HSOC

Iniciativa pro zvýšení kybernetické bezpečnosti českého zdravotnictví

31. 3. 2021

CÍL INICIATIVY

- Cílem této iniciativy je **vznik komunity**, která zvýší počet poskytovatelů zdravotních služeb provozujících bezpečné informační technologie s dostatečným technickým a personálním zázemím.
- Cíle a aktivity iniciativy jsou shrnuty v **memorandu** - https://hsoc.cesnet.cz/

- Zdravotnictví nejen v ČR čelí rostoucímu **riziku** kybernetických útoků.
- **Reálná hrozba** kybernetického napadení jednotlivých nemocnic i většího počtu zdravotnických zařízení současně roste den ze dne.
- **Velké rozdíly** v úrovni IT podpory a potřebami jednotlivých nemocnic.
- **Chybí sdílená vize**, jak využít výhody digitálních technologií k transformaci zdravotnictví.
- Problematika kybernetické bezpečnosti je ve zdravotnictví zásadně **personálně a finančně podhodnocena**

DŮVODY VZNIKU KOMUNITY

HSOC HOSPITAL SECURITY OPERATION CENTRE

Jméno	Instituce
Petr Pavlinec	Kraj Vysočina
Dušan Chvojka	Nemocnice Na Homolce
Antonín Hlavinka	FN Olomouc
Jan Kvaček	Nemocnice Na Bulovce
Vladimír Mařík	ČVUT
Martin Mareček	FNUSA
Ctirad Procházka	ÚVN
Miroslav Sučík	ÚVN
Lenka Lhotská	ČVUT CIIRC & FBMI
Oto Sládek	ČVUT FEL Kybertec s.r.o.
Michal Trefil	Odborný léčebný ústav Paseka, p.o.

Jméno	Instituce
Radek Řechka	Oblastní nemocnice Příbram, a.s.
Jiří Smetana	ZZS Karlovarského kraje
Jan Gruntorád	Cesnet
Andrea Rakovičová	ZZS Olomouckého kraje
Vladimír Dzurilla	NAKIT
Libor Seneta	Zdravotnická záchranná služba Královéh
Ivan Veselý	Všeobecná fakultní nemocnice
Josef Nouzák	Oblastní nemocnice Kolín, a.s.
Tomáš Iránek	Krajská nemocnice T. Bati, a. s
Martina Jirsová	Krajská nemocnice Liberec, a.s.

SIGNATÁŘI MEMORANDA

HSOC HOSPITAL SECURITY OPERATION CENTRE

- Odborní a technologičtí partneři
  - CESNET
  - NUKIB
  - NAKIT
  - OHA MVČR
  - ČVUT

