Krav, lovgivninger, rammeværktøj og anbefalinger! Der er meget at forholde sig til, når man arbejder med cybersikkerhed i et højt digitaliseret sundhedsvæsen, og det stiller ofte krav til både ressourcer og kapaciteter, som mange organisationer ikke kan honorere. Så hvor skal man prioritere sin indsats, og hvad er det rent faktisk, vi ser på tværs af sundhedssektoren?

Sundhedssektoren har i 2022 og 2023 etableret en tværgående overvågnings- og analyseplatform og opbygget et styrket operativt samarbejde imellem de lokale sikkerhedskapaciteter og sundhedssektorens centrale analysecenter i Sundhedsdatastyrelsen.

Gennem den nyeste teknologi overvåger og analyserer Platformen aktørernes infrastruktur og den aktivitet, der er på netværket. Formålet er at opdage, analyse og bidrage til at stoppe ondsindet aktivitet. Denne indsigt i datatrafikken giver et nærrealtidsbillede af, hvad der rent faktisk foregår på tværs af sektoren, og dette bidrager til at forstå de angrebsvektorer og metoder, som hackerne gør brug af.

Oplægget gør dig bl.a. klogere på:

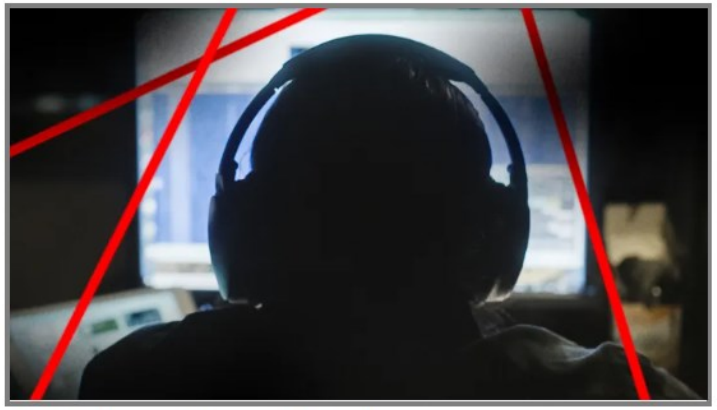
- Hvilke faktiske typer af cyberkriminalitet udspiller sig i cyberspace?
- Hvad rammer faktisk den danske sundhedssektor?
- Hvordan opdager man det?
- Hvordan kommer man med i platformen og samarbejdet som aktør i sundhedssektoren!?

Cyberkriminalitet – Det her skal du være bange for!

E-sundhedsobs session 85

SUNDHEDSDATA-STYRELSEN

Episoder



1. Putins spioner i Norden

19. APR 2023 | 53M

En hemmelig liste med navne på mistænkte russiske efterretningsofficerer sætter nordiske journalister i gang med at undersøge Putins spioner i Danmark, Norge og...

