Centrum kybernetických operací MF a státního cloudu - next gen SOC

Ondřej Nekovář, Jan Pohl

AFCEA - Bezpečnostní dohledová centra (SOC)

3. 11. 2022

Státní pokladna Centrum sdílených služeb, s. p.

SPCSS

Intro

Menu

- **CSIRT-SPCSS**
- **SOC SPCSS**
- **NG SOC SPCSS**
- **Centrum kybernetických operací MF a státního cloudu**

- **O čem to není . . .**

Intro

About Us

- **Ondřej Nekovář**
  - CISO, CDO
- **Jan Pohl**
  - Practical CISO advisor

Intro

Our topics

- **SPCSS**
- **DC, Cloud, Hybrid-cloud bezpečnost**
- **Resort MF**
- **Státní část eGC**

Intro

Our business

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

Intro

Our way in maturity

- **KII NDC**
- **SOC pro MF**
- **SOC pro resort MF**
- **Resortní centrum kybernetických operací MF**
- ***Dohledové centrum státní části eGC***

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**

CSIRT-SPCSS

Státní pokladna Centrum sdílených služeb, s. p.

SPCSS

CSIRT-SPCSS

- **IR**
- **CORE plus other**
- **www.spcss.cz/csirt**

SPCSS

CSIRT-SPCSS
Roles

- **Manažer incidentu**
- **Manažer řízení rizik**
- **Architekt KB**
- **Incident handler (SOC)**
- **Koordinátor vzdělávání**

CSIRT-SPCSS

MSSP - SOC

Context

Státní pokladna Centrum sdílených služeb, s. p.

Context

Environment

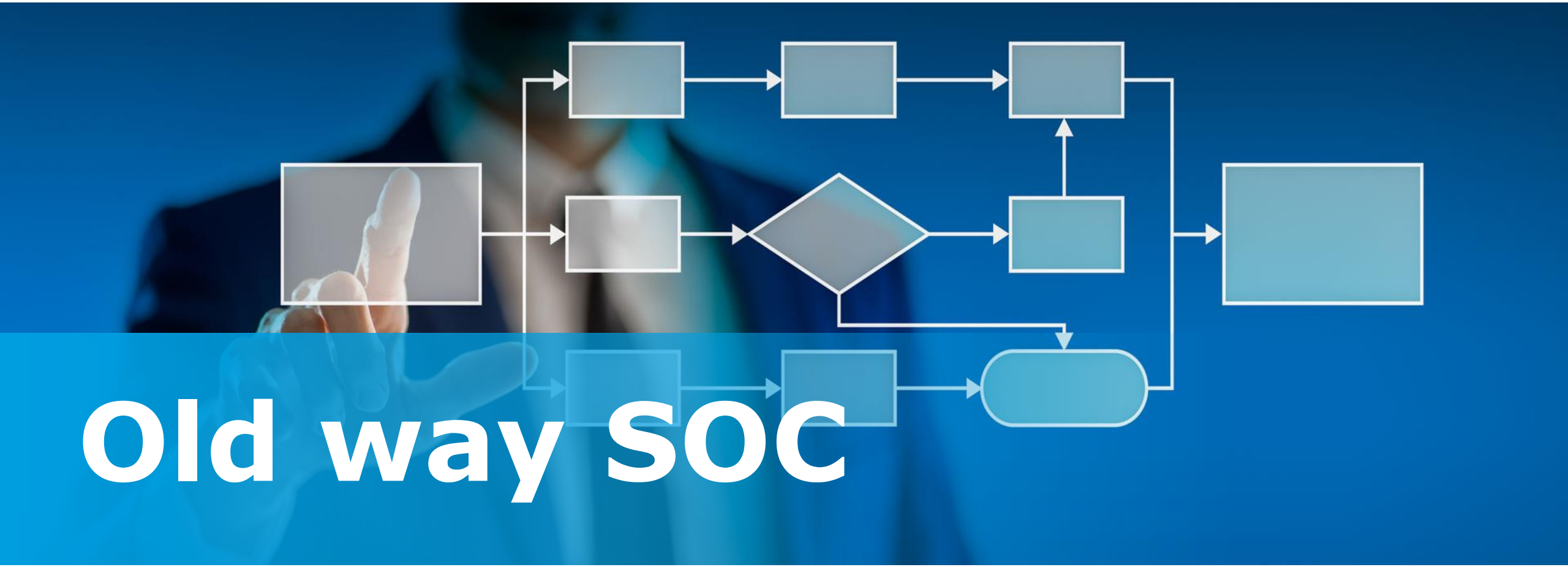
- **83 sledovaných technologií**
- **∞ množství formátů**
- **∞ dat a logů**

