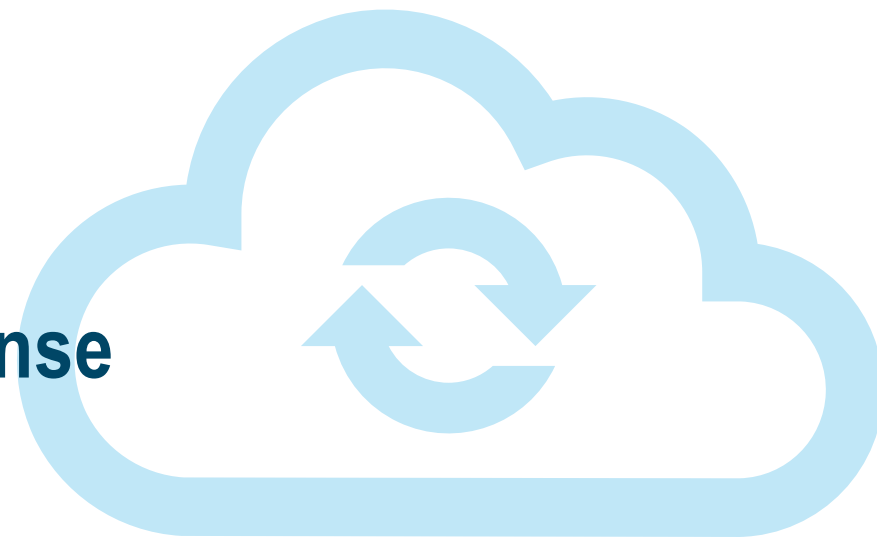


Intro

## Our business

- **SOC**
- **Threat-intel**
- **Incident response**
- **Vulnerability**
- **Threat hunting**
- **Adversary emulation**

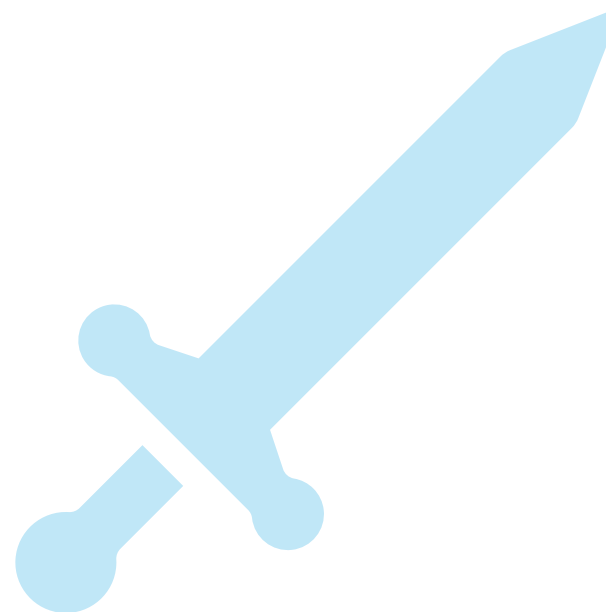
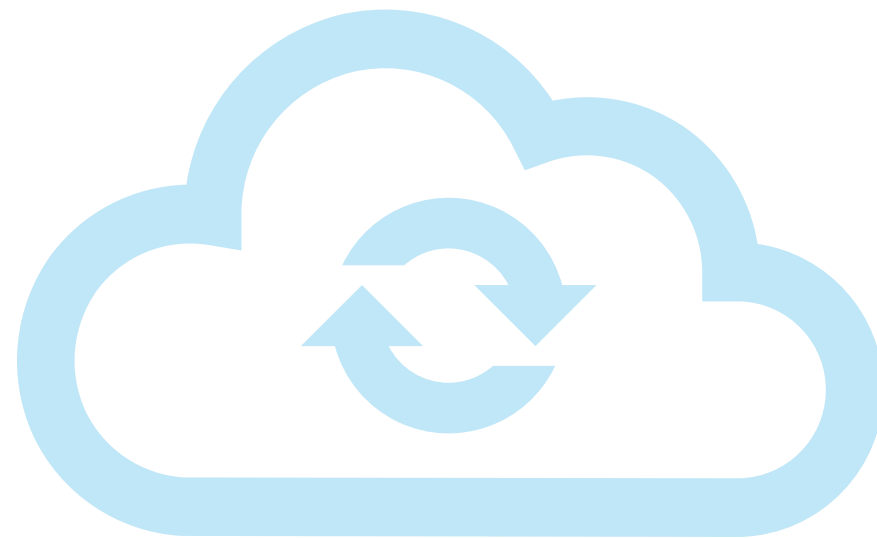
- **Active defense**
- **Identity**
- **Integration**
- **Risk**
- **Awareness (internal, external)**
- **Policy**



Intro

## Our goals

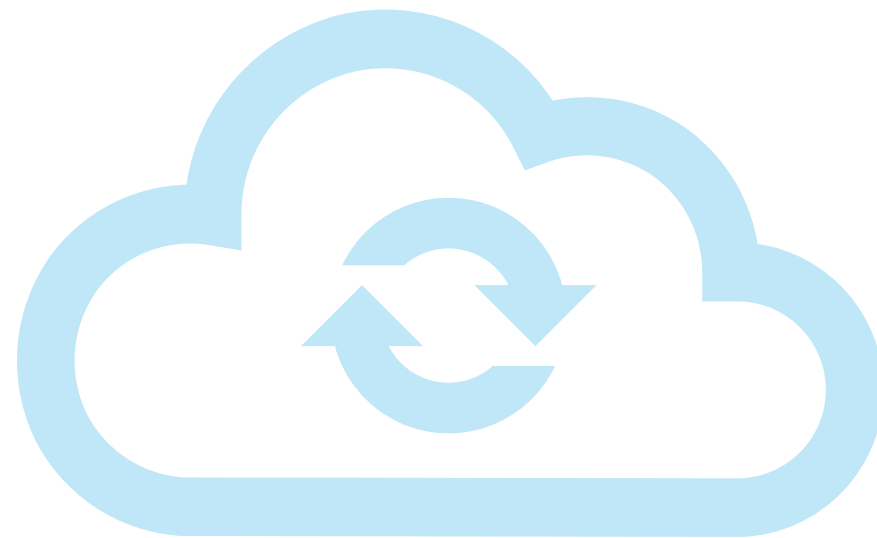
- **Resortní centrum kybernetických operací MF**
- ***Dohledové centrum státní části eGC***
- **NPO Program - Vybudování eGovernment cloudu**



Intro

## Our „Resort“ projects

- **Deception platform**
- **Threat-intel platform**
- **Incident response platform**
- **Passwordless**
- **SOCGRATES**