2. De russiske spionskibe

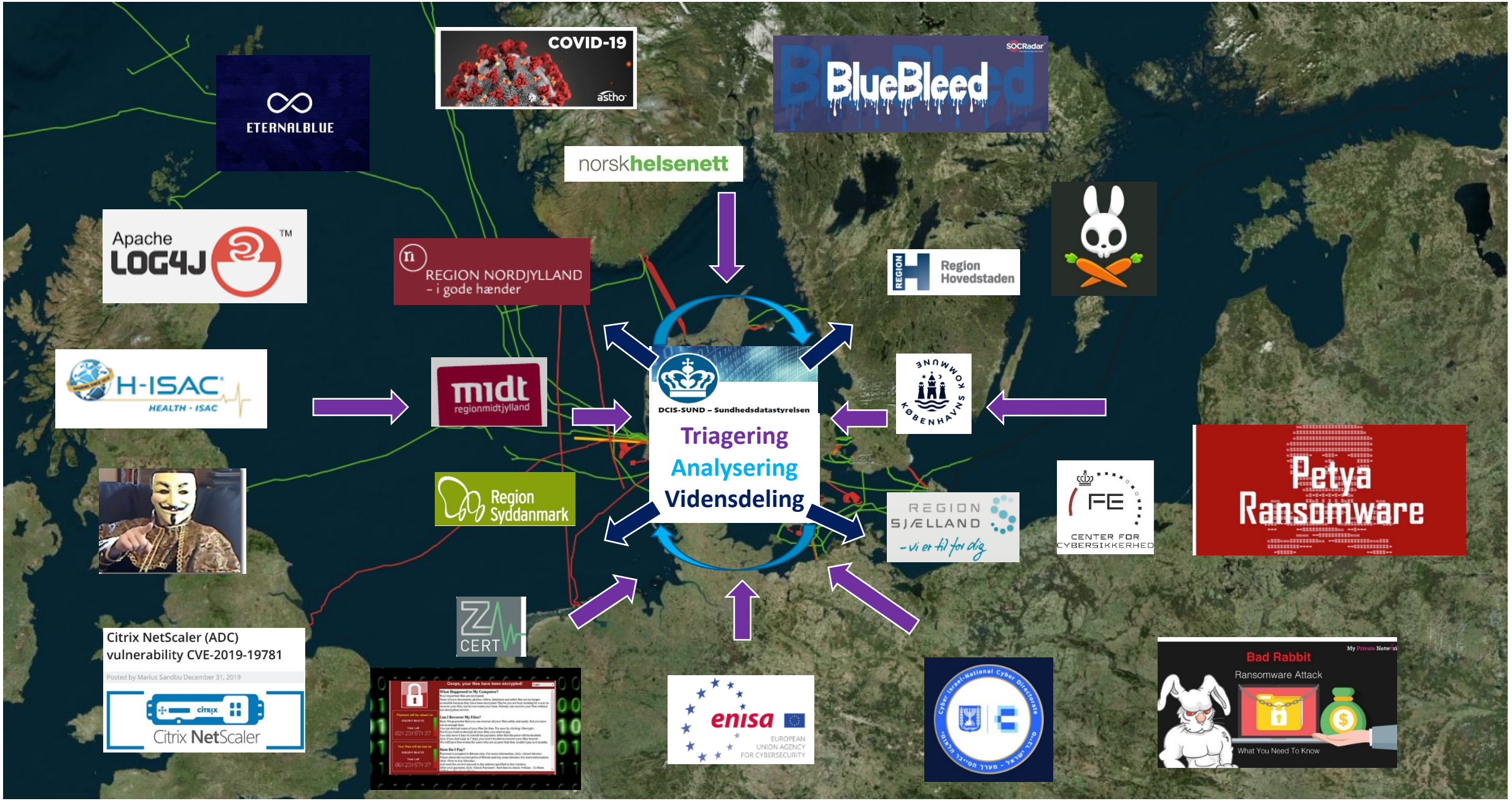
26. APR 2023 | 49M

En tidligere efterretningsofficer i England lytter med, da et formodet russisk spionskib sejler ind i indre dansk farvand mellem Sjællands Odde og Grenå. Skibet med en...

3. Kampen om sandheden

3. MAJ 2023 | 58M

Hemmelig radiokommunikation fra den russiske flåde kan måske hjælpe med at kaste lys over, hvad der skete, da Nord Stream-gasrørene blev sprængt i efteråret 2022....



