

# Building resiliency with active cyber defense for Government cloud



**SPCSS – Ondřej Nekovář**

**Digital Partnership for Cybersecurity and Resilience in Regions**

6. 10. 2022

Intro

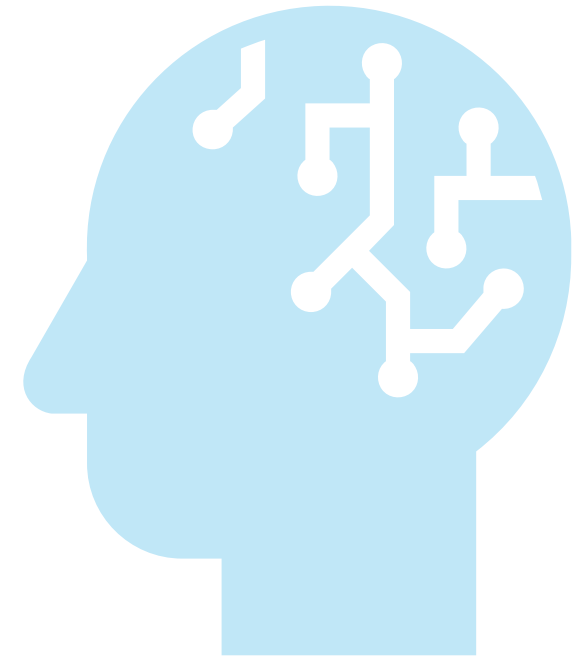
About Us

- **Ondřej Nekovář**

- **CISO, CDO**

- **30x person in the Team**

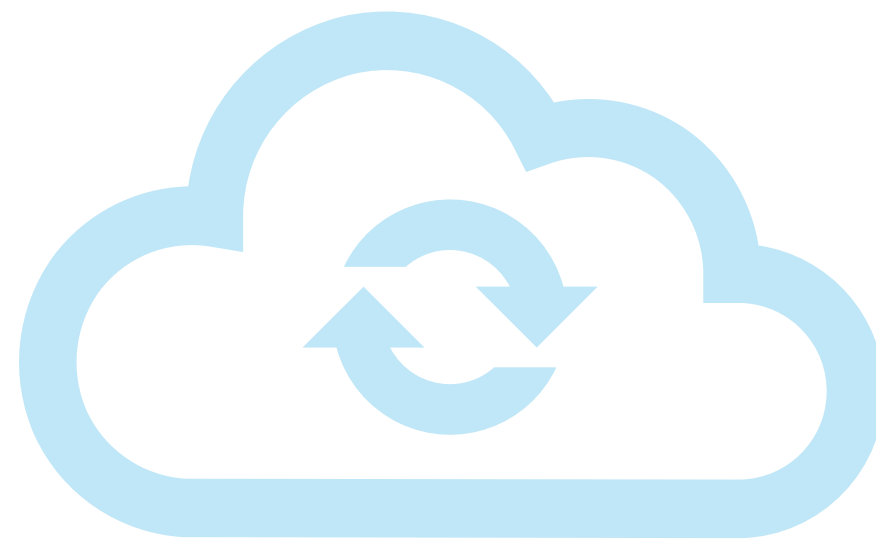
**Státní pokladna Centrum sdílených služeb, s. p.**



Intro

## Our topics

- **DC, Cloud, Hybrid-cloud security**
- **Ministry of finance**
- **eGovernment cloud (level 4)**