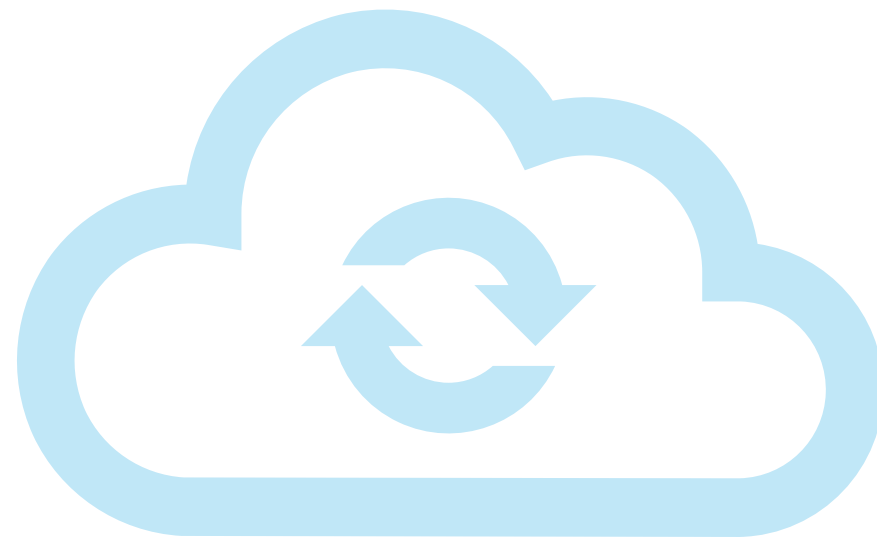




Intro

## Our „eGC“ projects

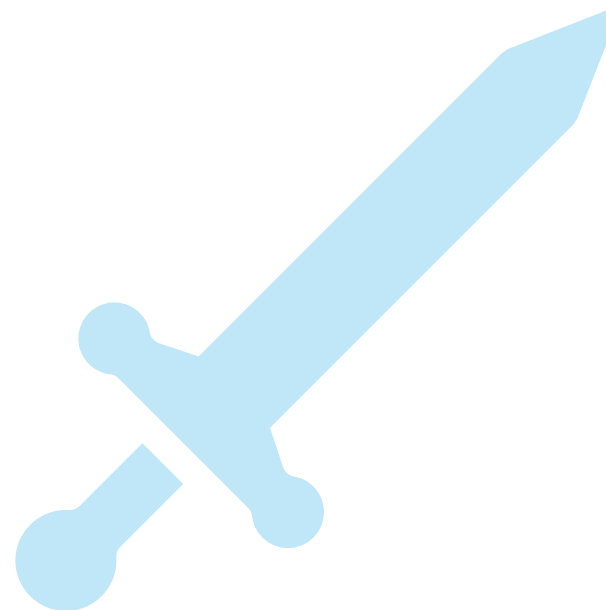
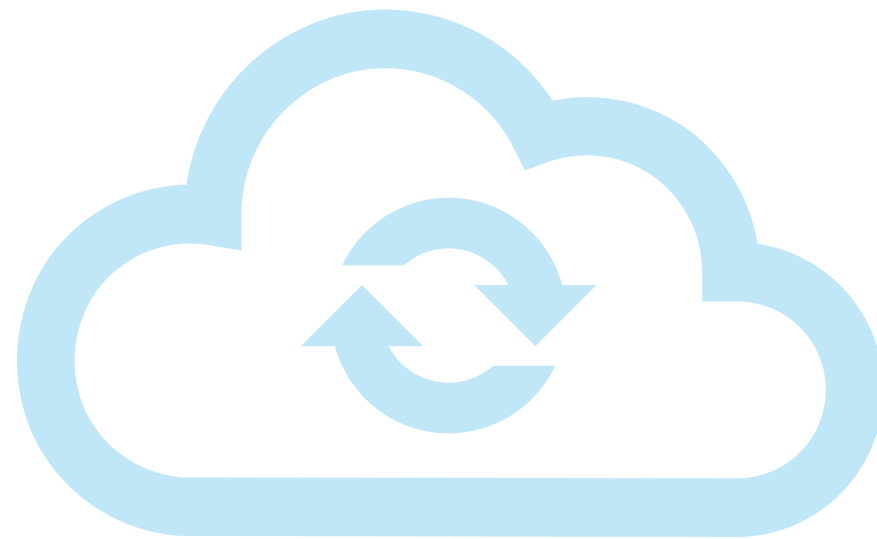
- **Příprava na provozování státní části eGC**
- **Assessment pro IS BÚ4 k přechodu do státní části eGC**
- **Realizace SOC2® - BÚ3 (Azure, AzS), BÚ4**



# Intro

## We did

- **FAKO**
- **MISP training**
- **Odborné prezentace**
- **Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti**
- **Metodika AR předmětu veřejné zakázky**
- **Metodika zabezpečení kubernetes**