Pas på kablerne - når du fisker og ankrer https://dkcpc.dk/

SUNDHEDSDATA-STYRELSEN

Strategien

Den nationale strategi for cyber- og informationssikkerhed fra maj 2022-2024

Primære fokusområder
- Hver sektor skal lave en strategi
- Oprette en DecentralCyber- og InformationsSikkerhedsenhed

Sundhedssektorens cyber- og informationssikkerhedsstrategi 2019-2022

Yderligere fokus
- Mere fokus på operative kapaciteter
- Mere fokus på samarbejde på tværs
- Flere faste krav til cybersikkerheden

Ny strategi Q3 2023
- Videreføre alt det gode

https://digst.dk/strategier/cyber-og-informationssikkerhed/

https://sundhedsdatastyrelsen.dk/da/strategier-og-projekter/cyberstrategi

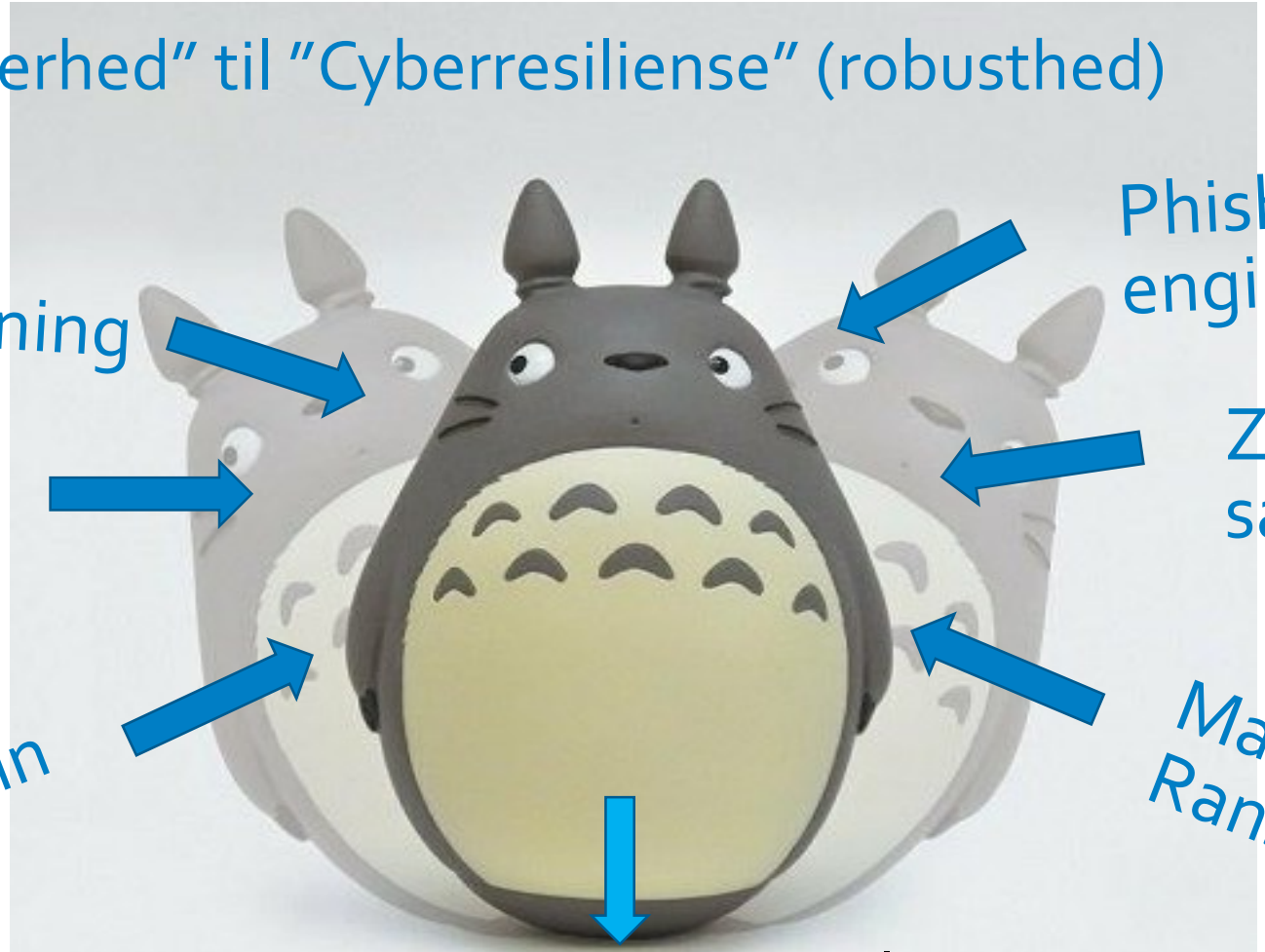
SUNDHEDSDATA-STYRELSEN

Hvordan opdager man hackere i en hel sektor??