Intro

## Our business

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

# Our goals



# Our way in maturity

- **Our CII National Data Centre**

- Impact on our CII

- **SOC for Ministry of Finance**

- Impact on our founder

- **Department of the Ministry of Finance SOC**

- Impact on all org. = Fulfilling the purpose of our organisation

# Our way in maturity

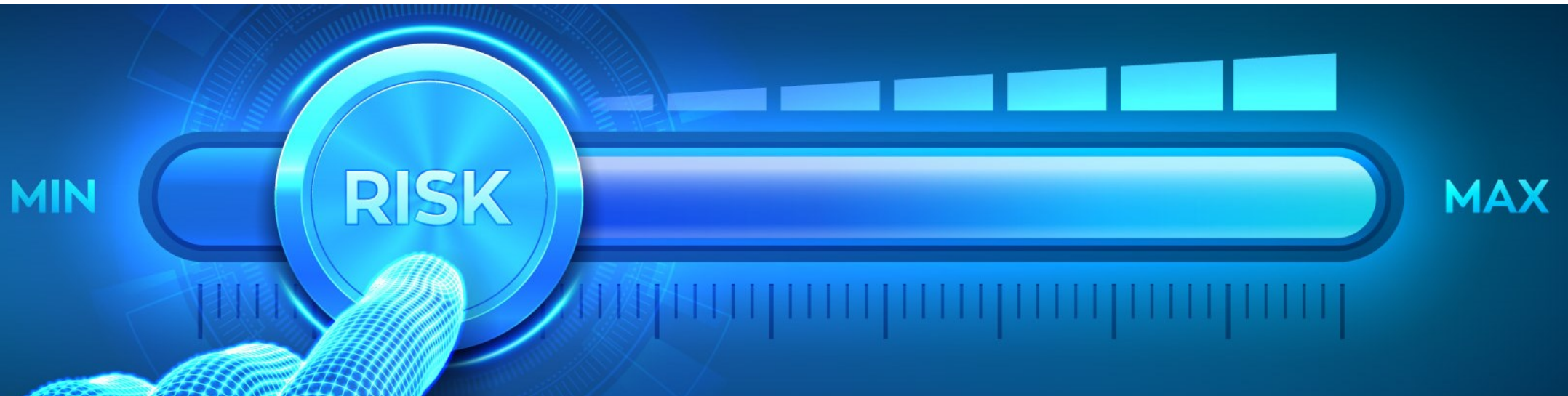
- **Cyber Security Centre of the state part of the eGovernment cloud**
  - Impact on all CII = Level of the Czech republic
- **What next?**
  - Does any European organisation need help?

# Our goals

- **Ministry of Finance Cyber Operations Centre**
- **Cyber Security Centre of the state part of the eGovernment cloud**
- Ministry of industry and trade - National Recovery Plan - Program - Building eGovernment Cloud



# How to hustle in Security?



Reactive vs active

***How we usually defend our environments and what need to be changed?***

# Reactive vs active

- **New technologies every year... EDR, XDR, SOAR, SOAPA...**
  - But do we have people to operate them?
- **How we engage with adversary if we want to engage...**
  - We block access to resources...
  - We block adversary from the environment (FW deny, isolation...)
  - We monitor the environment
- **BUT is it ENOUGH?**

Reactive vs active

***When defend, so how – just go  
active way of defense...***

# Reactive vs active

<b>Reactive defense</b>	Antivirus, Firewall, SIEM, incident response ...
<b>Active defence – Gray zone</b>	Beacons, Deception, Emulation, Hunt...
<b>Offensive operations</b>	Hacking back, cyber operations ...

# Reactive vs active

- **When defend, go active cyber defense**
  - **Add obstacles** - slows adversary down
  - **Add fake documents** - distract adversary – he doesn't know what to trust, what is fake and what is real
  - **Add shadow accounts** - which You monitor for early detection opportunity

# Reactive vs active

- **When engage, to what degree**

- Engage only at Your environment
- Prepare, Operate, Understand...

