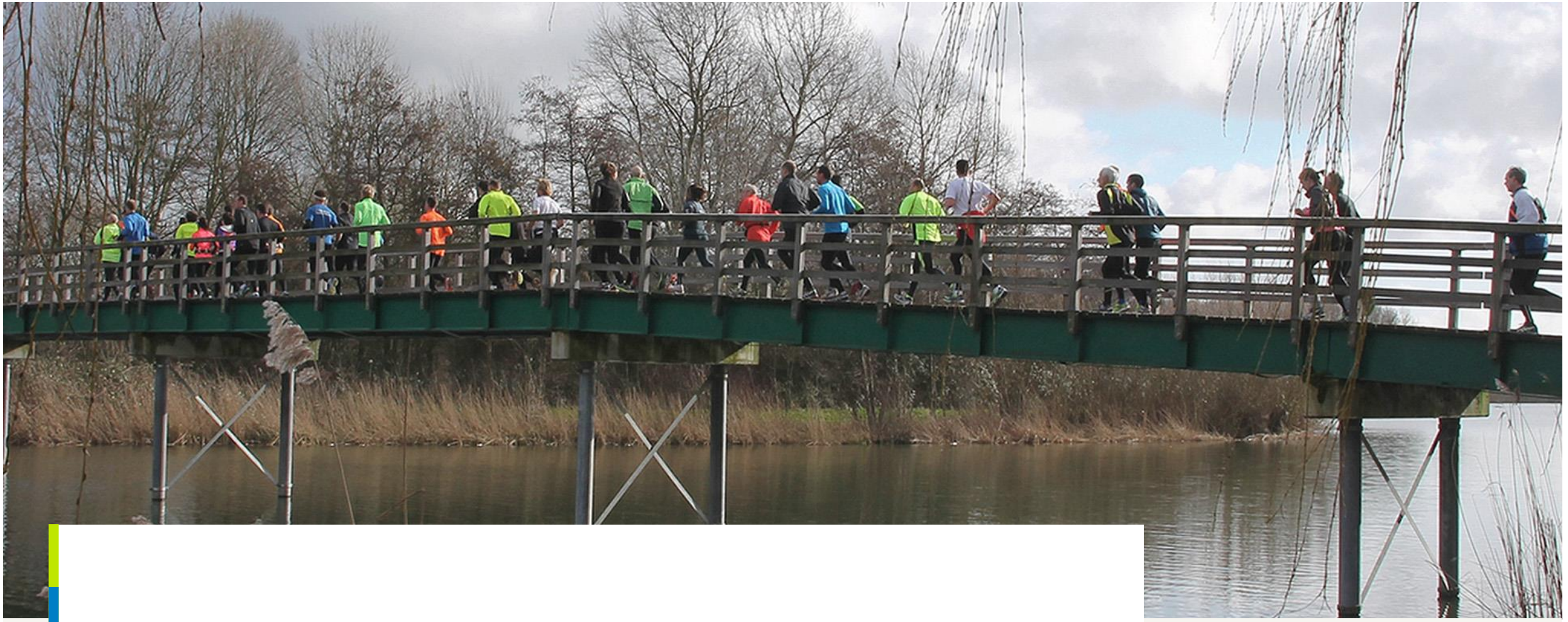
Trusselsbilledet set både inde fra og udefra, og hvorfor det er vigtigt at scanne for sårbarheder
Hvad kan der ske, hvis vi ikke gør noget ved vores sårbarheder?
Malware Information Sharing Platform (MISP) og hvad den giver sundhedssektoren af værdi

Cyber – fra DCIS

v/ Ole Fisker
Senior cyber security advisor i DCIS/SDS

SUNDHEDSDATA-
STYRELSEN



CIA og DCIS

SUNDHEDSDATA-
STYRELSEN

Det vi kikker ind i (trusselsbilledet) – Internt

Plan for sårbarhedsscanning og hvorfor vi skal være OBS på det

SUNDHEDSDATA-
STYRELSEN

Hvad gør vi, og hvorfor gør vi det? (Internt)

- Vi har lavet en service på SDN, som vi begynder at udbyde til dem, der vil brug det (sårbarhedsscanning)
- Rapporter om hvordan det ser ud fra SDN ang. sårbarheder på jeres services
- Hvorfor er det vigtigt?