3.2 Etablering af funktioner til overvågning og analyse af aktivitet på sundhedssektorens it-systemer og -infrastruktur

SUNDHEDSDATA-
STYRELSEN

Fra "Cybersikkerhed" til "Cyberresiliense" (robusthed)



DDoS overbelastning

Phishing & Social engineering

Industri spionage

Zero Day sårbarheder

Supply chain angreb

Malware & Ransomware

Business continuity plans

Løbende test af restore, beredskab og reetablering

Automatiseret Detection (and Response)

https://www.weforum.org/agenda/2021/11/why-move-cyber-security-to-cyber-resilience

Hvad er en SOC/SAC??

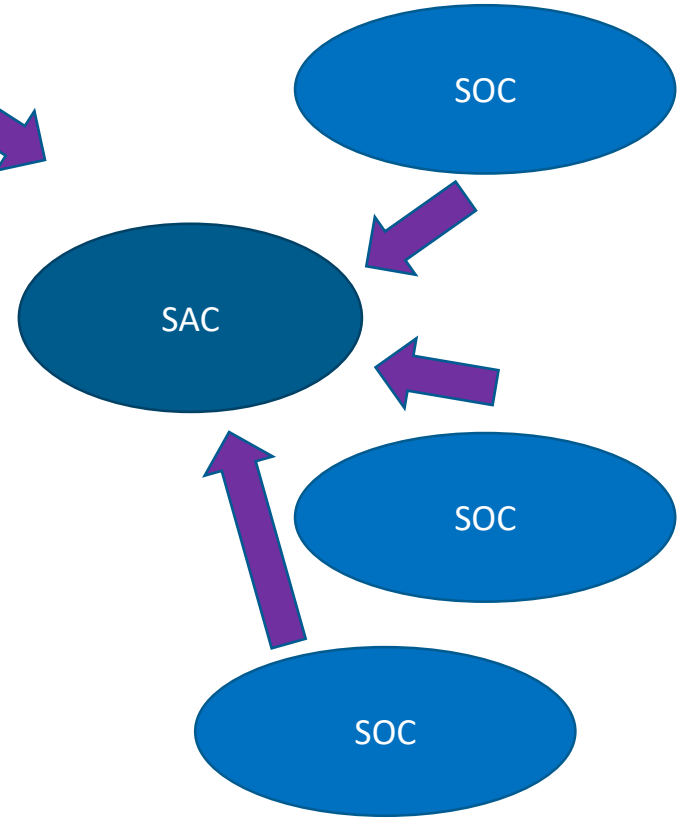
SOC: ”Security Operations Center”

med ansvar og fokus på lokal aktivitet

SAC: ”Security Analysis Center”

“Et ekstra par øjne”

