energycluster.dk

Sammen om grøn innovation

Danmarks klyngeorganisation for den samlede energisektor



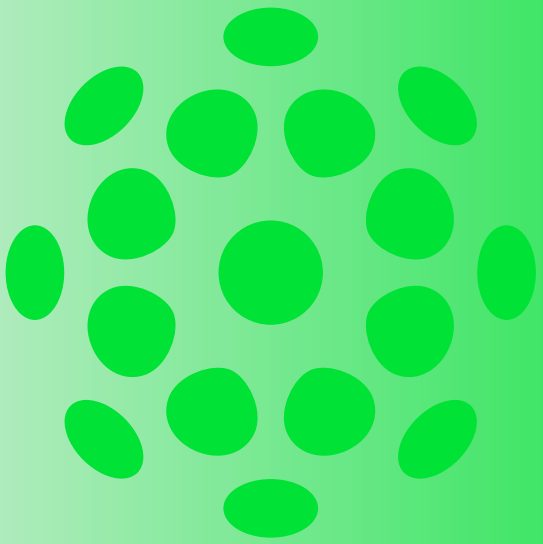
energy Cluster Denmark

Innovationsplatform for hele energisektoren

01 Vi skaber netværk mellem virksomheder, videninstitutioner og andre aktører i den danske energiklynge.

02 Vi accelerer udvikling, test og demonstration af nye grønne, sikre og globale energiløsninger.

03 Vi øger konkurrencekraften og innovation i de virksomheder, der engagerer sig i energiklyngen.



Energisystemet

01 Energiproduktion



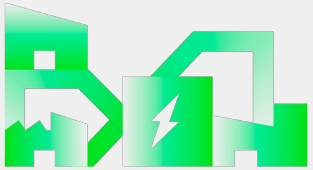
- Havvind
- Landvind
- Solenergi
- Biogas
- Geotermi
- Pyrolyse
- Biomasse
- Bølgeenergi
- Kraftvarme
- Olie og naturgas
- Anden energiproduktion

02 Energilagring



- El-lagring
- Gaslagring
- Termisk lagring
- Mekanisk lagring
- Anden energilagring

03 Energiinfrastruktur



- El-systemet
- Fjernvarmesystemet
- Gassystemet
- Anden energiinfrastruktur

04 Energieffektivitet



- Industri
- Bygninger
- Datacentre
- Anden energieffektivitet

05 Sektorkobling og CCUS



- CCUS
- Power-to-X
- Luftfart
- Godstransport
- Persontransport
- Maritim transport
- Landbrug
- Vandsektoren
- Anden sektorkobling

06 Digitalisering og sikkerhed



- Cyber- og fysisk sikkerhed
- Digital infrastruktur og fleksibilitet
- Smart Maintenance og Asset Management
- Dataudveksling og Data Spaces
- Anden digitalisering

Nøgletal

Antal medlemmer

500+

Mia. kr. i projektportefølje

3+

Små og mellemstore virksomheder

300+

Årlige events

100+

Mio. kr. fundraiset i 2025

600+

Billigere vedvarende energi

4%

Aktive innovationsprojekter

100+

Medarbejdere

40

Hvad tilbyder vi?

01 Innovation

- **Samarbejder mellem store, mellemstore og små virksomheder og forskere blandt vores 500+ medlemmer**
- **Projektfacilitering og projektledelse**
- **Projektudvikling fra A-Z. Vi finder de bedste partnere og finansiering til teknologiudvikling.**
- **Hjælp til samarbejdsaftaler, risikostyring, opfølgning på milepæle og meget mere.**

02 Administration

- **All-inclusive projektadministration. Medlemmerne bruger tid på det, de er bedst til.**
- **Vejledning om funding- og fundingregler samt dialog med fundinggiver.**
- **Hjælp til projektpraktik, fx afrapportering, timesedler, budgetopfølgning og udbetalinger.**
- **Kompetencer, viden og sparring indenfor fortolkning af statsstøtteregler.**

03 Netværk

- **Adgang til et bredt netværk og matchmaking med +500 virksomheder og videninstitutioner.**
- **Mulighed for innovations- og fagspecifikke netværksaktiviteter**
- **Gratis Årsmøde for alle medlemmer i hele energiklyngen**
- **Stå på ølkassen og/eller være vært**

04 Synlighed

- **Markant synlighed i energisektoren for medlemmer, der engagerer sig.**
- **Produktion af projektfilm og explainers til sociale medier.**
- **Pressemeddelelser i relevante medier, fx EnergiWatch og Børsen.**
- **Synlighed på LinkedIn med +20.000 følgere.**
- **Plads og taletid på konferencer og faglige events.**

Mit Energy Cluster

Dit digitale medlemsunivers

Vil du finde nye projektmuligheder – eller har du selv en idé,
du vil bringe i spil?