SPCSS:

- **On-premise**
- **Cloud (Azure, AzS, Google)**

IBM report 2021

SPCSS



Old way SOC

Kontext

SOC

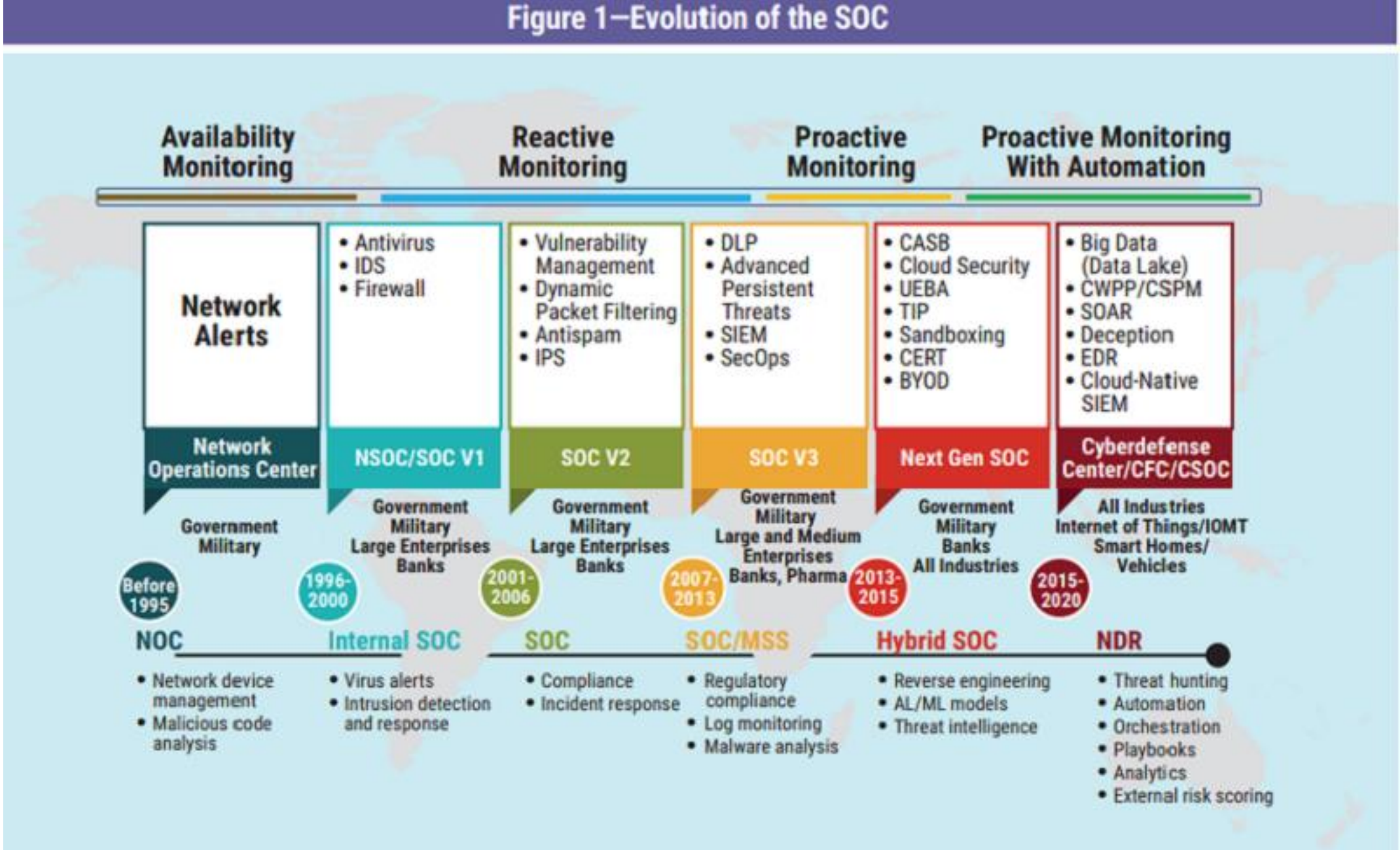
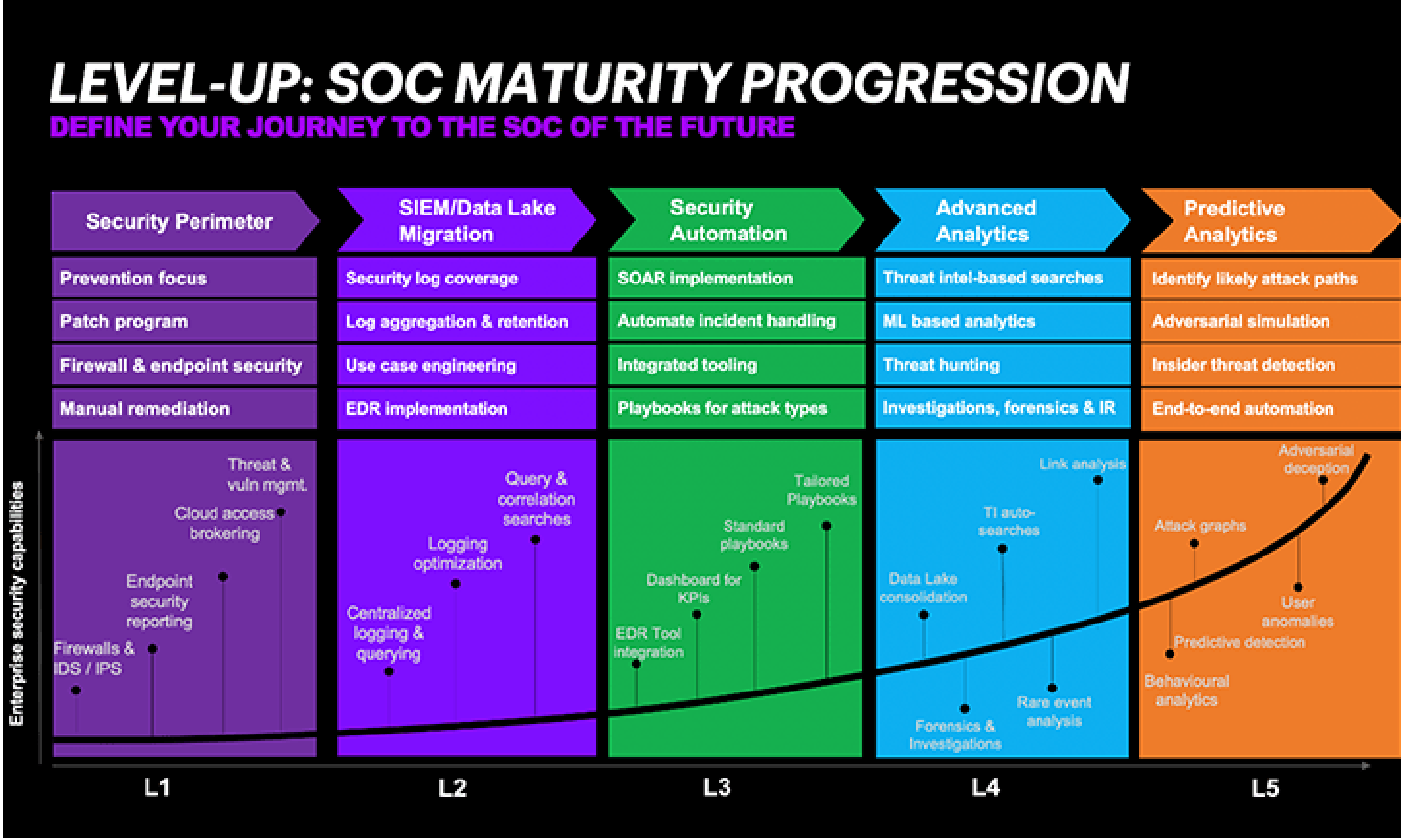