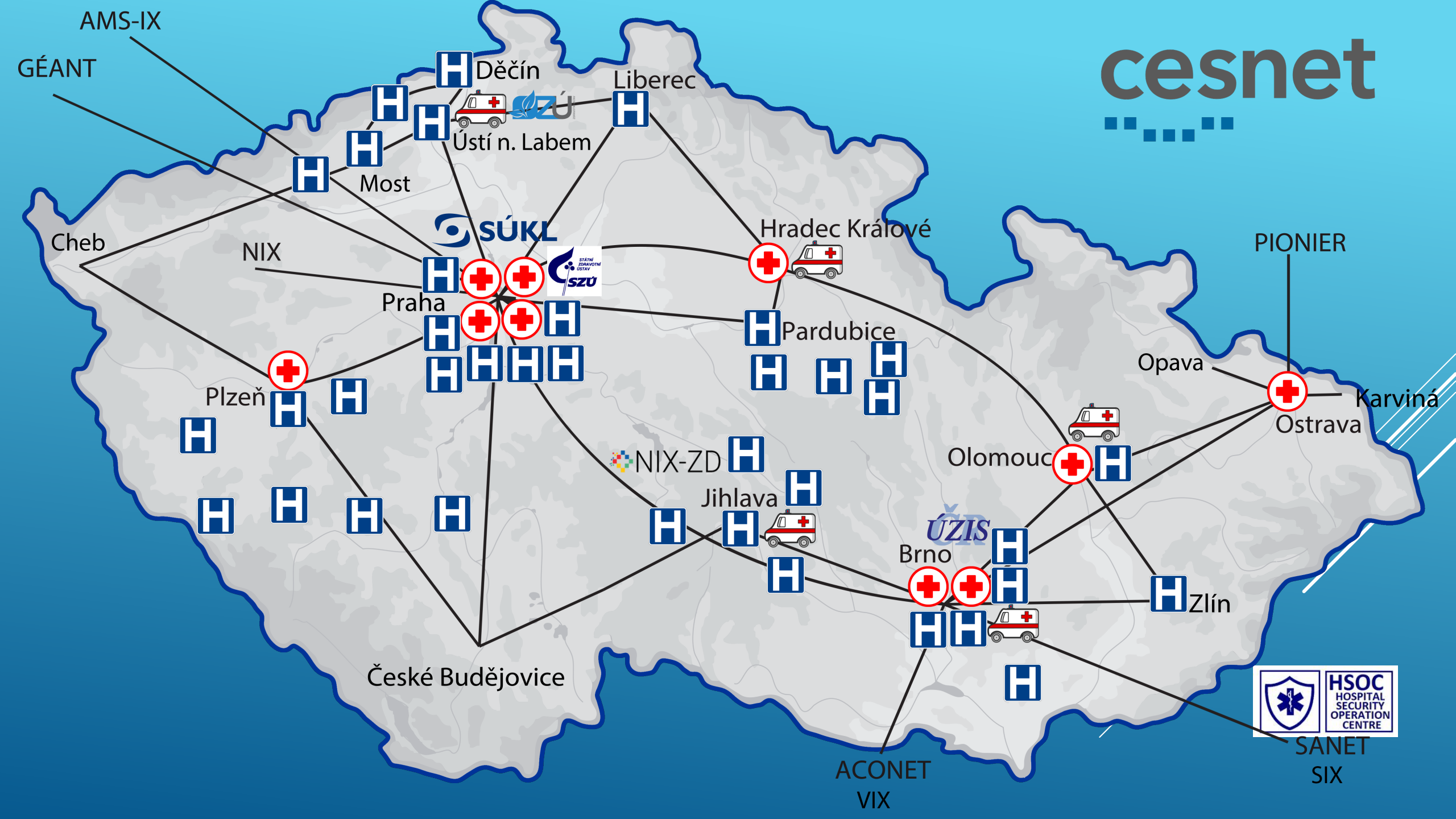
CÍL INICIATIVY

HSOC
HOSPITAL
SECURITY
OPERATION
CENTRE

CESNET – TECHNOLOGICKÝ PARTNER

- Národní síť pro vědu a výzkum
- e-infrastruktura CESNET - schválená vládou ČR
  - podpora specifických potřeb uživatelských komunit
  - provoz síťové infrastruktury – od počátku Internetu v ČR
  - připojeno 42 nemocnic
    - + další subjekty ve zdravotnictví (např. SUKL, SZU, ZZS,…)
    - Fakultní nemocnice, Krajské nemocnice, …
- CESNET CERTS
  - 1 CSIRT tým V ČR
  - mezinárodně akreditován
  - vznik a předání CSIRT.CZ (CZ.NICu)
- řada národní i mezinárodních bezpečnostních projektů
- Forenzní laboratoř
- ISO 27001

HSOC HOSPITAL SECURITY OPERATION CENTRE


AMS-IX
GÉANT
Děčín
Liberec
ÚZÚ
Ústí n. Labem
Most
SÚKL
Cheb
NIX
Praha
SZÚ
Hradec Králové
PIONIER
Pardubice
Opava
Plzeň
Karviná
Ostrava
NIX-ZD
Olomouc
Jihlava
ÚZIS
Brno
Zlín
České Budějovice
HSOC
HOSPITAL SECURITY OPERATION CENTRE
SANET
SIX
ACONET
VIX

CO JE A NENÍ CÍLEM hSOC

hSOC je…

- Platforma pro výměnu informací a dobré praxe
- Varovný a koordinační komunikační kanál
- Platforma pro provoz sdílených služeb a technologií
- Komunita IT a bezpečnostních profesionálů a nadšenců
- Prostor pro vzdělávání

hSOC není…

- Univerzální řešení bezpečnosti zdravotnického zařízení
- Subjekt (zatím)
- Dohledové bezpečnostní centrum