Med fokus på tværgående aktivitet og samarbejde på tværs af sektoren



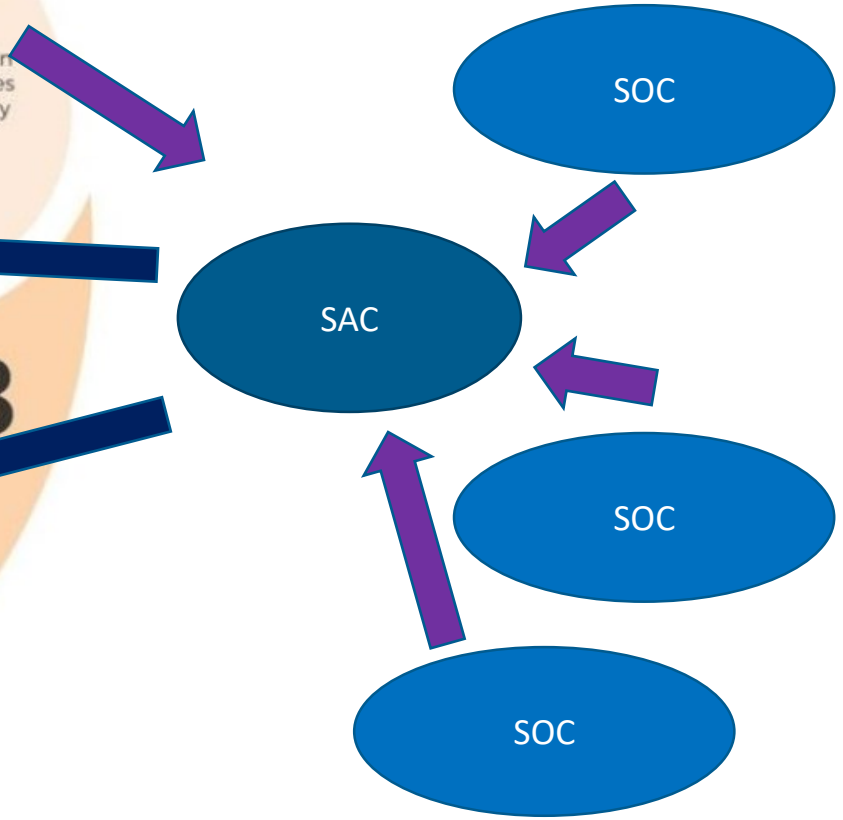
Hvad er en

Impact	Urgency	Priority ▲
Search	Search	Search
1 - High	1 - High	1 - Critical
2 - Medium	1 - High	2 - High
1 - High	2 - Medium	2 - High
3 - Low	1 - High	3 - Moderate
2 - Medium	2 - Medium	3 - Moderate
1 - High	3 - Low	3 - Moderate
3 - Low	2 - Medium	4 - Low
2 - Medium	3 - Low	4 - Low

SAC: ”Security Analysis Center”

“Et ekstra par øjne”

Med fokus på tværgående aktivitet og samarbejde på tværs af sektoren



Teknisk løsning, der skal håndterer en hel sektor ved fuld dækningsgrad?

- Op til 100 petabytes data om måneden (fra wikipedia. 200 PB: Alt udskrevet materiale i verden)
- Op til 250.000 medarbejdere
- Op til 600.000 enheder
- Meget bredt og sammenhængende IT-landskab
- Store forskelle i ressource allokeringen og cyber kompetencerne
- Mange legacy systemer og enheder
- Stor del af data hos aktører er betegnet som følsomme personoplysninger