Figure 1—Evolution of the SOC
Availability Monitoring
Reactive Monitoring
Proactive Monitoring
Proactive Monitoring With Automation
Network Alerts
• Antivirus
• IDS
• Firewall
• Vulnerability Management
• Dynamic Packet Filtering
• Antispam
• IPS
• DLP
• Advanced Persistent Threats
• SIEM
• SecOps
• CASB
• Cloud Security
• UEBA
• TIP
• Sandboxing
• CERT
• BYOD
• Big Data (Data Lake)
• CWPP/CSPM
• SOAR
• Deception
• EDR
• Cloud-Native SIEM
Network Operations Center
NSOC/SOC V1
SOC V2
SOC V3
Next Gen SOC
Cyberdefense Center/CFC/CSOC
Government Military
Government Military Large Enterprises Banks
Government Military Large Enterprises Banks
Government Military Large and Medium Enterprises Banks, Pharma
Government Military Banks All Industries
All Industries Internet of Things/IOMT Smart Homes/ Vehicles
Before 1995
1996-2000
2001-2006
2007-2013
2013-2015
2015-2020
NOC
Internal SOC
SOC
SOC/MSS
Hybrid SOC
NDR
• Network device management
• Malicious code analysis
• Virus alerts
• Intrusion detection and response
• Compliance
• Incident response
• Regulatory compliance
• Log monitoring
• Malware analysis
• Reverse engineering
• AL/ML models
• Threat intelligence
• Threat hunting
• Automation
• Orchestration
• Playbooks
• Analytics
• External risk scoring