HSOC HOSPITAL SECURITY OPERATION CENTRE

Ustanovení **pracovních skupin**

- Jejich komunikačních kanálů (maillisty, videokonference) https://hsoc.cesnet.cz/cs/skupiny
- **hSOC-Tech** - Technická pracovní skupina
  - Určeno pro bezpečnostní analytiky, síťové a SW specialisty
- **hSOC-Emergency** – Sdílení informací o bezpečnostních hrozbách
  - **Otevřené pro poskytovatele zdravotnických služeb (nemocnice, ZZS,…)**
  - Zapojeno 29 organizací včetně NUKIB, NAKIT,…
- **hSOC-Man** - právní, legislativní a institucionální aspekty
  - Určeno pro právníky, DPO, manažery
- **hSOC-HR** – lidské zdroje a vzdělávání v oblasti kybernetické bezpečnosti
  - Určeno pro personalisty a pedagogy,

NA ČEM PRACUJEME

HSOC HOSPITAL SECURITY OPERATION CENTRE

46 zapojených subjektů a další „sledující“ aktivitu

- Podpora a zapojení NUKIB, NAKIT, OHA MVČR, …
- Vyhražená síťová infrastruktura (HSOC-VRF)
- Sdílení know-how a lidských kapacit
  - best-practice, koncepce a design architektury
  - 5 školení, seminářů a školení
  - technologické standardy
  - potenciál vzniku společného (komunitního) CSIRT týmu
- Nastavení workflow a procesů u zapojených subjektů
- Emergency komunikační kanály
  - mailing-listy, videokonferenční systém

HSOC HOSPITAL SECURITY OPERATION CENTRE

HSOC STATUS

Uzavřená bezpečná síť HSOC

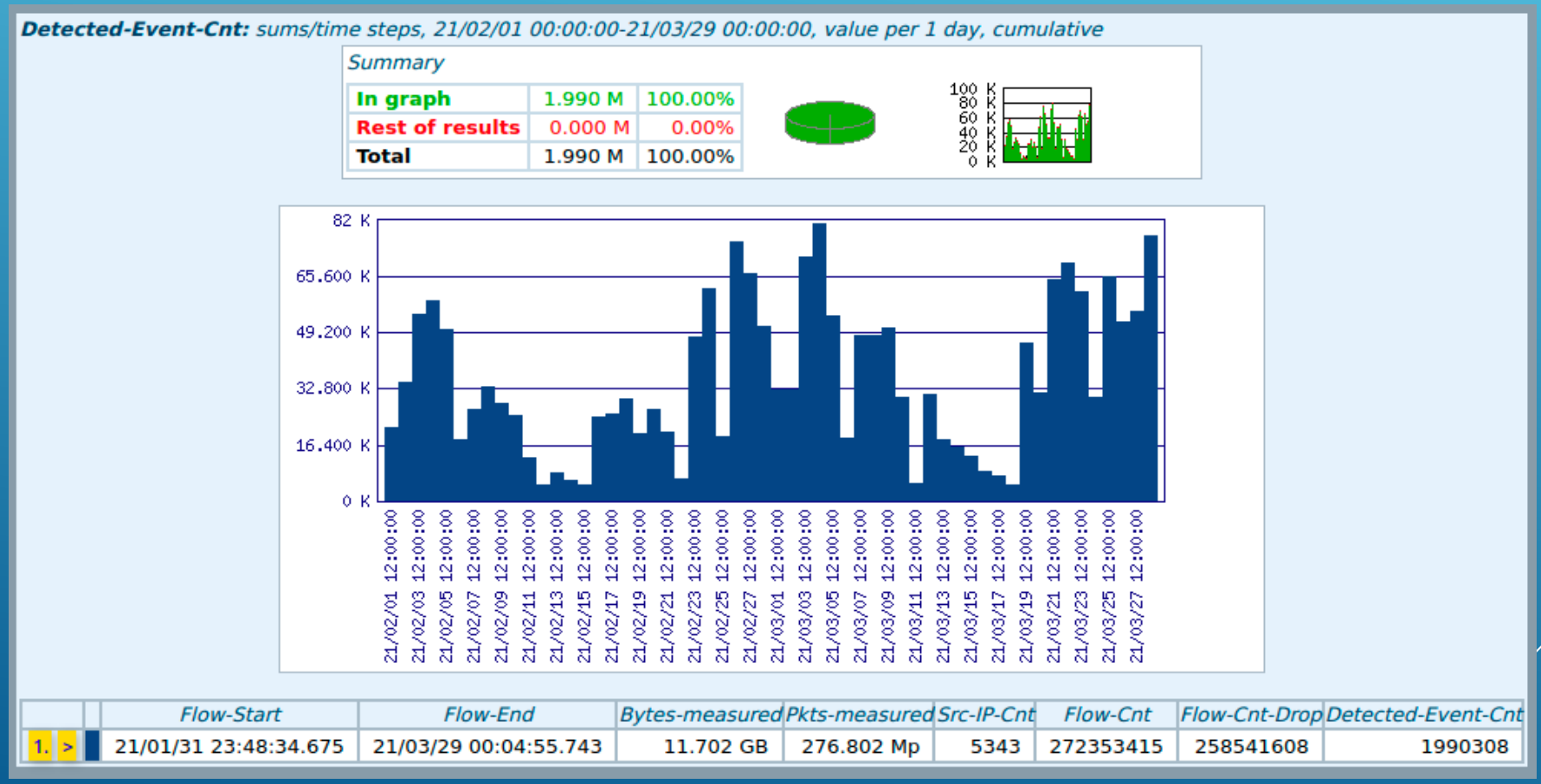
- Prvních 5 nemocnic zapojeno: FNUSA, NNH, Nem.Jihlava, UVN, KN Liberec,
  - … další v procesu připojování: FN Olomouc, VFN, FN Brno …
- Redundantní geografické připojení - přepojení s Internetem v několika lokalitách
- Monitorovací a bezpečnostní nástroje
- Společné politiky a pravidla
  - V současnosti denně cca 80 – 90 tis. detekovaných a automaticky mitigovaných hrozeb na perimetru sítě
- Sdílení know-how a lidských kapacit
  - Potenciál vzniku společného CSIRT týmu