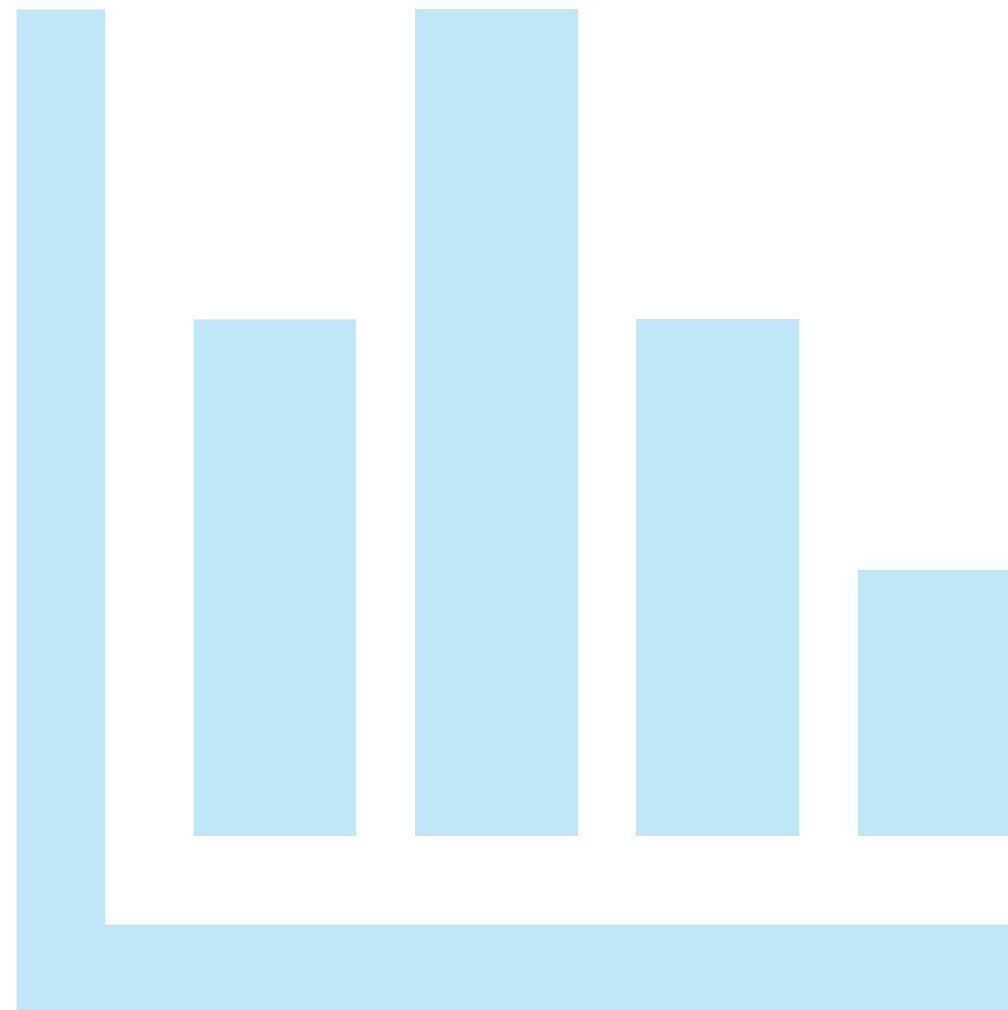
# Kontext

**Stage 2/4**

Intro

# Statistiky environment

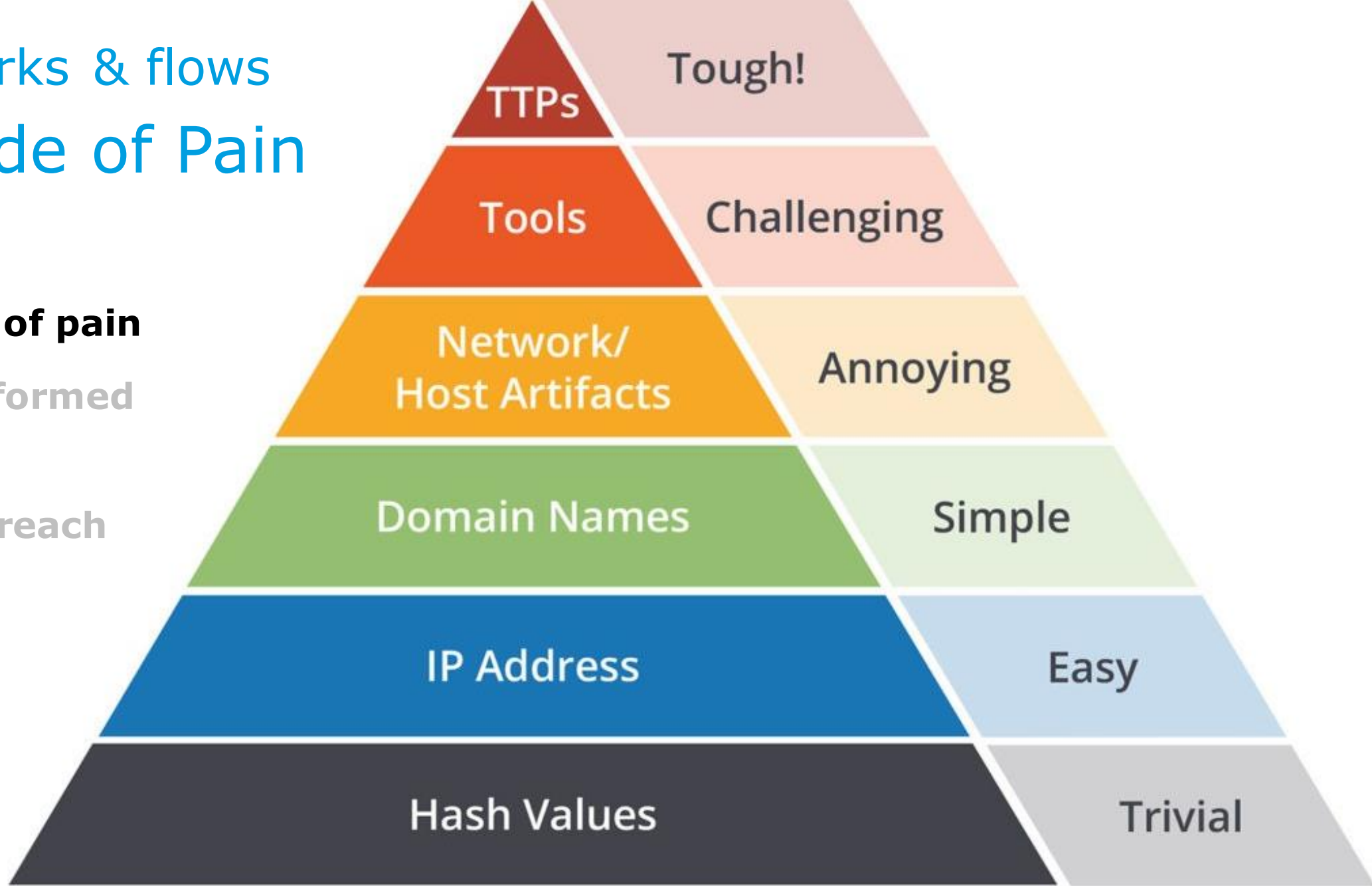
- **83** sledovaných technologií
- ∞ množství formátů
- ∞ dat a logů



# Frameworks & flows

## Pyramide of Pain

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



Source: David J. Bianco, personal blog

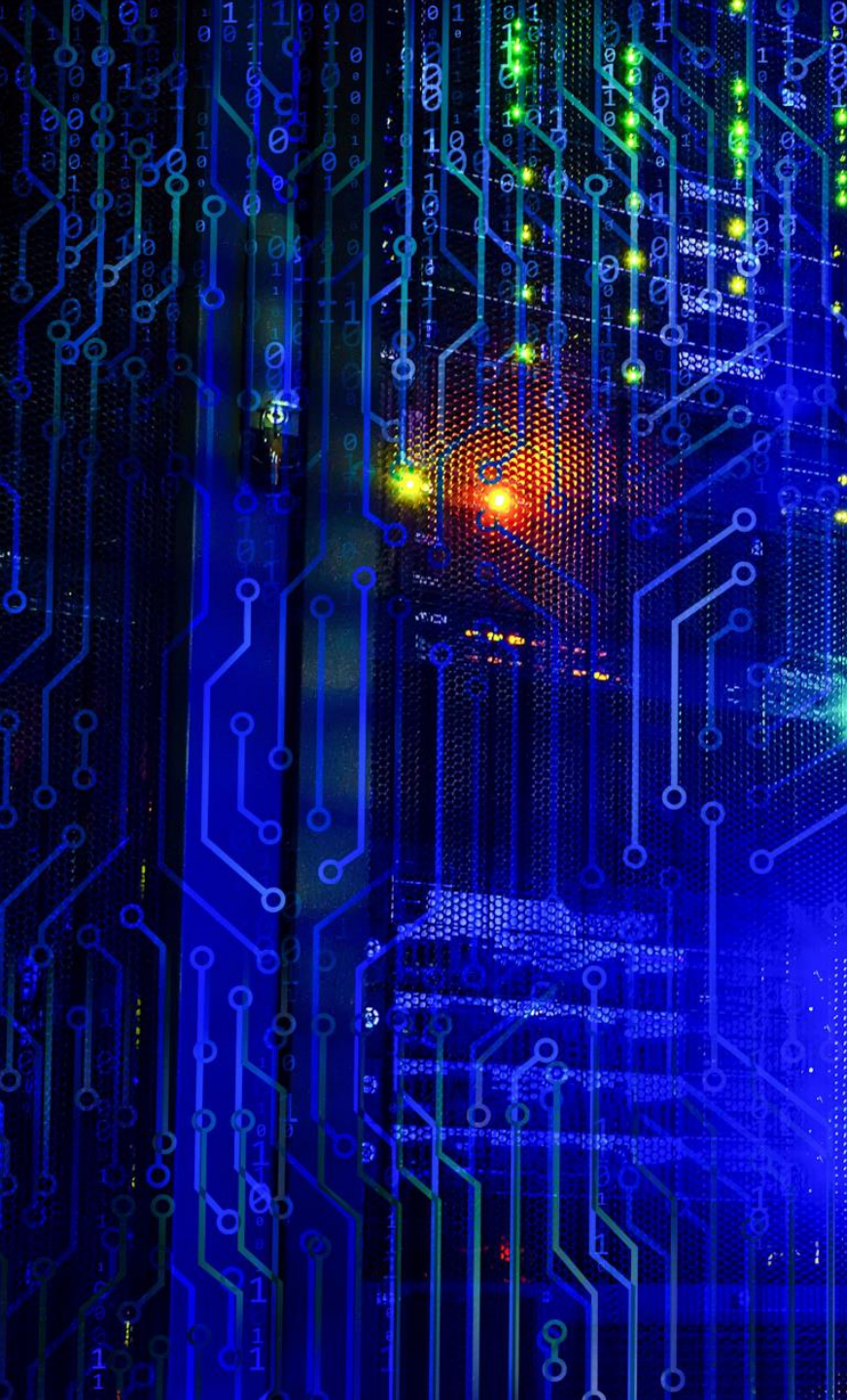


# Frameworks & flows

## Threat Informed Defense

- Pyramide of pain
- **Threat Informed Defense**
- The Assume Breach Paradigm
- Detection Engineering Methodology
- Alerting & Detection Strategy