På Mit Energy Cluster kan du finde åbne calls og projektidéer,
søge relevante samarbejdspartnere og kompetencer og få feedback på egne projektforslag.

- Eksklusivt **for medlemmer af Energy Cluster Denmark**
- Fællesskab med +550 brugere fra energisektoren
- Tilgængelig på alle platforme mobil, tablet og computer

app.energycluster.dk

Mit Energy Cluster - mere værdi i dit medlemskab

Adgang til nye projekter

Få unik adgang til Energy Cluster Denmarks
pipeline af kommende innovationsprojekter
og kommende fundingcalls.

Din projektidé i spil

Del din projektidé med andre medlemmer og
få sparring med energiklyngens projektledere.

De rigtige samarbejdspartnere

Match med andre medlemmer, og få direkte
adgang til eksperternes kontaktinformationer.

Eksklusiv viden samlet ét sted

Publikationer, Slides fra keynotes, projektrapporter webinarer, skabeloner og meget mere.

Tak for i dag



Pernille Jensen
Membership Manager

+(45) 31 20 28 17

pej@energycluster.dk

www.energycluster.dk

https://www.linkedin.com/company/energyclusterdenmark/

Sammen om innovation – meld dig ind i dag!

Energy Cluster Denmark er innovationsplatform for den samlede danske energisektor.

Vores opgave er at sætte det stærkeste hold, så vi sammen fastholder og styrker Danmark som grøn frontløber for udvikling og demonstration af innovative energiløsninger.

Innovation og samarbejde er nøglen – og derfor har vi brug for jeres kompetencer til at nå Danmarks grønne mål.

Meld dig ind her:

What is now proved was once only imagined

EARLY BIRD (-20%)
Gælder indtil 31. december 2026

energy Cluster Denmark

ÅRSMØDE 2027

SAMMEN OM INNOVATION

19. og 20. maj 2027 | Aarhus Congress Center



AARHUS CONGRESS CENTER

Tilmeld dig allerede i dag
energycluster.dk

Virksomhedsudvikling Danmark


Cybertruslen for forsyning og kritiske infrastruktur

Agenda

01	Hvem er vi
02	Metode – hvad er en cybertrusselsvurdering
03	Cybertruslen mod kritisk infrastruktur og forsyning
04	Tendenser - Hybrid, AI, supplychain og kvante
05	-
06	-
07	-
08	-

Hvem er vi
(meget lidt om det)

Styrelsen for Samfundssikkerhed



Styrelsen for
Samfundssikkerhed

Trusselsvurderingsenheden

- Følger cybertruslen på et strategisk niveau
- Sætter trusselsniveauerne på nationalt niveau på cyberområdet
- Udgiver trusselsvurderinger på nationalt og sektorniveau

- Løbende dialog med tjenesterne for informationsdeling og koordinering



International cyber agencies share fresh advice to defend against China-linked covert networks

New advisory highlights how to defend against attacker tactics believed to be used by the majority of China-linked actors to hide malicious cyber activity.

National Cyber Security Centre · ASD ACSC · Canadian Centre for Cyber Security · BND · Bundesamt für Sicherheit in der Informationstechnik · 国家サイバー統括室

Novo Nordisk ramt af »sikkerhedshændelse

Genopbygger it-system

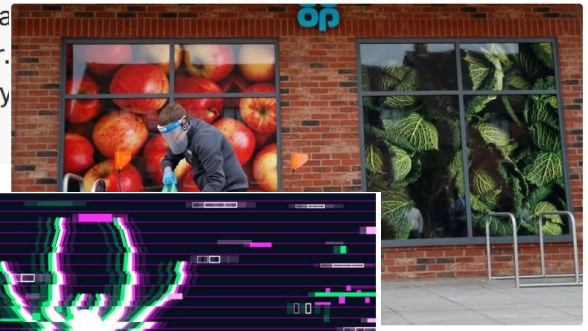
bunden

UK retailer Co-op restoring systems following major cyberattack

The company is carefully ramping up systems and is boosting deliveries to its 2,300 food stores after stock issues.