Hvor mange sårbarheder tror I, der er hos jer?

Gør jeres leverandører det de skal, når vi snakker om, at de skal beskytte jeres infrastruktur/services?

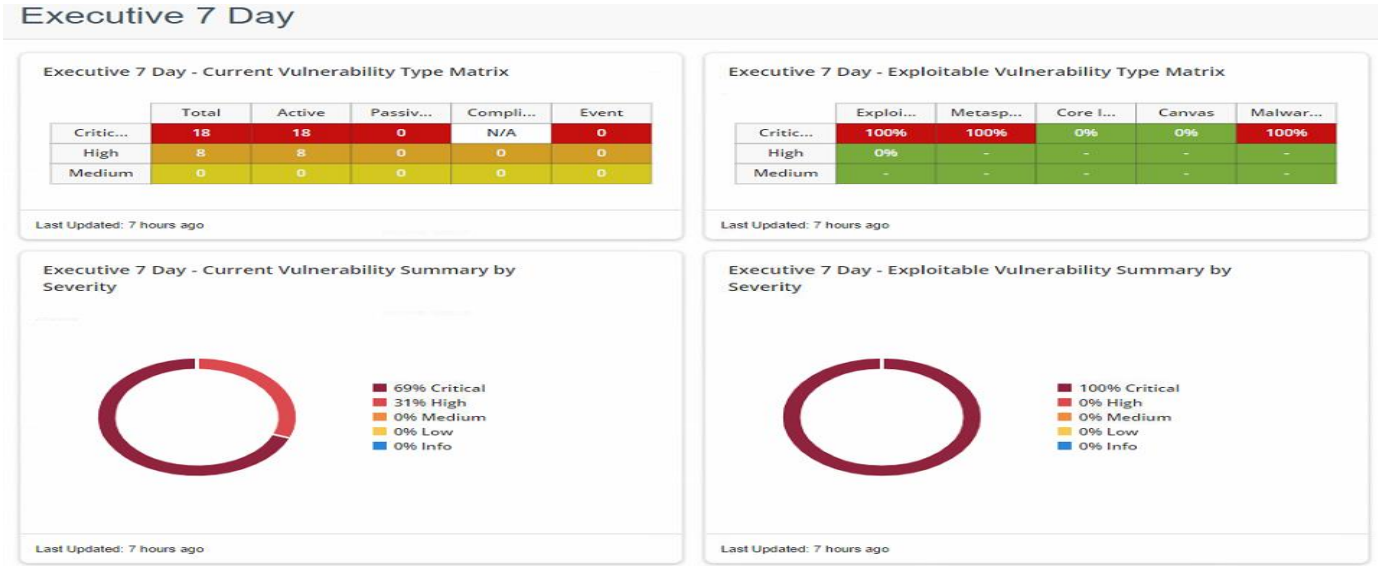
Hvad gør vi, og hvorfor gør vi det? (Internt)

- Lige nu bruger vi Tenable Sc. på SDN
- Vi er ved at lave en rammeaftale på et værktøj, så omkostningen kan komme ned
- Vi ønsker også at lave et samarbejde med de af jer, som vil være med til et fælles overblik over sårbarheder

Hvad er fordelen ved, at vi har det samme værktøj?

Hvad får vi ud af et fælles overblik ?