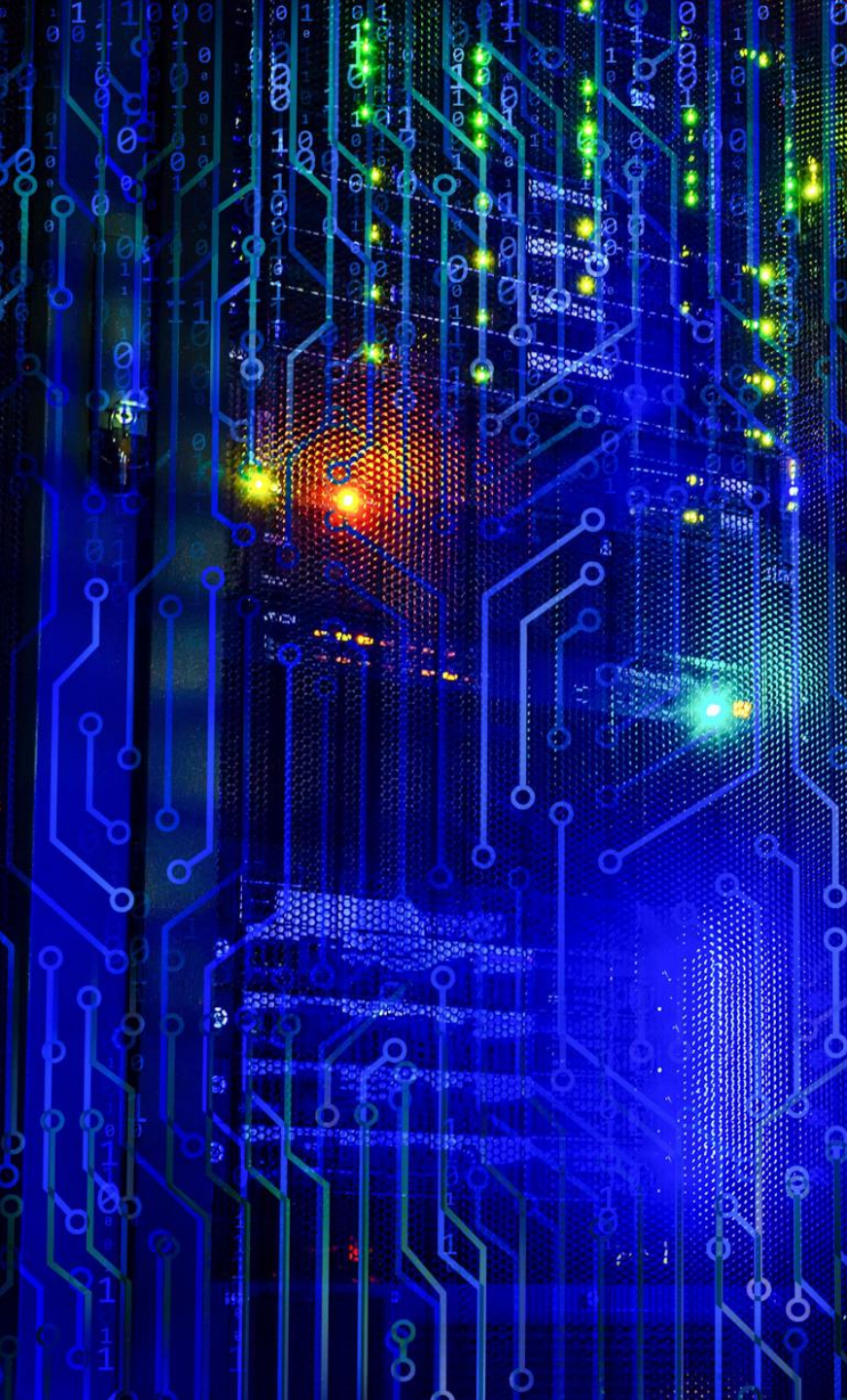


Frameworks & flows

# The Assume Breach Paradigm

- Pyramide of pain
- Threat Informed Defense
- **The Assume Breach Paradigm**
- Detection Engineering Methodology
- Alerting & Detection Strategy