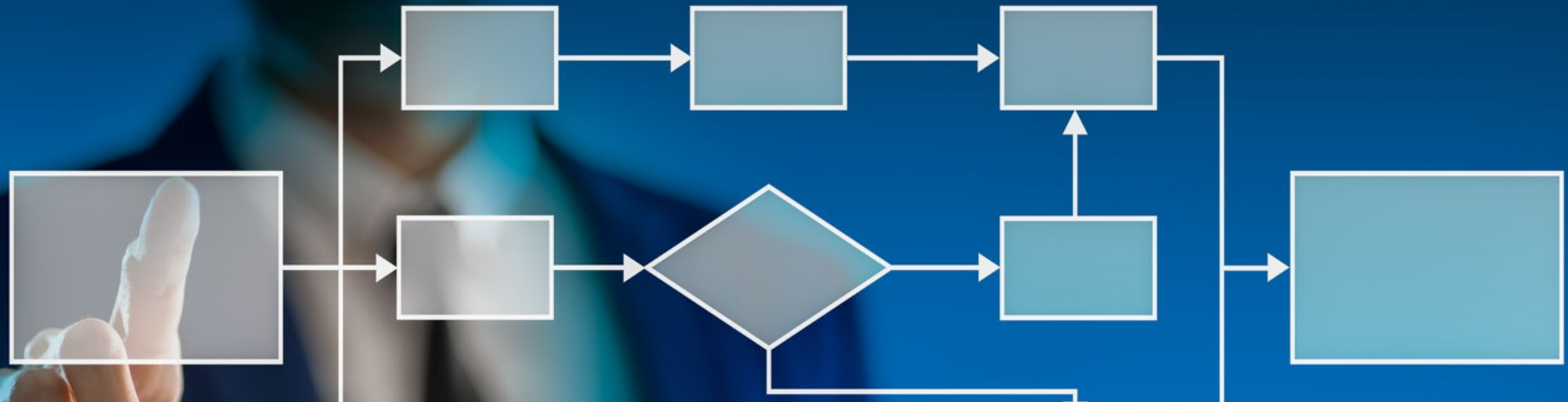
**...BUT how?**

# Reactive vs active

- **Prepare** your environment for deception activities - create your threat landscape, emulate
- **Operate the environment** – deploy tokens, shadow accounts, honeypots...
- **Understand you adversary** – do threat intelligence, analyze, learn...



# On-Premise vs Cloud vs Gov cloud



# On-Premise vs Cloud vs Gov cloud

- **Is cloud a new on-prem environment?**

...no, but seems like since traditional borders of perimeter doesn't exist anymore, perimeter begins on each workstation on each server and on each instance of cloud

# On-Premise vs Cloud vs Gov cloud

- **What are challenges?**

- Unknown environment of cloud, unknown people operating infrastructure...
- Unknown location and whereabouts of our data – need extra layer of crypto – dance like no one watching, encrypt like everyone is...

# On-Premise vs Cloud vs Gov cloud

- **Use public or government cloud?**
  - Depends on data sensitivity...
  - ...get the data of citizens to government cloud
  - Put apps and services to public or hybrid
    - front door to public
    - backend to hybrid
    - communication to private

# On-Premise vs Cloud vs Gov cloud

- **Communication in/for governments organizations via Government cloud and CI**
  - Cannot be dependable on all third party
  - Need to distinguish between different sensitivity...as I stated before

# Only cloud or Government cloud is not enough



Only cloud or Government cloud is not enough

**This is never enough... NEVER...  
we need a mindset...**

# Only cloud or Government cloud is not enough

- **Use reactive tools**
- **Filling gaps in Security with Active Cyber Defense elements...**
- **Fortunately, we have the ACD Gray zone and activities we can do...**



# Active Cyber Defence Gray Zone

<b>Adversary emulation</b>	<b>Adversary Takedowns</b>
<b>Beacons</b>	<b>Ransomware</b>
<b>Deterrence</b>	<b>Rescue Missions</b>
<b>Deception</b>	<b>Sanctions, Indictments &amp; Remedies</b>
<b>Tarpits, Sandboxes &amp; Honeypots</b>	
<b>Threat Intelligence</b>	
<b>Threat Hunting</b>	