Sårbarheder



Sårbarheder

- Dette er ikke fra SDN (vi snakker kun om 40 server på denne rapport)

Apache Log4j Unsupported Version Detection	Misc.	Critical		28	28	
Apache Log4j 1.x Multiple Vulnerabilities	Misc.	Critical	9.0	28	28	
Microsoft Open Management Infrastructure < 1.6.8.1 Multiple Vulnerabilities	Web Servers	Critical	9.7	24	24	
Microsoft Open Management Infrastructure (OMI) package < 1.6.8-1 Multiple Vulnerabilities	Misc.	Critical	9.7	24	24	
Apache Log4j 2.x < 2.16.0 RCE	Misc.	Critical	10.0	10	10	
Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.0	9	9	

Hvad sker der, når vi ikke gør noget ?

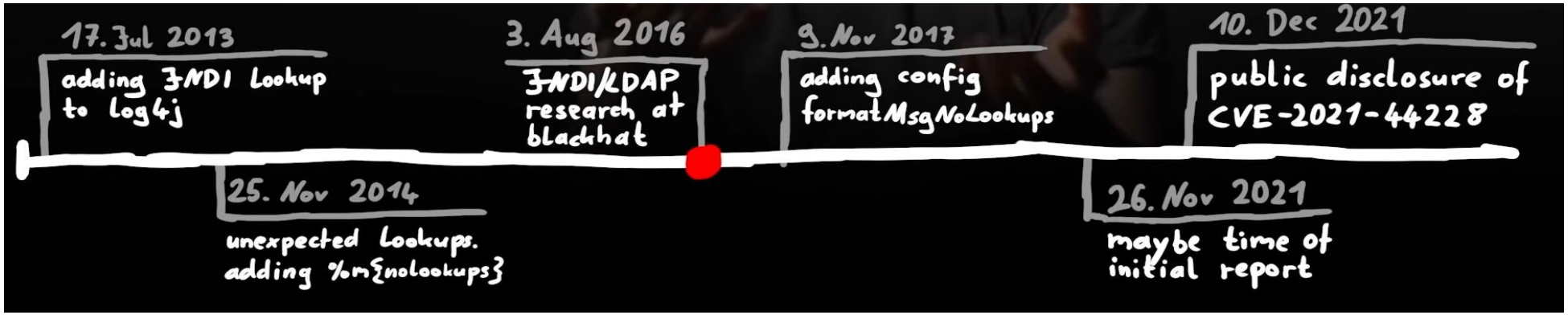
CVE-2021-44228