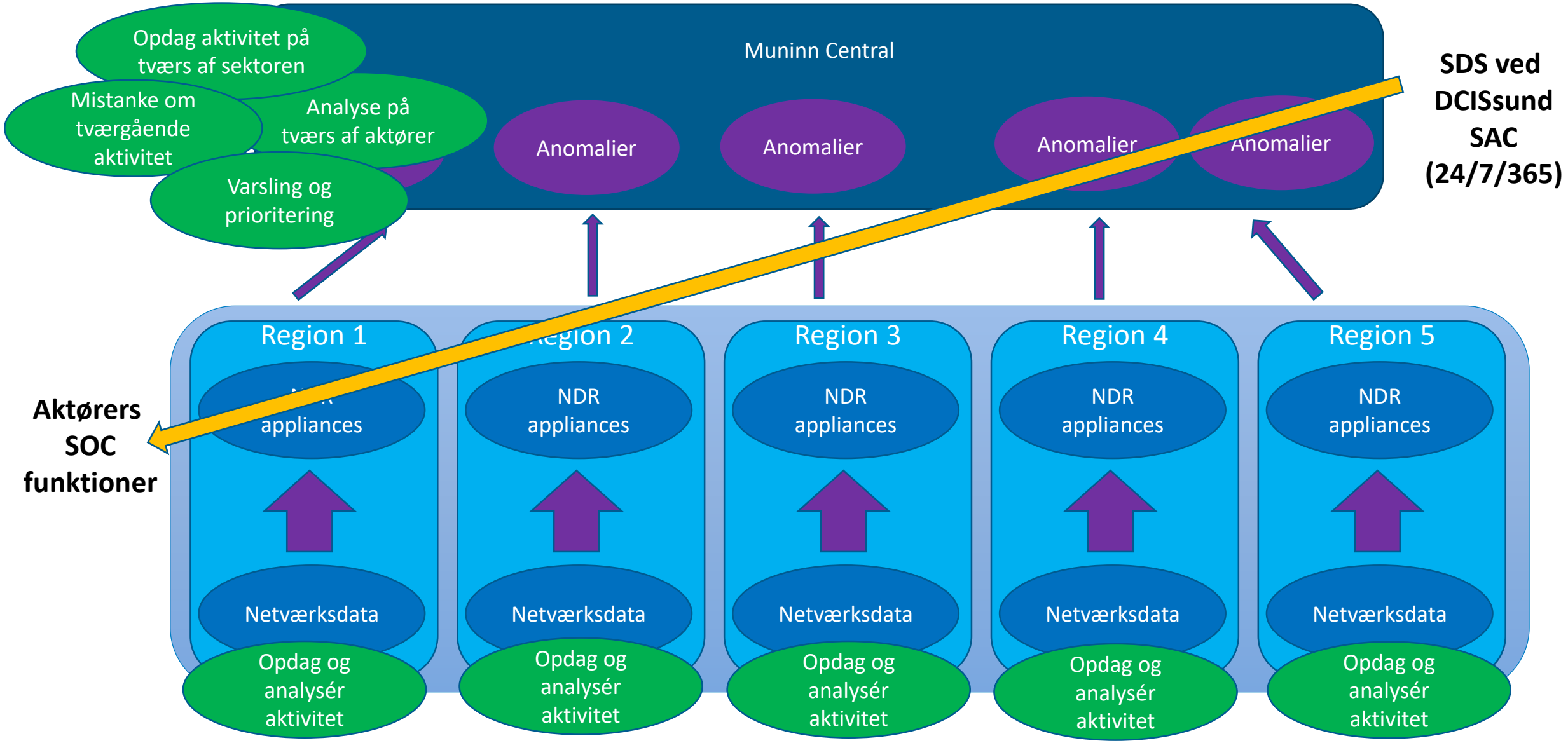
Sundhedssektoren:

- 10 statslige styrelser, 5 Regionale aktører, 98 Kommuner
- 5-6000 i det nære sundhedsvæsen, herunder almen praksis og speciallæger
- 3000 øvrige aktører, herunder fx apoteker, privathospitaler, Fys/ergo mv.

Hastighedsmål:
Indenfor 15 min
kritisk tværgående
angreb rapporteres
(24/7/365)

Lokal dækningsgrad:
>95% af ind- udgående
>80% af "datacenter trafik"
så meget som muligt af klientnetværk

Løsning baseret på Netværk Detection and Response (NDR)



SUNDHEDSDATA-STYRELSEN

Internationalt samarbejde

HelseCERT

H-ISAC HEALTH - ISAC

CTI LEAGUE

EU HEALTH ISAC

SUNDHEDSDATA-STYRELSEN

Trusler

Triagering
Analysering
Vidensdeling

SAC

Aktivitet

Dagligt operationelt teknisk samarbejde SAC / SOC

SOC

SOC

SOC

Muninn

aeven

Varslings system

MISP Threat Sharing

Nationalt samarbejde

ENERGI CERT

TELEDCIS

SØFARTSSTYRELSEN

FINANSTILSYNET

MISP Threat Sharing

Trusler
Sårbarheder
Aktivitet

FE CENTER FOR CYBERSIKKERHED

Mattermost

Sektor samarbejde

Indications of Compromise (IOC)