Kontext

SOC


LEVEL-UP: SOC MATURITY PROGRESSION
DEFINE YOUR JOURNEY TO THE SOC OF THE FUTURE
Security Perimeter
SIEM/Data Lake Migration
Security Automation
Advanced Analytics
Predictive Analytics
Prevention focus
Patch program
Firewall & endpoint security
Manual remediation
Security log coverage
Log aggregation & retention
Use case engineering
EDR implementation
SOAR implementation
Automate incident handling
Integrated tooling
Playbooks for attack types
Threat intel-based searches
ML based analytics
Threat hunting
Investigations, forensics & IR
Identify likely attack paths
Adversarial simulation
Insider threat detection
End-to-end automation
Enterprise security capabilities
Threat & vuln mgmt.
Cloud access brokering
Endpoint security reporting
Firewalls & IDS / IPS
Query & correlation searches
Logging optimization
Centralized logging & querying
Tailored Playbooks
Standard playbooks
Dashboard for KPIs
EDR Tool integration
Link analysis
TI auto-searches
Data Lake consolidation
Forensics & Investigations
Rare event analysis
Adversarial deception
Attack graphs
User anomalies
Predictive detection
Behavioural analytics
L1
L2
L3
L4
L5

Old way SOC

SOC basic

- SOC 24x7
- Multitenant
- Monitoring
- Detection
- Incident handling (IR tool, Playbooks)
- Passive CTI (MISP passive income)
- Forensic
- Vulnerability management

Old way SOC

Roles

- **L1 operátor**
- **Analytik KB (L2,L3)**
- **Architekt SIEM**
- **Administrátor SIEM**
- **Incident handler**
- **Správce pravidel SIEM**
- **SOC manager**

Old way SOC SPCSS

SOC old way

- **Based on reactive part**
- **Incident response cycle**
- **Response (reakce)**
- **Recovery, remediation**
- **Log management – správa logů**
- **Root cause investigation – vše na základě incidentů, které se staly**

Old way SOC SPCSS

Reactive vs active

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

SPCSS

Old way SOC SPCSS

SOC old way

- **Čím víc monitorů, tím víc SOC**


NO GO TODAY !!!

Next gen SOC

Státní pokladna Centrum sdílených služeb, s. p.

SPCSS

Next gen SOC
Principles

- **Threat-based**
- **Pro-active**
- **Integrated**
- **Automated**
- **Orchestrated**
- **Transparent**
- **Cooperated**
- **Educated customer**
- **Deceive**

Next gen SOC
Mindset

- **Threat Informed Defense**
- **The Assume Breach Paradigm**
- **Continuous monitoring and testing**
- **Paramilitar** – zkušenosti a přístup z armády (ACD operátor US Army)
- **Continuous training** (hasiči)

Old way SOC SPCSS

Reactive vs active

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

SPCSS

Next gen SOC

Active Cyber Defence Gray Zone by DCG420

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

SPCSS

Next gen SOC

Processes

Old way SOC processes plus:

- **CTI**
- **Threat hunting**
- **Detection engineering**
  - **ADS**
  - **Rules management**
  - **Data management**
- **Adversary emulation**
- **ACD Deception technology**

Next gen SOC

Roles

Old way SOC processes plus:

- **CTI operator**
- **OSINT operator**
- **Detection engineer**
- **Threat hunter**
- **Tool administrator**
- **Logsource engineer**
- **Use-case manager (Playbook manager)**

Must have for next gen SOC

Státní pokladna Centrum sdílených služeb, s. p.