Published May 14, 2025

David Jones
Reporter



TRUSSELSVURDERING

Skærpet trussel fra destruktive cyberangreb

30-06-2026

Trusselsvurderingen skal informere organisationer og beslutningstagere i Danmark om en skærpet trussel fra destruktive cyberangreb, som udgår fra russiske statslige hackere. Viden om truslen er bl.a. relevant for beskyttelsen af digitale systemer i samfundsvigtige organisationer og den kritiske infrastruk

Trusselsvurderingen er udarbejdet af Styrelsen for Samfundssikkerhed me inddragelse af vurderinger fra Forsvarets Efterretningstjeneste.

Hovedvurdering

- SAMSIK vurderer, at der er en skærpet trussel for destruktive cyberangre Ruslands statslige hackere mod Danmark. Det gælder særligt wiper-angr cyberangreb, der manipulerer operationel teknologi (OT).
- SAMSIK vurderer nu, at det er muligt, at Danmark kan blive udsat for fors destruktive cyberangreb fra russiske statslige hackere, hvor hensigten er mere omfattende konsekvenser for samfundsvigtige funktioner end hidtil.
- Der er tale om en skærpelse af truslen inden for det gældende trusselsni MIDDEL.
- Truslen er skærpet, fordi Ruslands statslige hackergrupper sandsynligvis en øget risikovillighed i forhold til at udføre destruktive cyberangreb mod europæiske NATO-lande.
- Den skærpede trussel fra destruktive cyberangreb gælder på tværs af det danske samfund, herunder også organisationer med ansvar for kritisk infrastruktur.
- Pro-russiske hackergrupper, hvoraf nogle har forbindelse til den russiske udgør forsat en del af trusselsbilledet. SAMSIK vurderer dog, at disse ha tekniske kapaciteter er begrænsede sammenlignet med Ruslands statslig hackere.

Styrelsen for Samfundssikkerhed

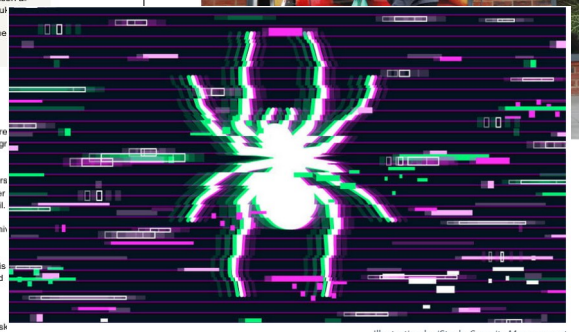


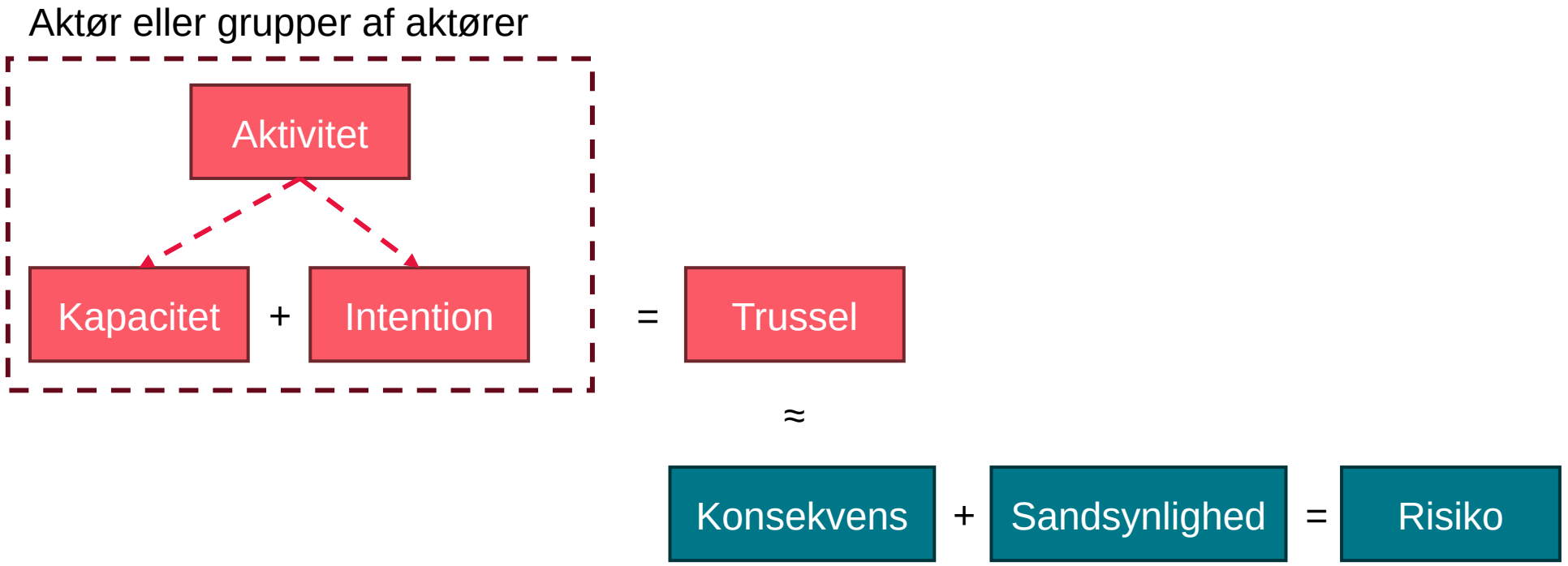
Illustration by iStock; *Security Management*