Log4J

- Sårbarheden har været der siden 2013

1. Demo
2. Demo

Log4J



Sårbarhed har været der siden 2013

Dette kunne bruges fra Office version 2013

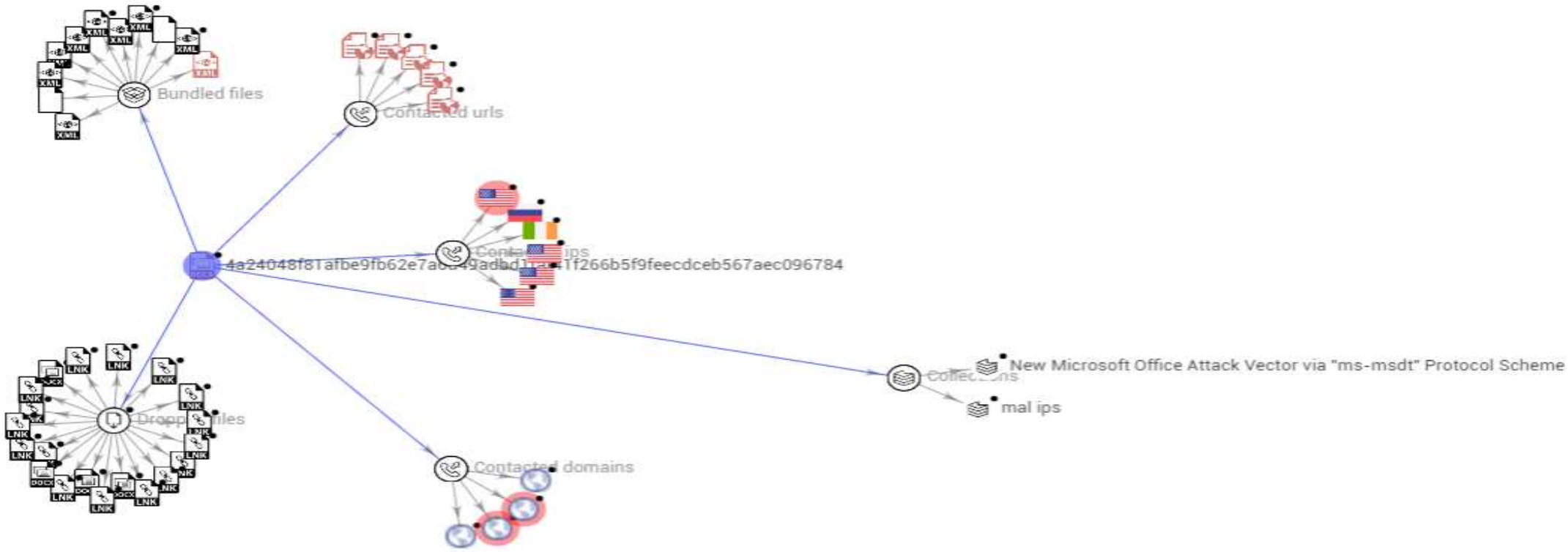
CVE 2021 40444

- Hvor længe har man kunne gøre dette?
- Der er kun en manuel fix på dette lige nu:

```
C:\>reg delete hkcr\ms-msdt /f
The operation completed successfully.
```

- Demo

Dette kunne bruges fra Office version 2013



SUNDHEDSDATA-
STYRELSEN

Det vi kikker ind i (trusselsbilledet) – Eksternt

Plan for Cycognito og hvorfor vi skal være OBS på det

SUNDHEDSDATA-
STYRELSEN

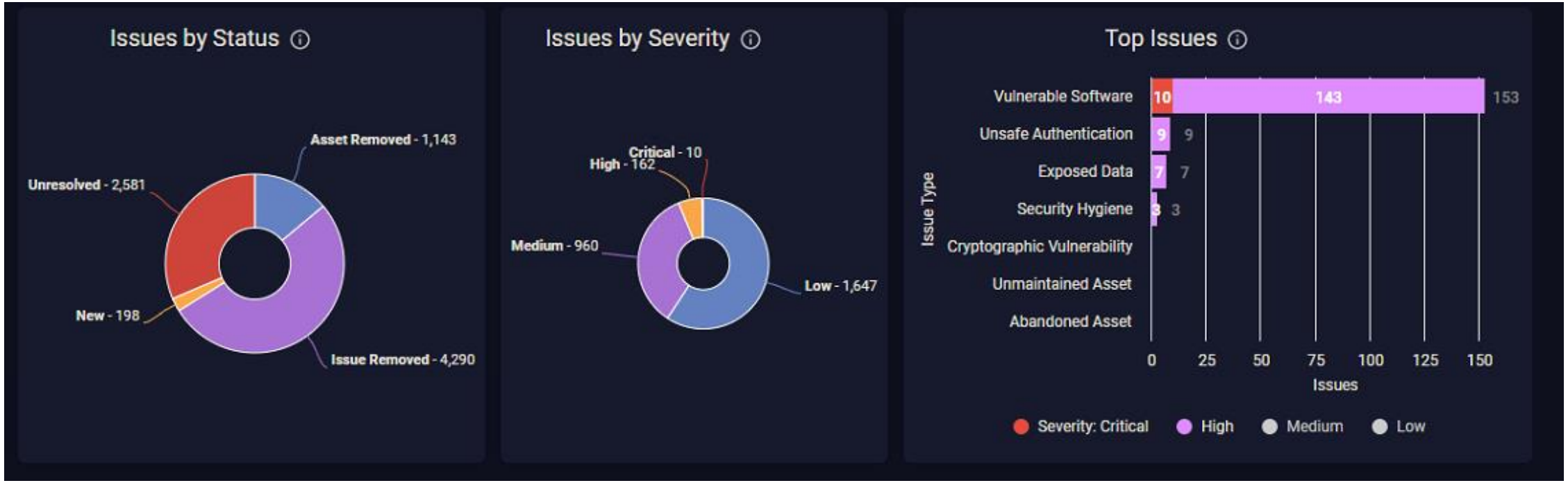
Det vi kikker ind i (trusselsbilledet) – Eksternt