SPCSS

Must have for next gen SOC

Take it easy and good

Get Your tools straight:

- **Nekupuj nepotřebné (krabice)**
- **Tune your tools (neustále a opakovat)**
- **Automate**
- **Orchestrate**

Must have for next gen SOC

CTI

- Know Your attack surface
- Know your adversary from intel point of view
- Monitor your environment (external)
- Engage (false personas, false accounts, false social live – be a spy)

Must have for next gen SOC

Hypothesis

- **Know your adversary**
- **Know adversarial tradecraft**
- **Know your enviroment**
- **Don’t be afraid to fail (Try it!)**

Must have for next gen SOC

Data and rules management

- **Data pipelines**
- **Data and log source engineering**
- **Rules management (ADS)**

Must have for next gen SOC

Train or die

- **Train SOC people same as L1**
- **Train all company – let them know you are bad and know**
- **Continuous education**

Must have for next gen SOC

Adversary engage

- **Dont be good, be bad and ugly**
- **Deceive**

Must have for next gen SOC

Cooperation

Centrum kybernetických operací MF a státního cloudu = NG SOC

Státní pokladna Centrum sdílených služeb, s. p.

SPCSS

Centrum kybernetických operací MF a státního cloudu

Státní pokladna Centrum sdílených služeb, s. p.

SPCSS

Centrum kybernetických operací MF a státního cloudu

Whats in the BOX

- **Old SOC**
- **Next gen SOC**

PLUS…

Centrum kybernetických operací MF a státního cloudu

Plus…

- **R&D**
  - Research
  - PoC
- **CTI**
  - Data-leak
- **Information exchange**
  - E-mail
  - Resortní platforma MISP
- **Communication**
  - Authorities
  - Community
  - Customers
- **Notification**
  - Actual threats
  - Summary

SPCSS

Centrum kybernetických operací MF a státního cloudu

Plus…

- **Awareness program**
  - Adversary emulation
  - Training
  - Table-top
  - Lessons learned
  - Phishing campaing
- **Reporting**
  - CTI
  - SOC
  - Vulnerabilty management

Take aways

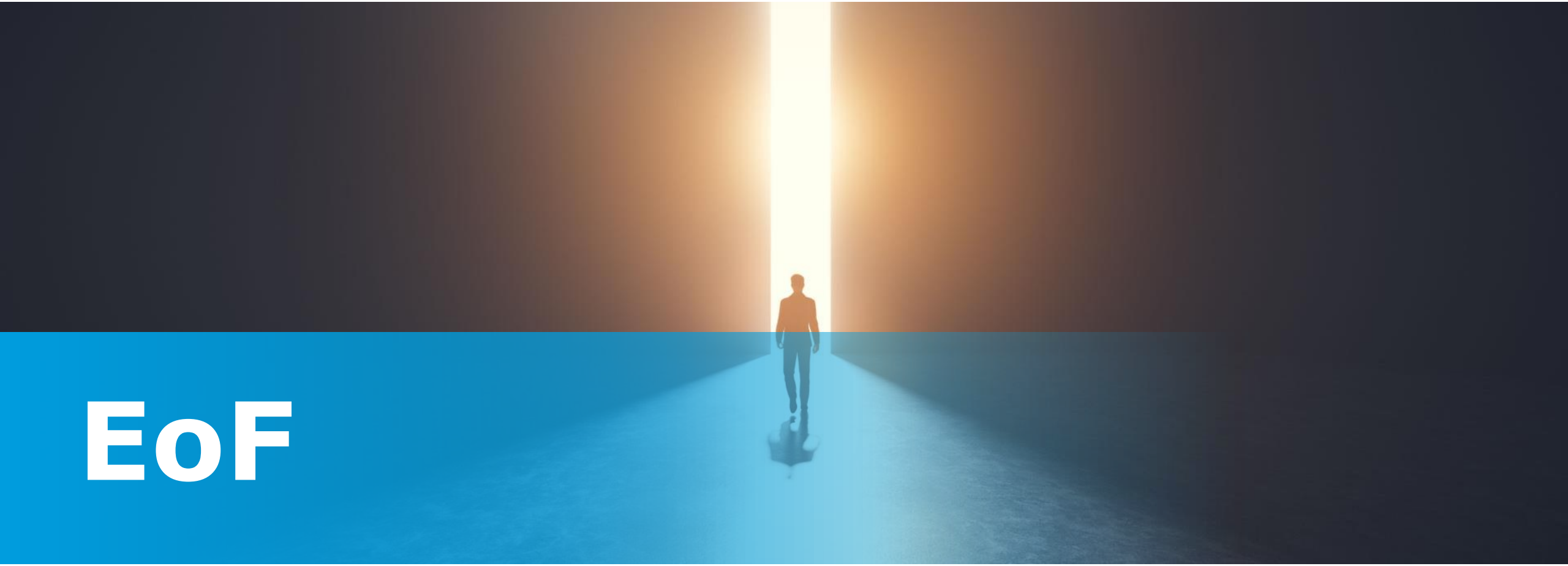
Státní pokladna Centrum sdílených služeb, s. p.