# Lessons learned



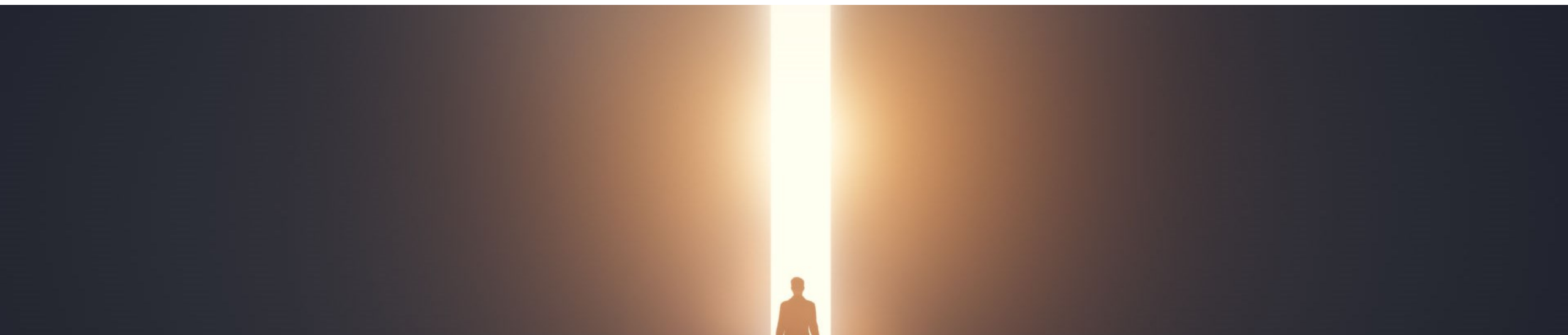
Lessons learned

***So what is current trend in the  
cyber security?***

# Lessons learned

- **Adversaries are fast in everything**
- **Need to know your:**
  - environment
  - supply chain
  - threat landscape
  - possibilities
- **Stay active**

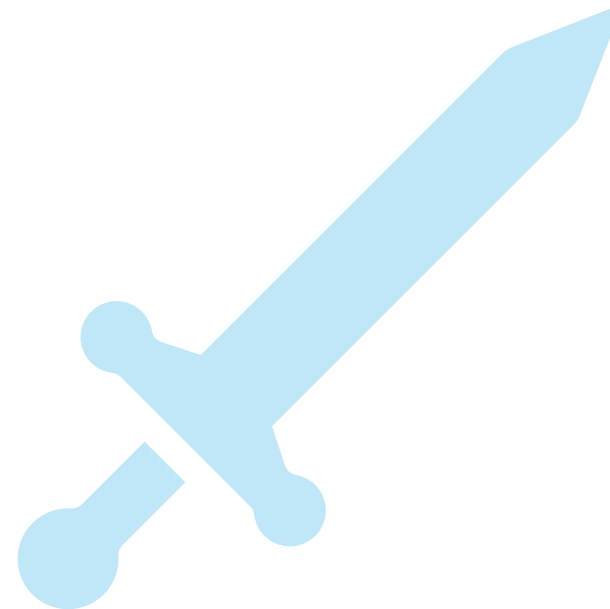
# EoF



EoF

Next time

- **Blackhat EU 2022**
- **And other not that famous conf 😊**
- **Just Follow us**