- Vi har købt en service, som alle regioner har adgang til (sårbarhedsscanning eksternt fra)
  - Måske kommer flere aktører på
- Rapporter om hvordan det ser ud eksternt fra
- Hvorfor er det vigtigt?

Hvor mange sårbarheder tror I, der er hos jer?

Gør jeres leverandører det de skal, når vi snakker om, at de skal beskytte jeres infrastruktur/services?

Det vi kikker ind i (trusselsbilledet) – Eksternt



SUNDHEDSDATA-
STYRELSEN

Det vi kikker ind i (trusselsbilledet) – Eksternt

- Man har set på hvor mange sårbarheder, vi kender til lige nu

  Man gætter på, at man har kendskab til ca. 8 % af alle sårbarheder (i 2020)

- Rapport fra CyCognito

Det vi kikker ind i (trusselsbilledet) – Eksternt

- SQL Injection

SUNDHEDSDATA-
STYRELSEN

Det vi kikker ind i (trusselsbilledet) – Eksternt

- SQL Injection

select * FROM users Where name=’olef’ and password=’’ OR ‘1’=’1’

Det vi kikker ind i - MISP

Plan for MISP

SUNDHEDSDATA-
STYRELSEN

Det vi kikker ind i – MISP (hjælpeværktøj)

- Plan for Open Source Threat Intelligence and Sharing Platform og hvorfor vi skal bruge det
- Geo Block? Event i MISP
- IOC/IOB kan deles hurtigere
- Malware Sample og flere kan kikke på det samme på samme tid
- Vi kan dele hurtigt og nemt med alle, som er på MISPen

National

MISP Threat Sharing

International

norskhelsenett

H-ISAC HEALTH - ISAC

DCIS-SUND – Sundhedsdatastyrelsen

Triagering

Triagering

MISP Threat Sharing

TELEDCIS

SØFARTSSTYRELSEN

FINANSTILSYNET

”Ekstra par øjne oven på egen SOC”
”Giver tilbage til sektoren”
”Sektorsituationsoverblik”