SPCSS

Take aways

Keep in mind

- **Adversaries are faster in everything**
- **Need to know your:**
  - environment
  - supply chain
  - threat landscape
  - possibilities
- **Aim to processes and loop**
- **DO NOT NEED ANY OTHER BOX, just IMPROVE**
- **Stay active**



EoF

Státní pokladna Centrum sdílených služeb, s. p.

SPCSS

EoF

Next time

- **Blackhat EU 2022**

  - Strengthening Cyber Resiliency in a Time of Geopolitical Crises: Applying Threat Intelligence & Active Defense to Protecting Critical Information Infrastructures

  - **7.12.2022, London**

EoF

Community

Defcon Group 420 Czech republic

- www.DCG420.org

MeetUps

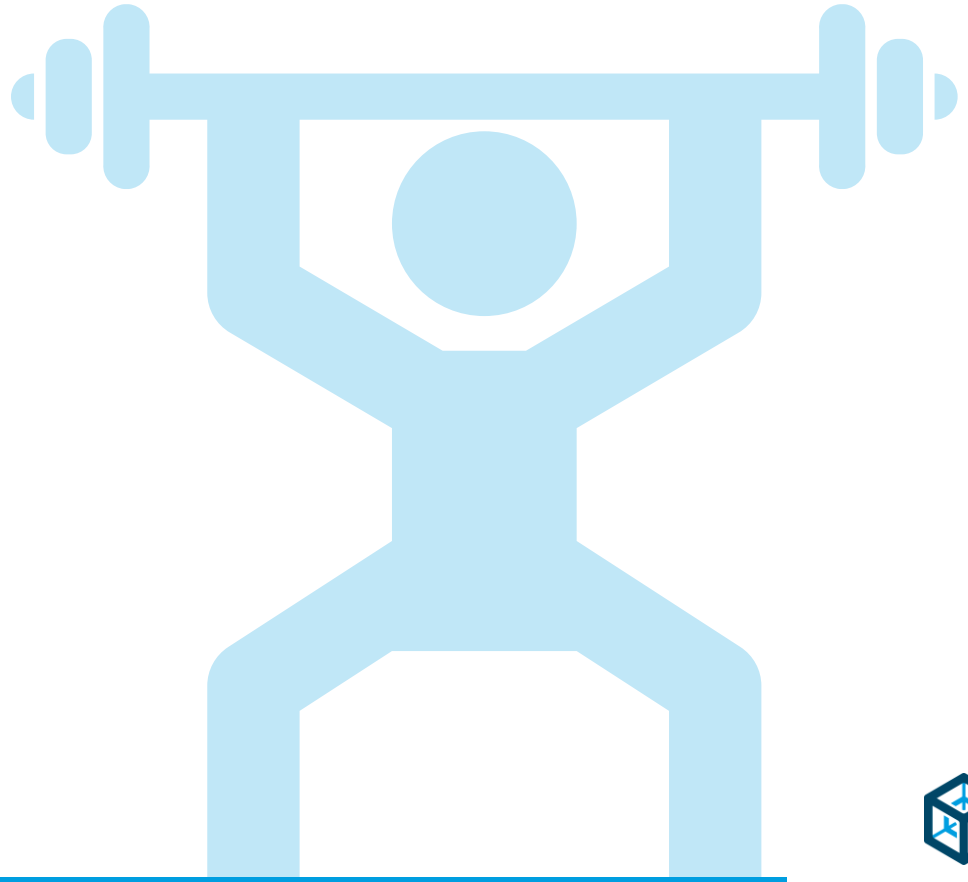
- DCG420.eventbrite.com

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

EoF

Our Conference

Fórum aktivní kybernetické obrany 2023

- 3. ročník
- Jaro 2023, česky

Registrace

- E-mail csirt@spcss.cz

EoF

Keep in touch

- **Web www.spcss.cz/csirt**
- **E-mail csirt@spcss.cz**
- **Twitter @csirtspcss**
- **Twitter @Th30ne__**
- **Twitter @adversary_mr**

Děkujeme za pozornost

Q&A