INFORMATION SECURITY · CYBERCRIME · CYBERSECURITY

Scattered Spider Cyber Criminals Turn to Insurance Companies as Next Targets

Metode – hvad er en cybertrusselsvurdering

Hvad er cybertrusselsvurderinger?



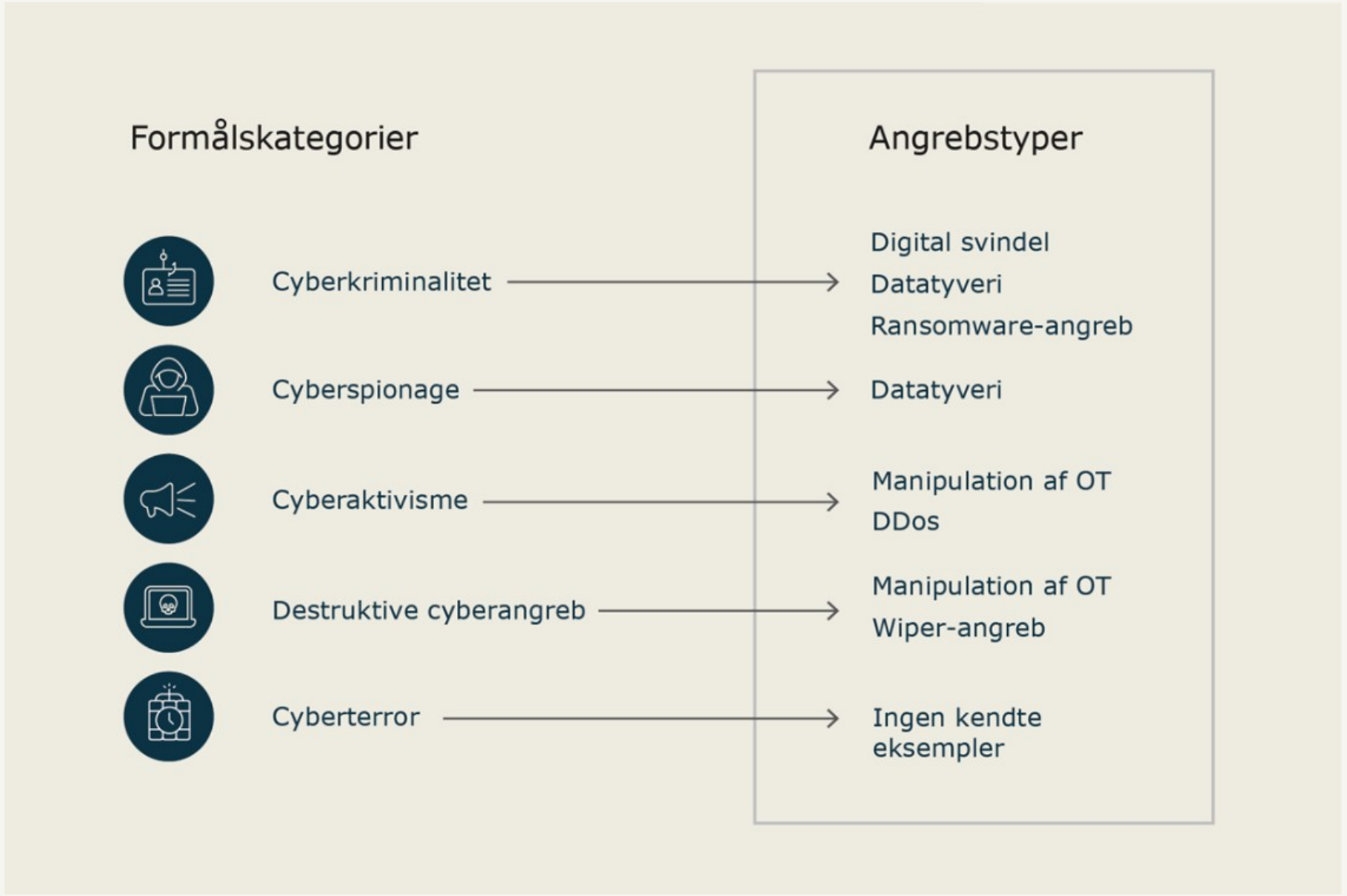
Et særligt sprog

INGEN	Der er ingen tegn på en trussel. Der er ingen aktør, der både har kapacitet til og intention om angreb/skadelig aktivitet.
LAV	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men enten er kapaciteten eller intentionen eller begge dele begrænset.
MIDDEL	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men der er ikke indikationer på specifik planlægning af angreb/skadelig aktivitet.