SAC

Operativt samarbejde

SOC

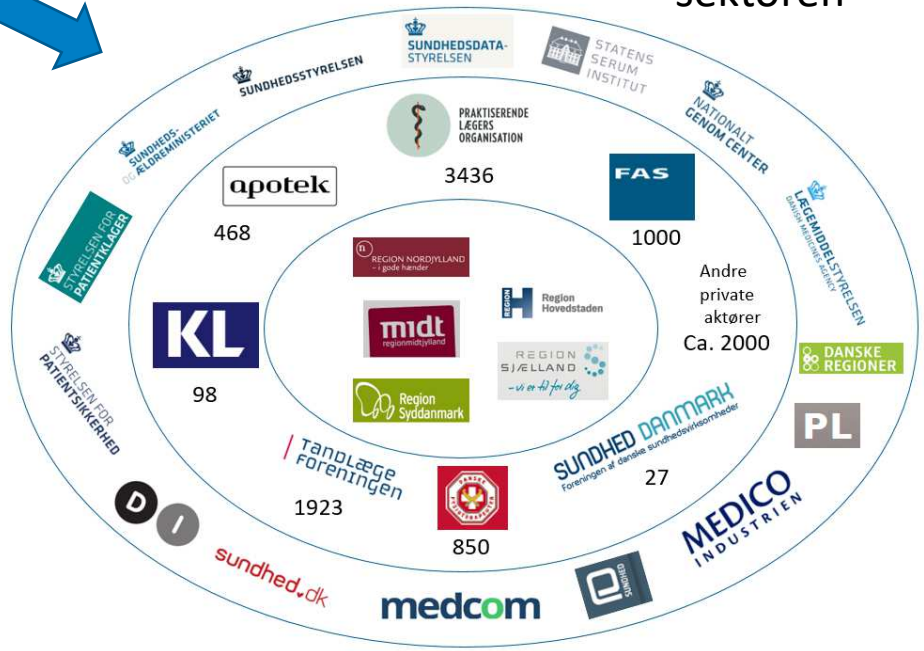
SOC

SOC

Impact	Urgency	Priority
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

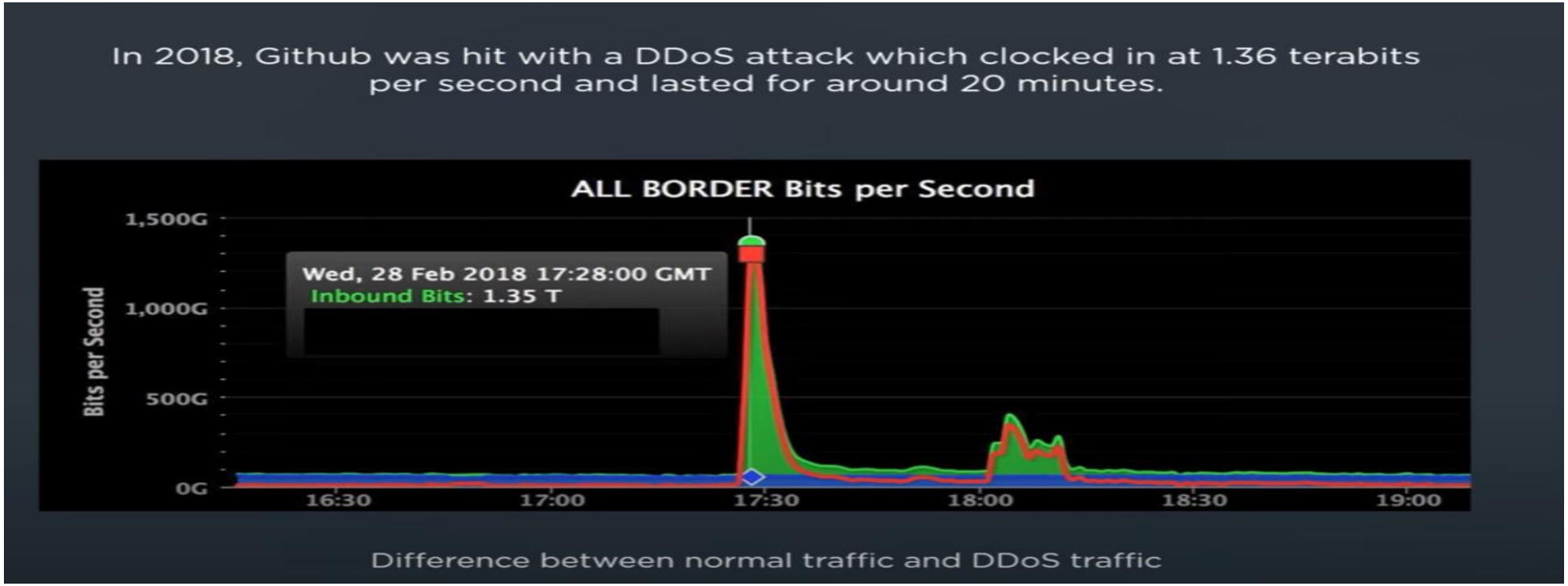
Mulighed for automatisk beskyttelse ud fra IOC’er og IOB”