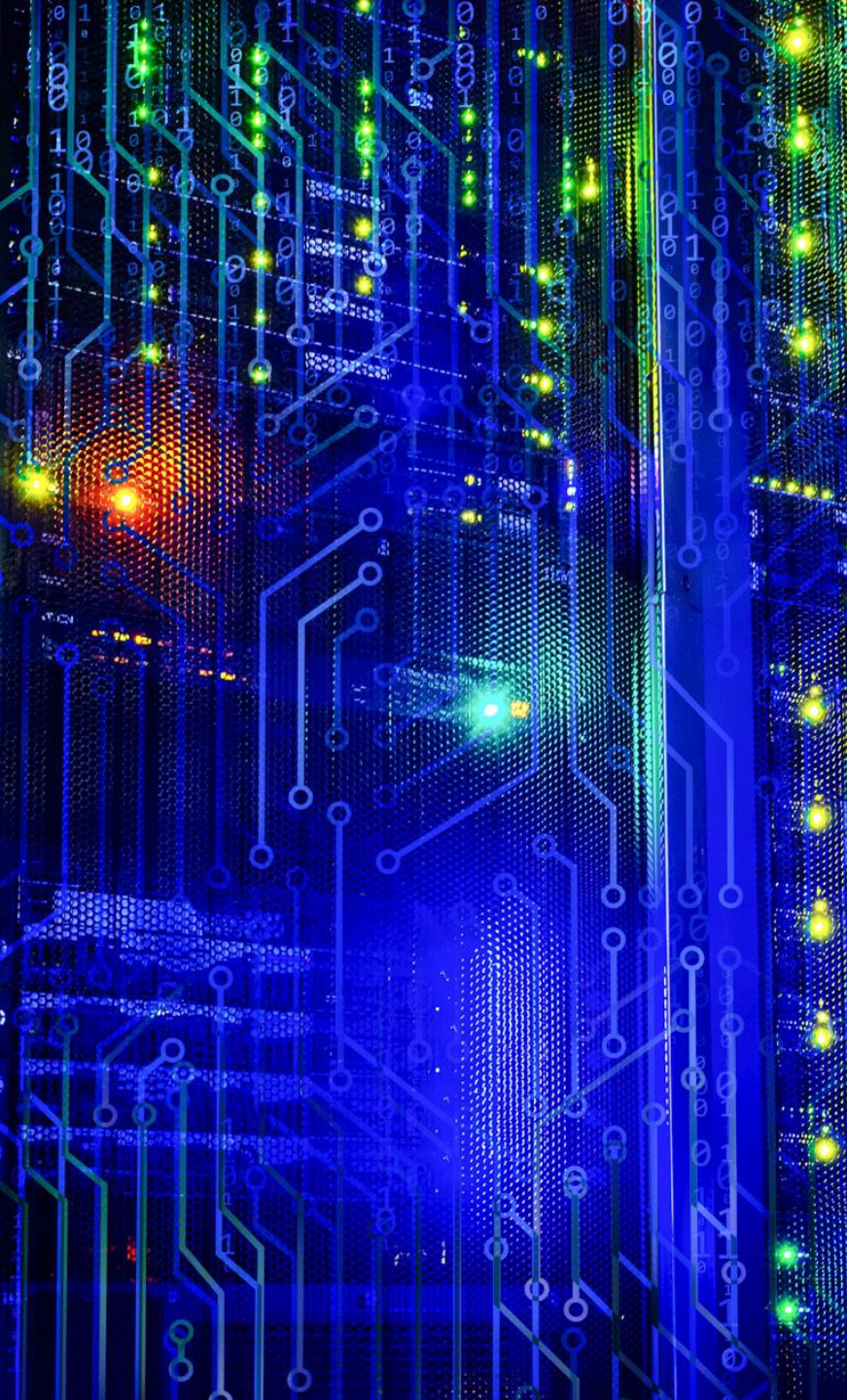
# Frameworks & flows

## DEM

- Pyramide of pain
- Threat Informed Defense
- The Assume Breach Paradigm
- **Detection Engineering Methodology**
- Alerting & Detection Strategy





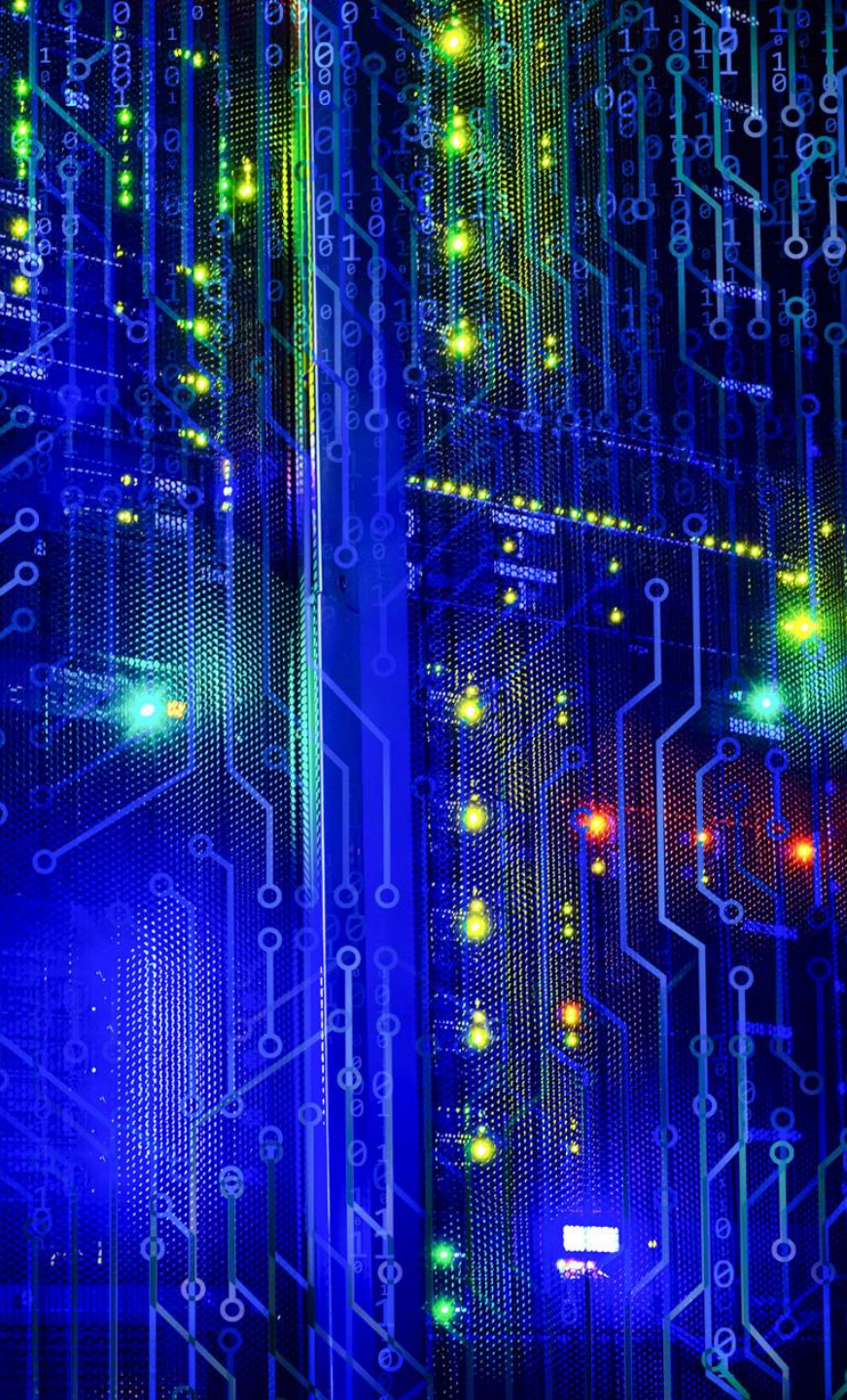


# Frameworks & flows

## DEM

- **Detection Engineering Methodology**
  - **Select Target Technique**
  - **Research Underlying Technology**
  - **Proof of Concept Malware Sample(s)**
  - **Identify Data Sources**
  - **Build the Detection**