SUNDHEDSSTYRELSEN

SUNDHEDSDATA-STYRELSEN

STATENS SERUM INSTITUT

NATIONALT GENOM CENTER

LÆGEMIDDELSTYRELSEN

SUNDHEDS- OG ÆLDREMINISTERIET

STYRELSEN FOR PATIENTKLAGER

STYRELSEN FOR PATIENTSIKKERHED

PRAKTISERENDE LÆGERS ORGANISATION 3436

apotek 468

FAS 1000

REGION NORDJYLLAND – i gode hænder

Region Hovedstaden

midt regionmidtjylland

REGION SJÆLLAND

Region Syddanmark

Andre private aktører Ca. 2000

KL 98

DANSKE REGIONER

PL

TANDLÆGE FORENINGEN 1923

SUNDHED DANMARK 27

850

MEDICO INDUSTRIEN

sundhed.dk

medcom

Sårbarheder

CYCOGNITO

tenable

Mulighed for automatisk beskyttelse ud fra IOC'er og IOB'er" i firewall (Ved A1)

Operative "SOC'er" hos aktører

SUNDHEDSDATA-STYRELSEN

Tilslutning: Proces

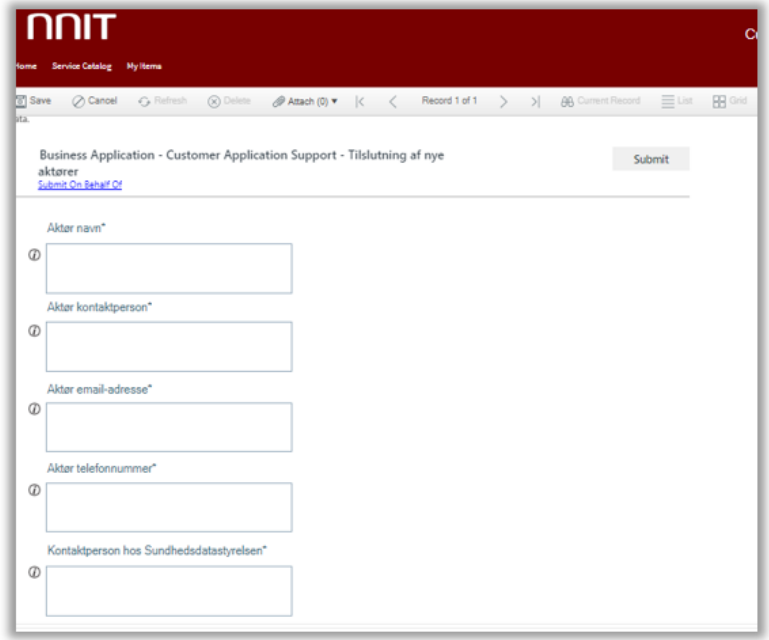
DCISSund@sundhedsdata.dk

Bestilling af ny aktør

SDS bestiller "Ny aktør" gennem NNITs Customer Service Portal

SDS registrerer følgende informationer i sagen:

- Aktør navn
- Kontaktperson info for aktøren
  - Navn
  - E-mail
  - Telefonnummer
- Kontaktperson hos SDS



SUNDHEDSDATA-STYRELSEN

Spørgsmål?

Søren Bank Greenfield

SBGR@sundhedsdata.dk

SUNDHEDSDATA-
STYRELSEN

Sundhedsdatastyrelsen
Ørestads Boulevard 5
2300 København S

T: +45 7221 6800
E: kontakt@sundshedsdata.dk
W: sundhedsdata.dk

Kontakt

DCIS Sund

DCISSUND@sundhedsdata.dk

DCISSund på Twitter
@dcissund

DCISSund information
https://sundhedsdatastyrelsen.dk/informationssikkerhed