Resten af sektoren



Det vi kikker ind i – MISP (hjælpeværktøj)

- Demo DDOS < hPing3 –s –flood –V –p 80 (ip adr vi ønsker at ramme) (syn flood) >
- Se script efter demo



SUNDHEDSDATA-STYRELSEN

QR og hvad man kan gøre

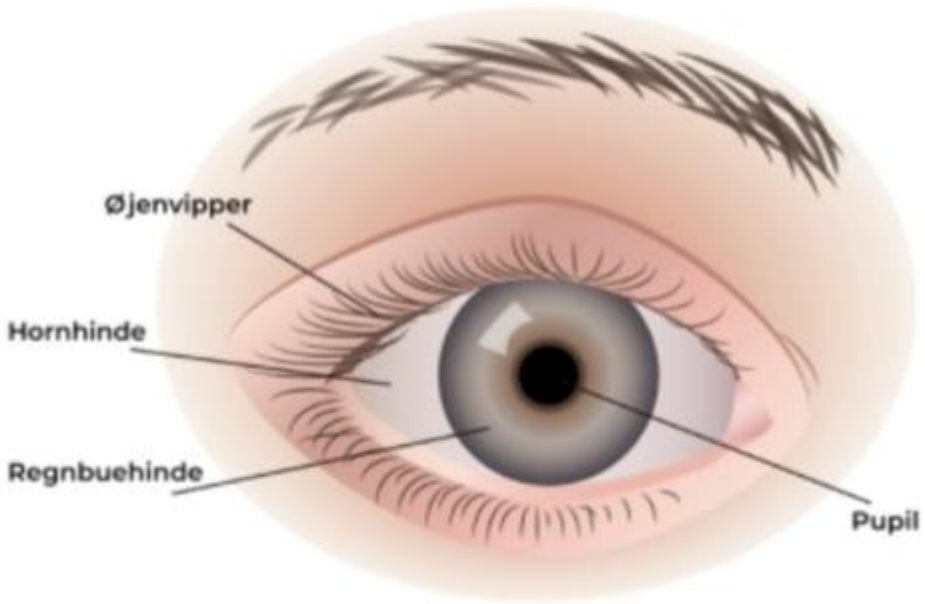
SUNDHEDSDATA-
STYRELSEN

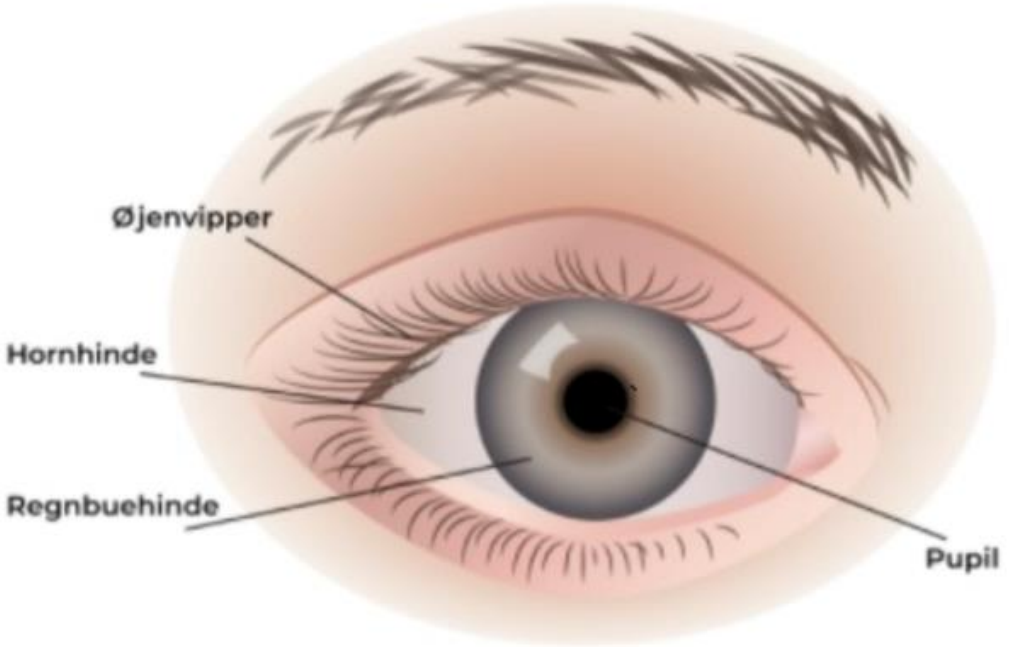
QR koder – links og alt det der