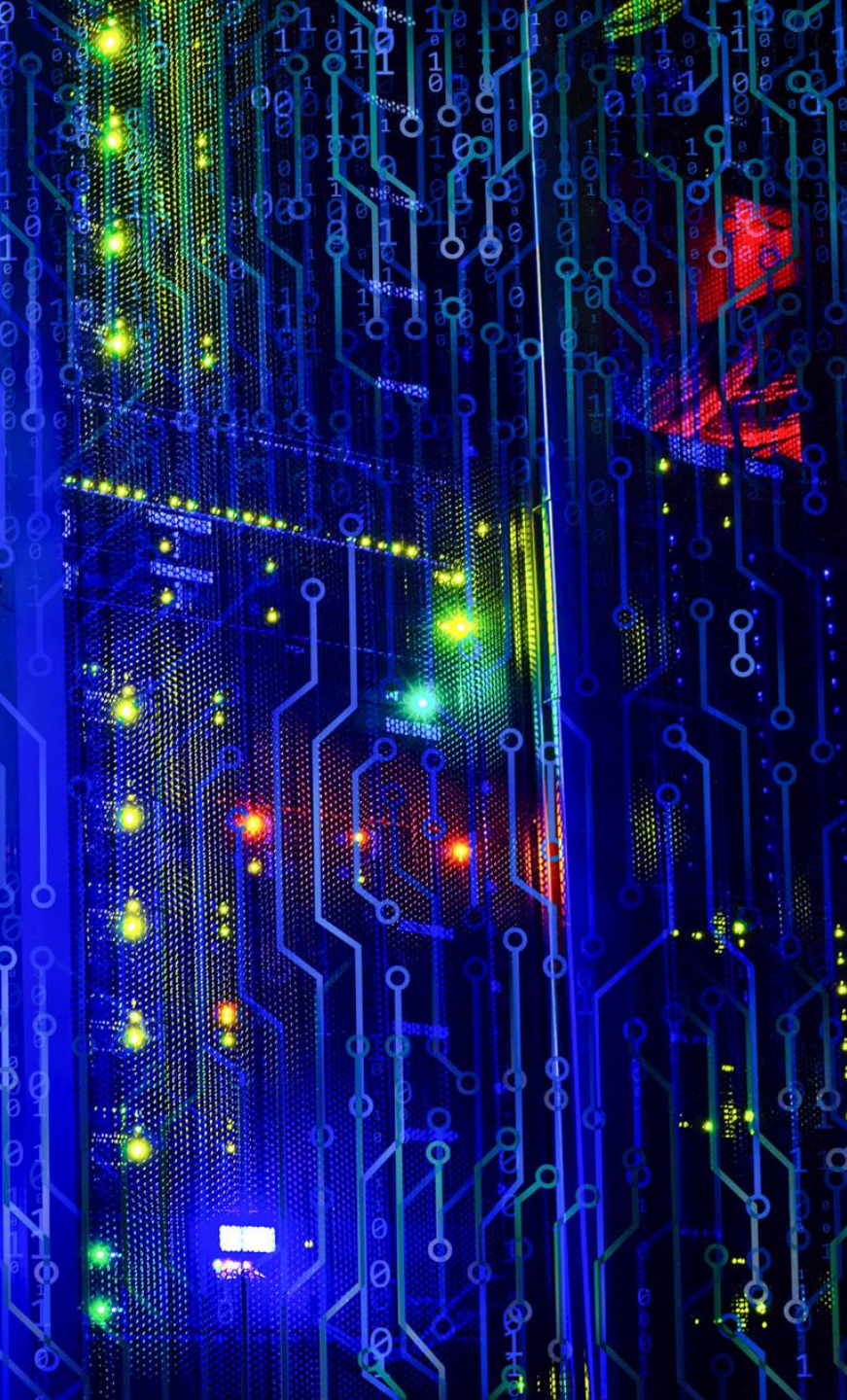


# Frameworks & flows

## ADS

- Pyramide of pain
- Threat Informed Defense
- The Assume Breach Paradigm
- Detection Engineering Methodology
- **Alerting & Detection Strategy**





# Frameworks & flows

## ADS

- **Alerting & Detection Strategy**
  - **Goal**
  - **Categorization**
  - **Strategy Abstract**
  - **Technical Context**
  - **Blind Spots and Assumptions**
  - **False positives**
  - **Validation**
  - **Priority**
  - **Response**