HØJ	En eller flere aktører har kapacitet til og foretager specifik planlægning af angreb/skadelig aktivitet, eller har allerede gennemført eller forsøgt angreb/skadelig aktivitet.
MEGET HØJ	Der er enten oplysninger om, at en eller flere aktører iværksætter angreb/skadelig aktivitet, herunder oplysninger om tid og mål, *eller* en eller flere aktører iværksætter kontinuerligt angreb/skadelig aktivitet.

Et givent trusselsniveau er udtryk for SAMSIKs vurdering af aktørers intention, kapacitet og aktivitet på baggrund af de tilgængelige oplysninger. Niveauerne svarer til Forsvarets Efterretningstjenestes (FE) trussels- og sandsynlighedsniveauer.

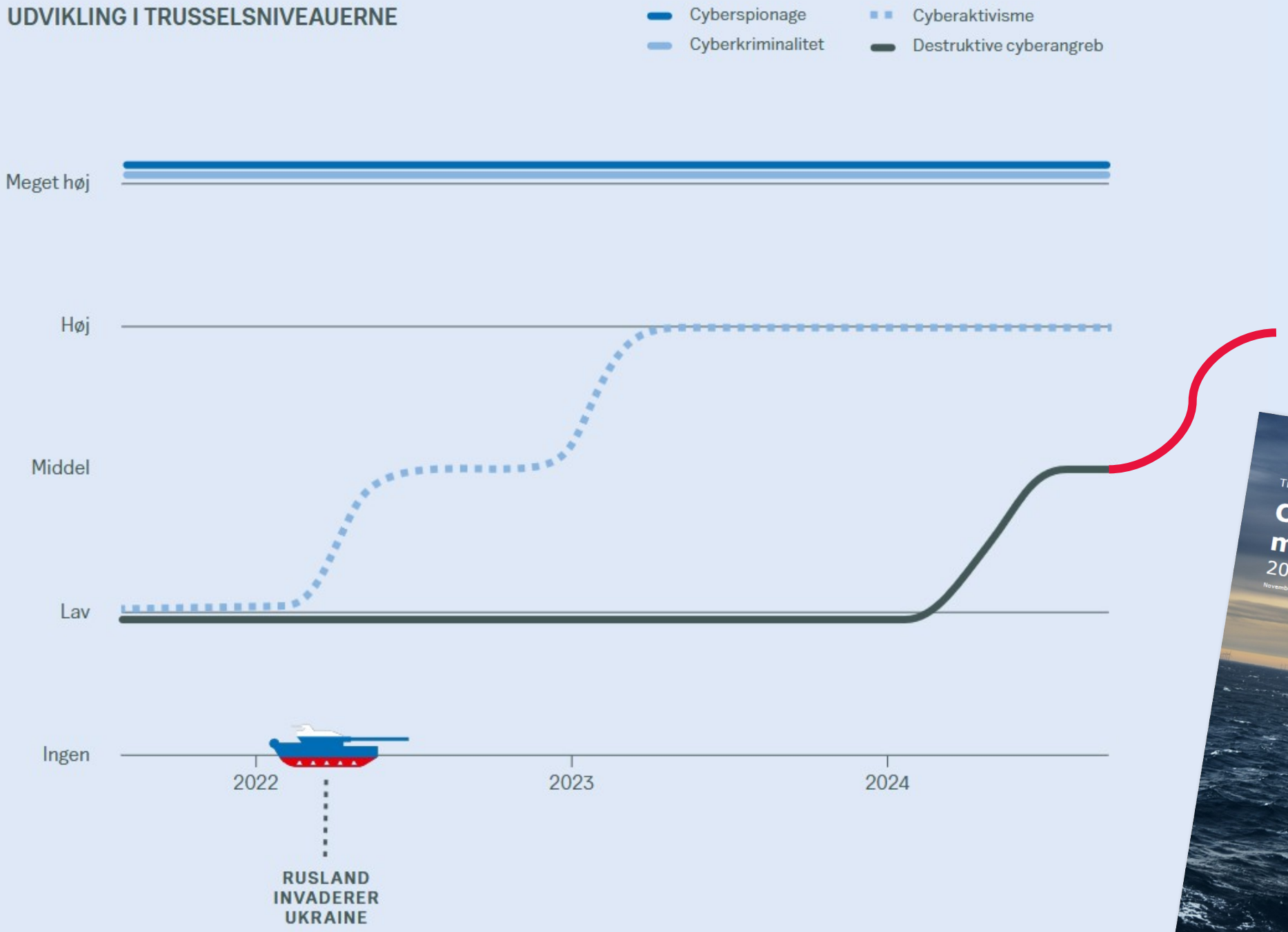
SAMSIK bruger denne skala for sandsynligheder i analyser:

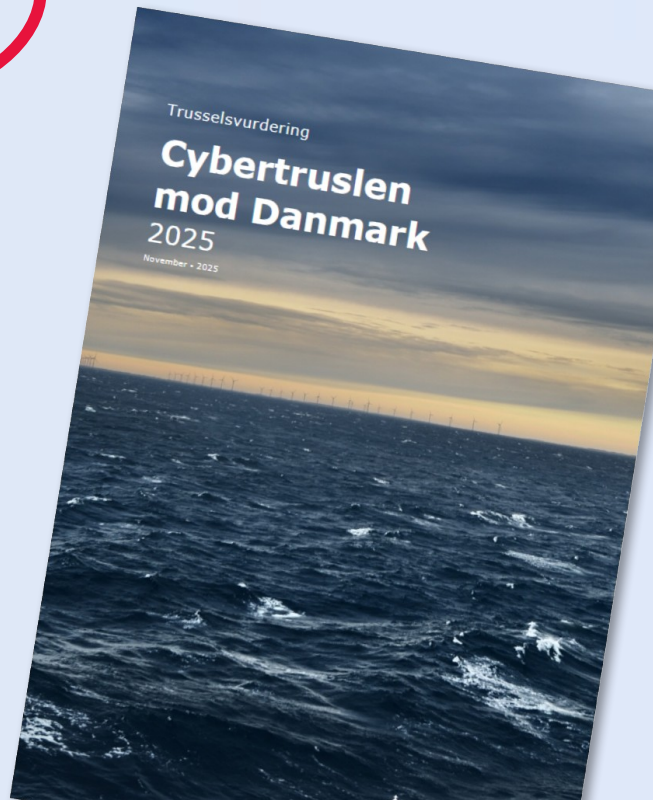



Formålskategorier
Angrebstyper
Cyberkriminalitet
Digital svindel
Datatyveri
Ransomware-angreb
Cyberspionage
Datatyveri
Cyberaktivisme
Manipulation af OT
DDos
Destruktive cyberangreb
Manipulation af OT
Wiper-angreb
Cyberterror
Ingen kendte eksempler

Cybertruslen mod kritisk infrastruktur og forsyning

UDVIKLING I TRUSSELSNIVEAUERNE





Udvikling i trusselsbilledet

- **Juni 2024:** trusselsniveauet for destruktive cyberangreb hæves fra LAV til MIDDEL
- **Juni 2026:** trusselsniveauet for destruktive cyberangreb skærpes inden for niveauet MIDDEL
- **September 2026:** trusselsniveauet for destruktive cyberangreb hæves fra MIDDEL til HØJ





Forsyningssektoren som mål

- Digital frontlinje i den hybride krig
- Organisationer der udgør rygraden i kritisk infrastruktur
- Symbolske mål hvor synligheden og effekten er betydelig ved nedetid
- Mål for både statslige og ikke-statslige hackere
- Fragmenteret landskab hvor nogle enheder har lavt beskyttelsesniveau