EoF

# Community

## Defcon Group 420 Czech republic

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

## MeetUps

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



EoF

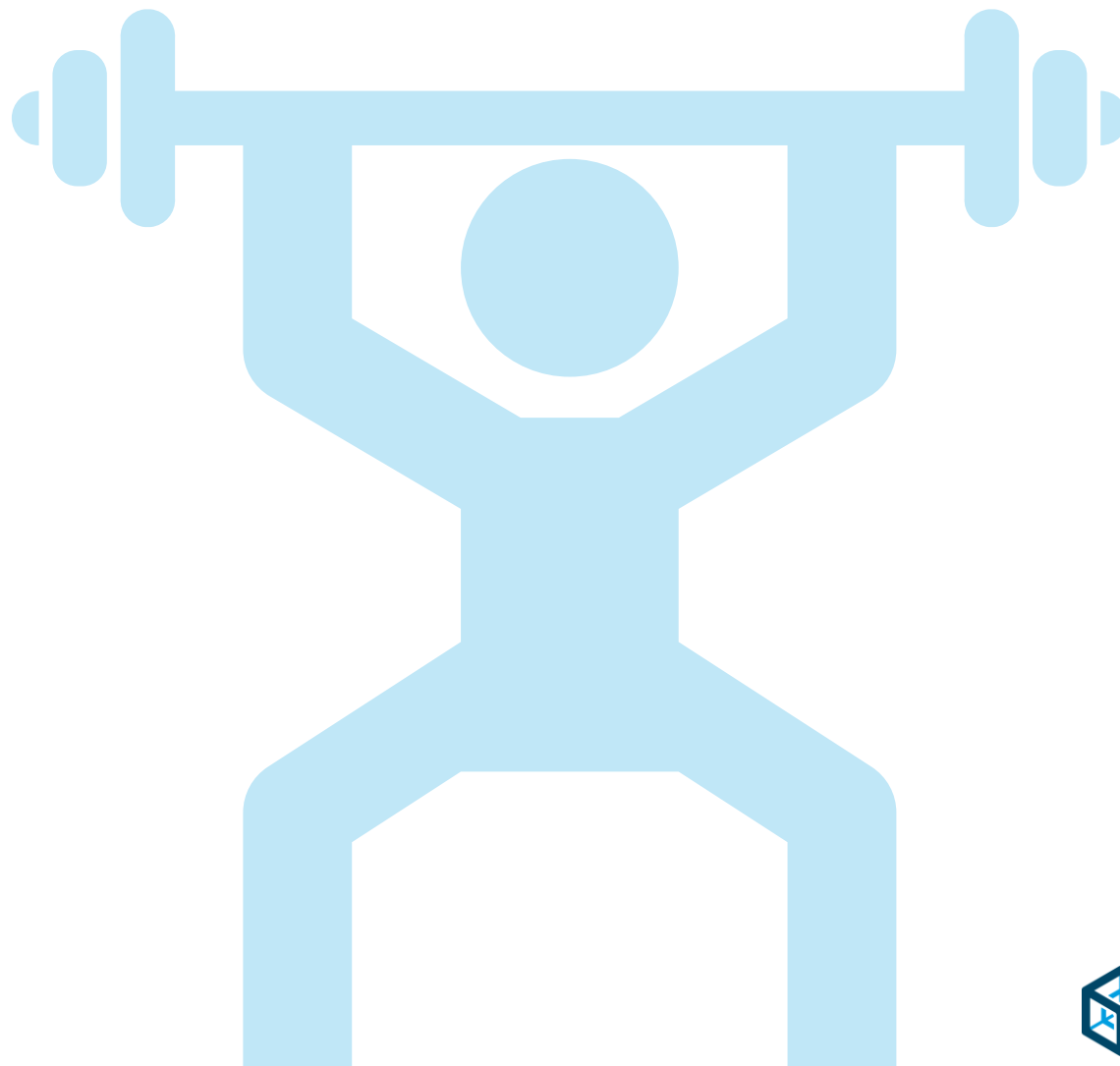
# Our Training

## MISP Training 2023

- 5. ročník - MISP, AIL, CyCAT
- **New: workflows, corellation**
- Free – On-site/On-line
- Spring 2023, ENG

## Registration

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





EoF

# Our Conference

## **Fórum aktivní kybernetické obrany 2023**

- Spring 2023, CZE

## **Registration**

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



EoF

# Keep in touch

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



# Thank you



**Q & A**