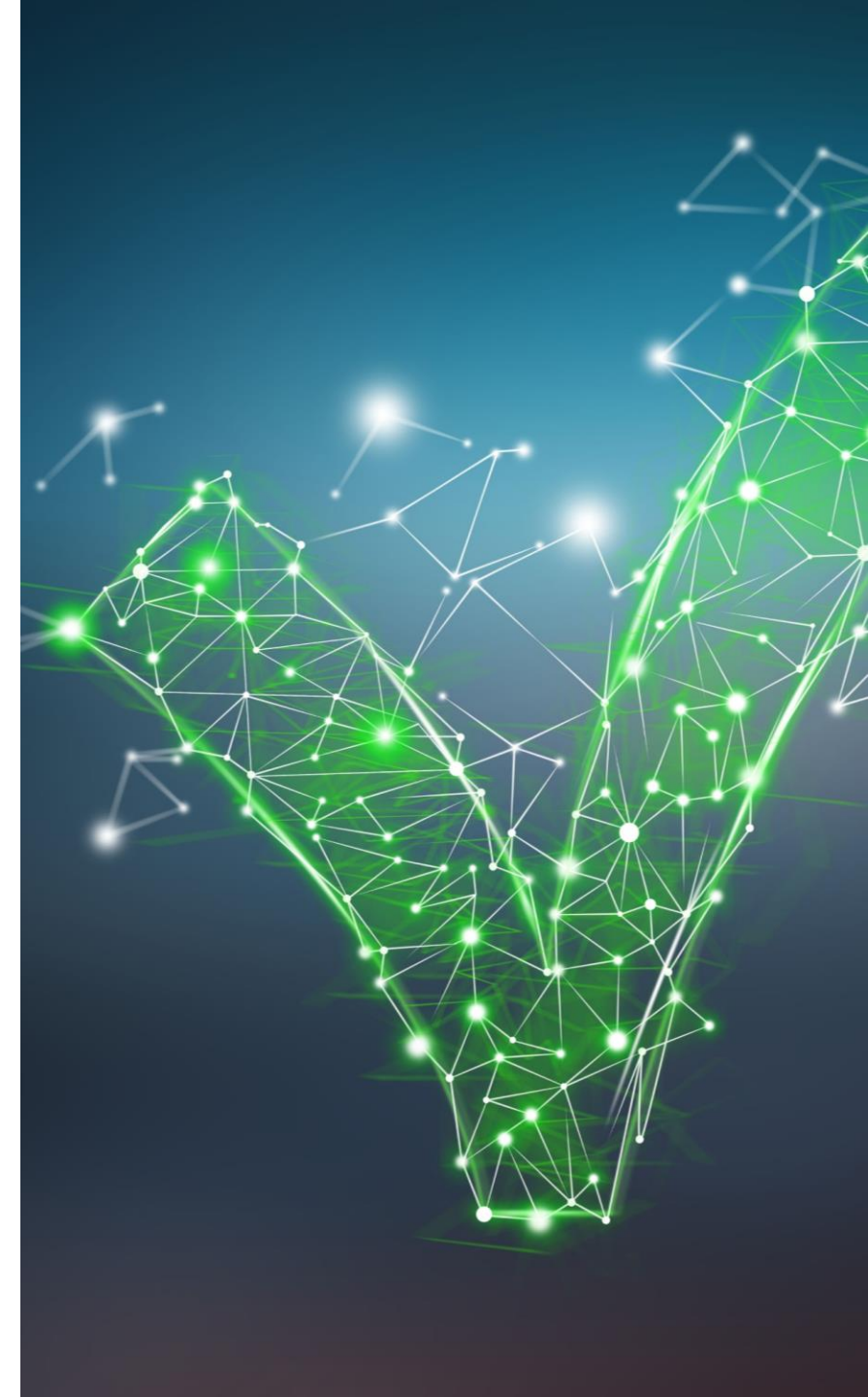
# Validation

**Stage 3/4**

# Validation

## How to validate?

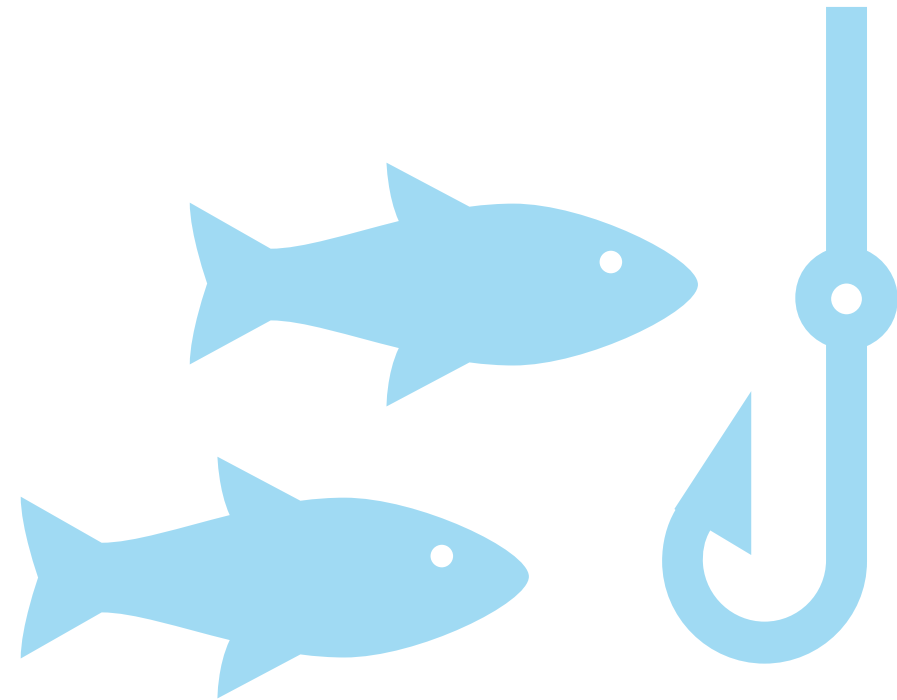
- **Signature AV vs SIEM**
- **Hard to understand build in rules**
- **Need use it between multiple tools**
- **False positives?**



# Validation

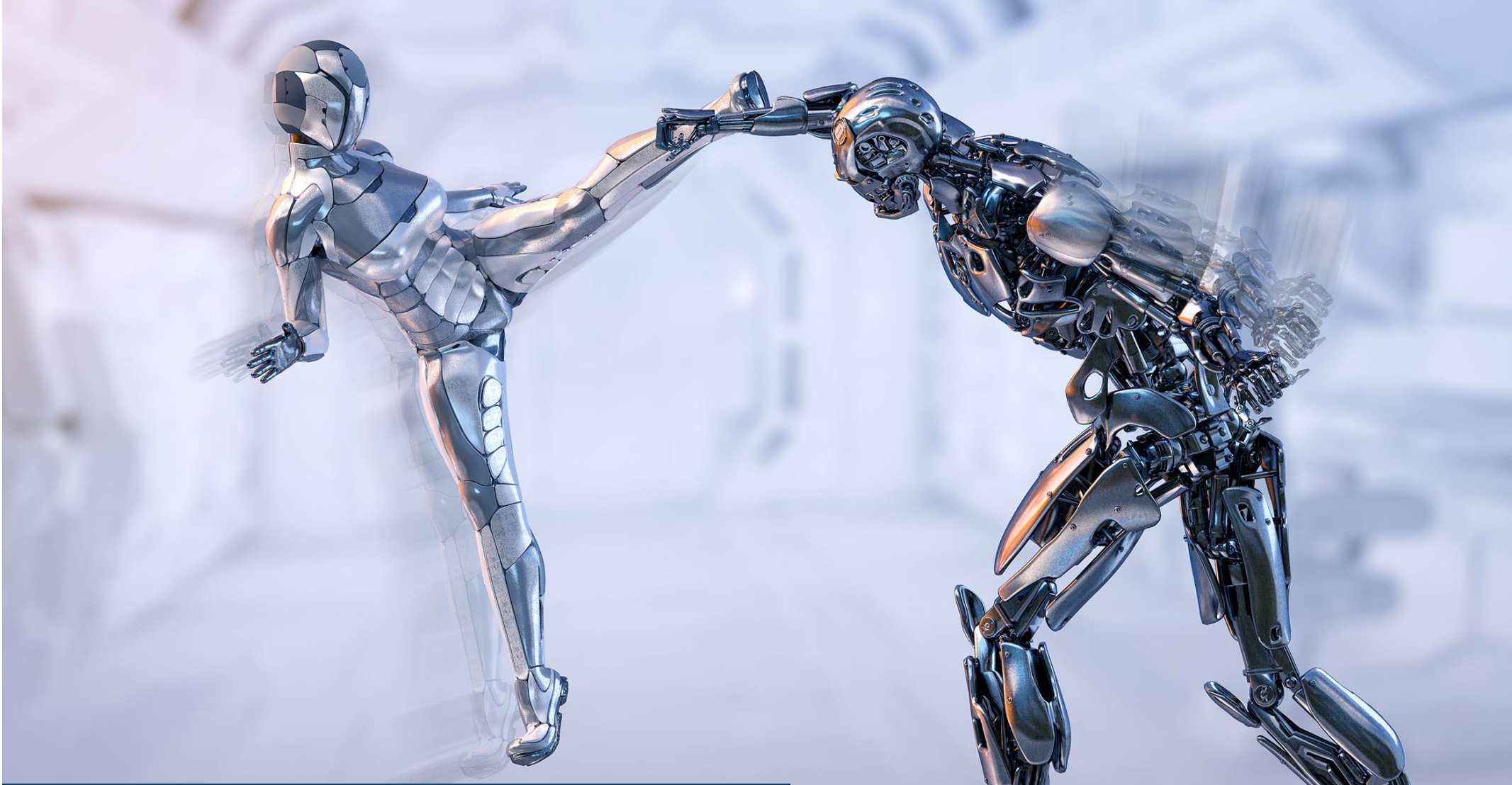
## Adversary emulation

- **Emulate Adversary to know how works**
- **Emulate Adversary to stop them**
- **Emulate Adversary to prepare**
- **AND, AND . . .**
- **Emulate Adversary to **VALIDATE****