QR koder – links og alt det der

QR koder – links og alt det der

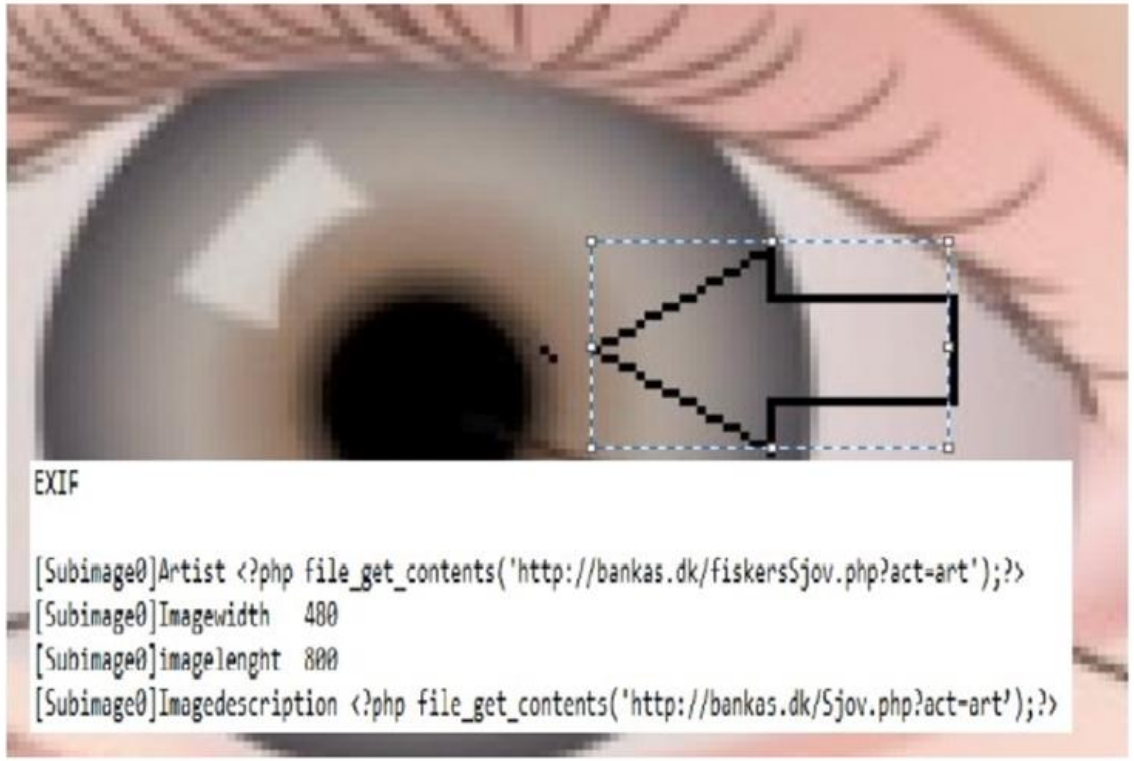
Til Demo af Qrcoder





QR koder – links og alt det der.

Til Demo af Qrcoder



Spørgsmål☺

SUNDHEDSDATA-
STYRELSEN

Ole Fisker

OLEF@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

Word Doc Oles og Tak for i dag

SUNDHEDSDATA-
STYRELSEN