HSOC – VRF

- Geografická redundance přepojení do Internetu ve dvou lokalitách
- Ochrana
  - proti podvržení IP adres (IP spoofing),
  - proti podvržení oznamovaných prefixů od peering-partnerů,
  - proti amplifikačním (volumetrickým) DDoS útokům,
  - proti agresivním i pomalým scanům,
  - nástroji pro uživatele pro analýzu a regulaci svého provozu v síti e-infrastruktury CESNET,
  - automatickým přesměrováním provozu k vyčištění v jádru globálního internetu (celosvětová mitigace vůči detekovaným zdrojům nežádoucího provozu.
- Tvrději nastavené limity a politiky
  - Možnost omezení, zahození útoku ještě na páteřní síti

Denní agregovaný pohled

- 82 tisíc detekovaných událostí za den
- celkem 1.99 mil. detekovaných událostí a týkal se 5343 zdrojových IP adres
- Cca 95 % podle detekce zahozena



	Flow-Start	Flow-End	Bytes-measured	Pkts-measured	Src-IP-Cnt	Flow-Cnt	Flow-Cnt-Drop	Detected-Event-Cnt
1. >	21/01/31 23:48:34.675	21/03/29 00:04:55.743	11.702 GB	276.802 Mp	5343	272353415	258541608	1990308

HSOC HOSPITAL SECURITY OPERATION CENTRE

Další aktivity a plány hSOC

- Metodika penetračního testování
- Podpora komunitního sdílení prostřednictvím projektové metodiky -
- Příprava projektové žádosti do fondu GEANT
- Prezentace konceptu hSOC novému vedení AKČR (v rámci eHealth strategie krajů)
- Návrh metodiky řízení bezpečnosti v nemocnicích – principy ISMS, vznik (certifikovaných) CSIRT týmů
- Návrh další strategie v oblasti využití neveřejných sítí ve zdravotnictví (KIVS-CMS, VCR hSOC, síť AKČR, TESTA-NG) – jednání s OHA MVČR

HSOC
HOSPITAL SECURITY OPERATION CENTRE

VÍCE NA ….

HTTPS://HSOC.CESNET.CZ/

HSOC
HOSPITAL
SECURITY
OPERATION
CENTRE