# Adversary Emulation High level

- Vulnerability management
- Penetration testing
- Adversary emulation



# Adversary Emulation Tools of Trade

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

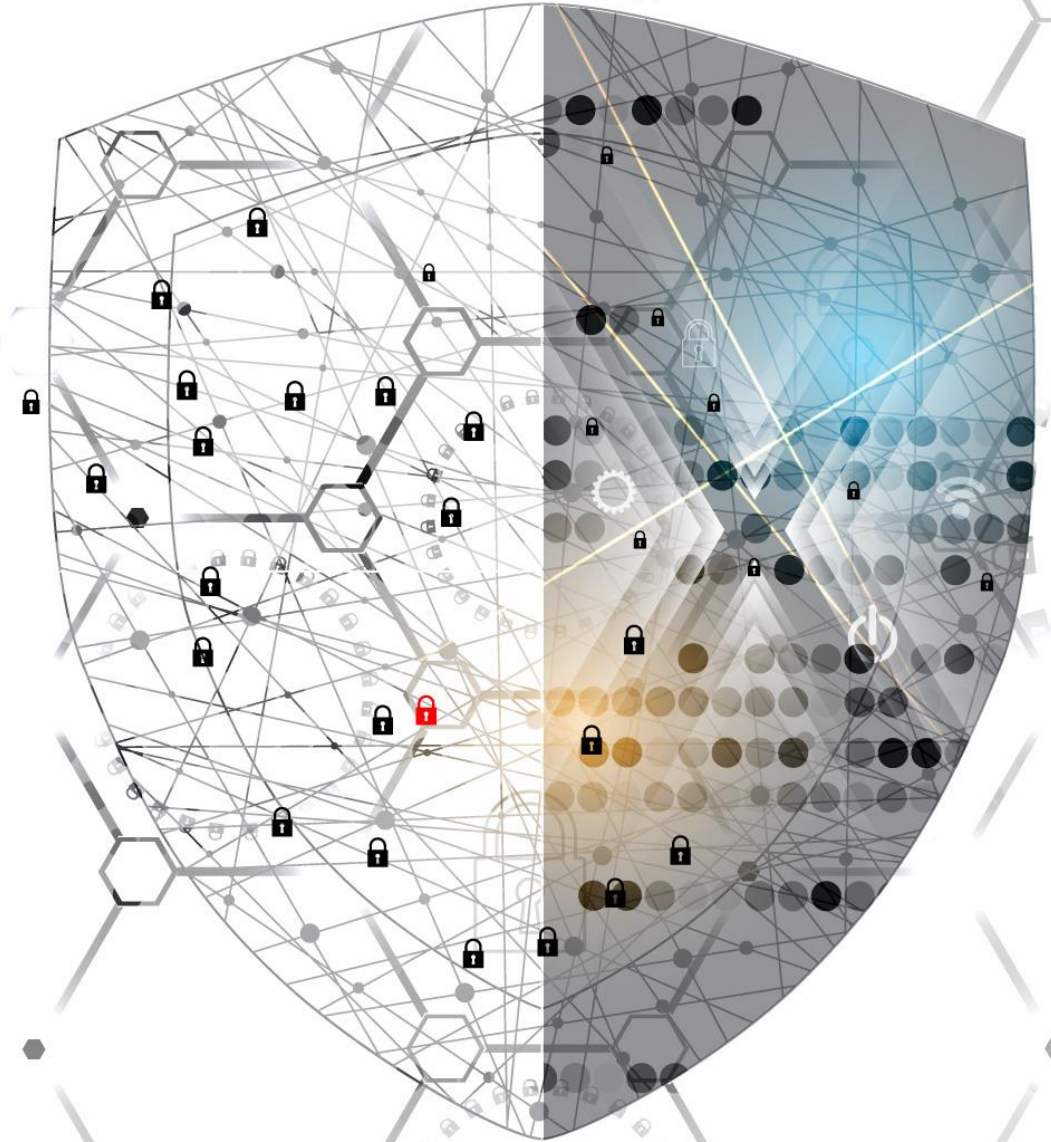




Red Teaming

## The prostředí

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



# EoF



**Stage 4/4**

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/DCG420>
- <https://github.com/SecurityRiskAdvisors/VECTR>
- <https://blog.palantir.com/alerting-and-detection-strategy-framework-52dc33722df2>
- <https://specterops.io/>



EoF

# Community

## Defcon Group 420 Czech republic

- [www.DCG420.org](http://www.DCG420.org)

## MeetUps

- [DCG420.eventbrite.com](http://DCG420.eventbrite.com)



EoF

# Our Training

## **NÚKIB CyberCon 2022**

### **Workshop**

- **Adversary emulation pro malé týmy - fundamentals**
- 13.9.2022

### **Přednáška**

- **Analýza rizik předmětu veřejné zakázky – Best practise**
- 14.9.2022

EoF

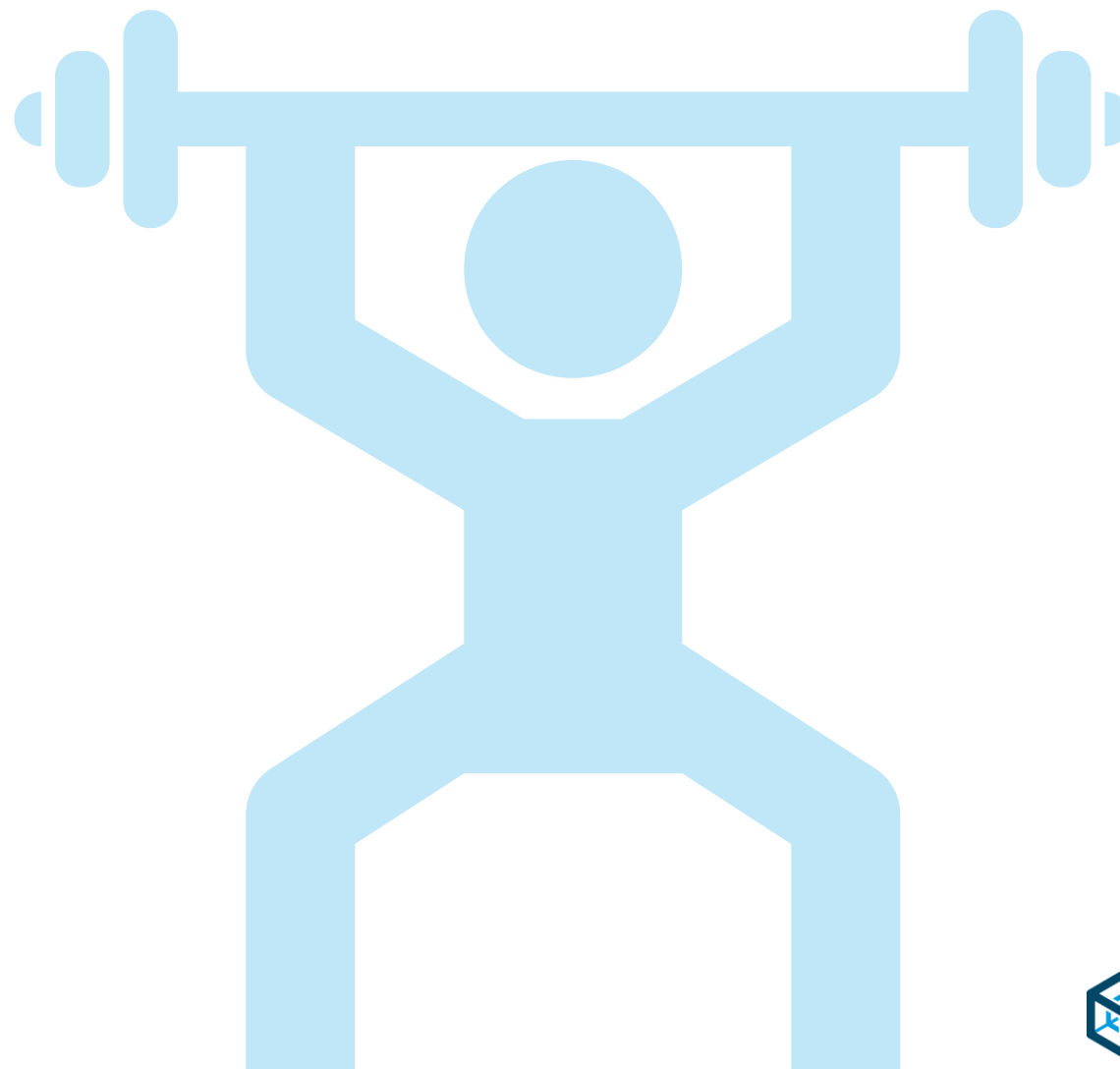
# Our Training

## MISP Training 2023

- 5. ročník - MISP, AIL, CyCAT
- **New: workflows, corellation**
- Zdarma – On-site/On-line
- Jaro 2023, anglicky

## Registrace

- [www.spcss.cz/misp](http://www.spcss.cz/misp)



EoF

# Our Conference

## **Fórum aktivní kybernetické obrany 2023**

- 3. ročník
- Jaro 2023, česky

## **Registrace**

- E-mail [csirt@spcss.cz](mailto:csirt@spcss.cz)





EoF

## Keep in touch

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



# Děkujeme za pozornost

**Q & A**