Uafhængige

Kriminelle

Pro-russiske

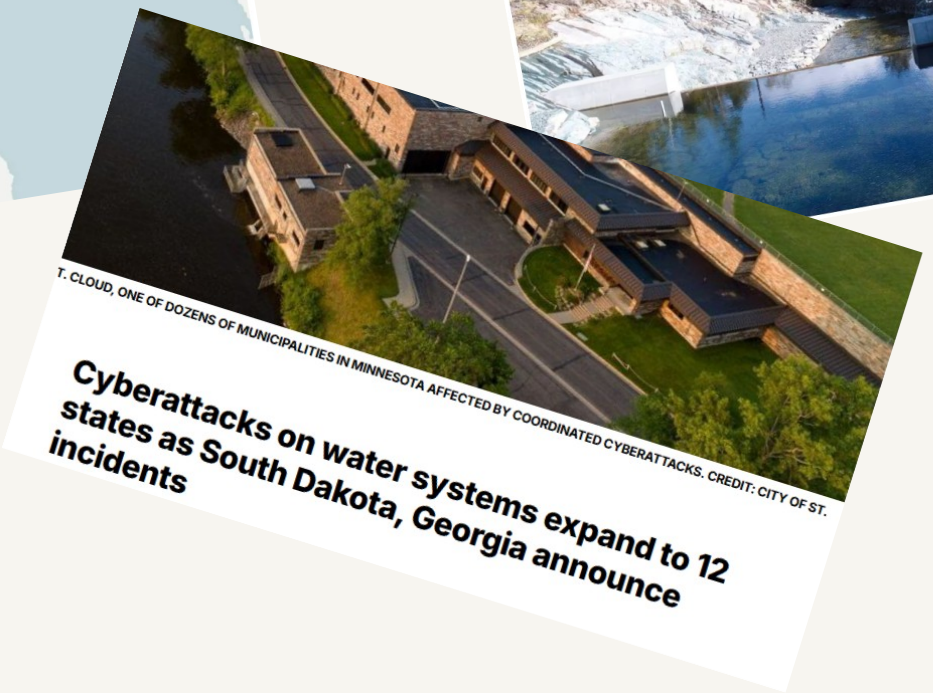
Statslige

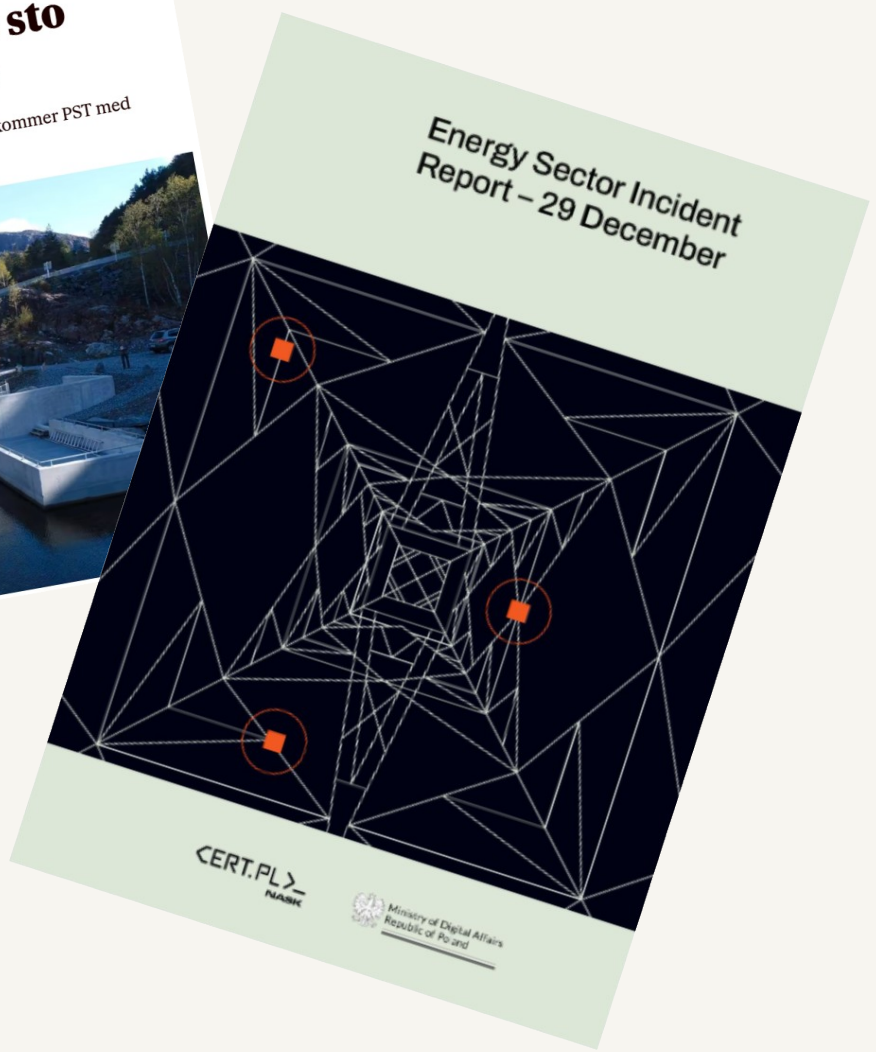


Eksempler på cyberangreb mod forsyningsområdet









Tendenser – Hybrid, AI, supplychain og kvante

Tendenser

Hybride trusler

- Formet af resterende konflikt / eskalations niveauer

Truslen fra AI

- Hastighed og kvantitet, kvalitet

Supplychain trusler

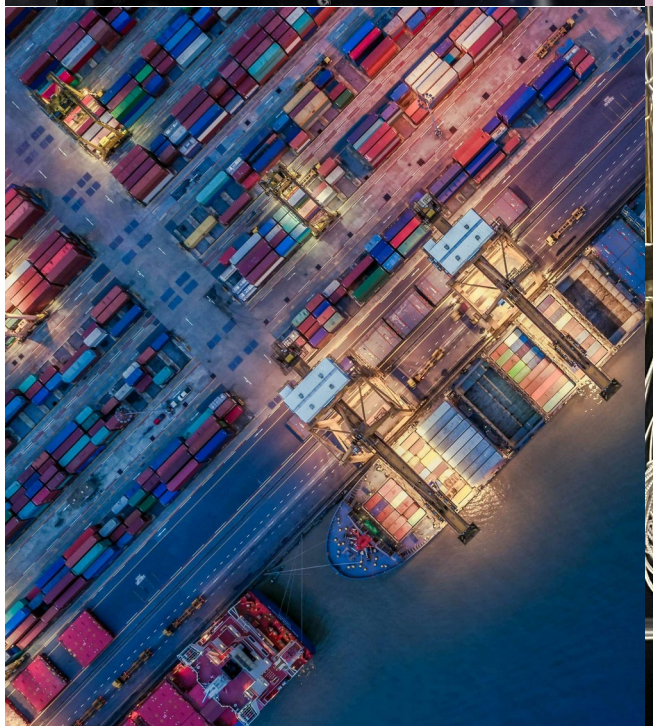
- Store afhængigheder af eksterne leverandører

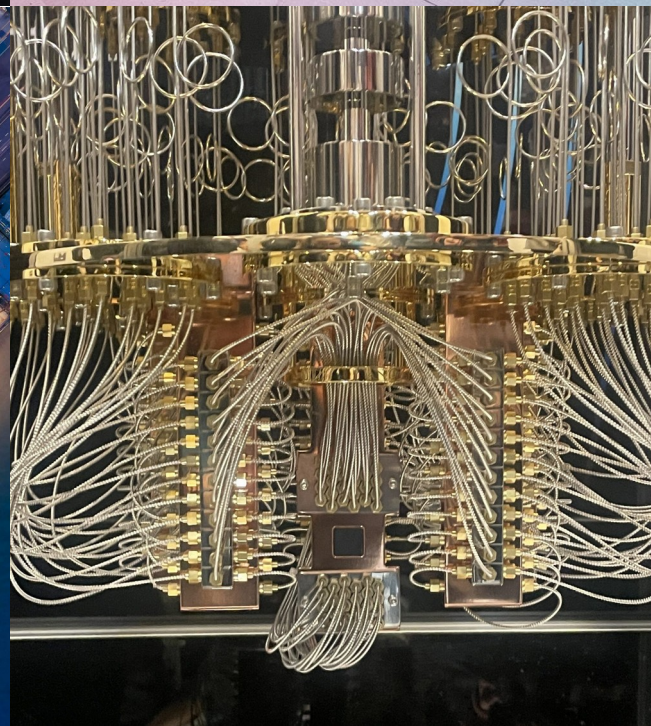
Truslen fra kvanteteknologi

- Indhent nu, dekrypter senere
- Forfalskede digitale signature









Styrelsen for Samfundssikkerhed

Rådgivning og vejledning

SAMSIK tilbyder en bred vifte af rådgivning, bl.a. til organisationer inden for kritiske infrastruktur. Vejledninger kan tilgås styrelsens hjemmeside – www.samsik.dk – og omfatter bl.a. følgende:

- **Cyberforsvar der virker**
- **Beskyt din organisation mod phishing-angreb**
- **Passwordsikkerhed**
- **Cybersikkerhed i leverandørforhold**
- **Reducér risikoen for ransomware**
- **Logning – en del af et godt cyberforsvar**
- **Sådan imødegås digital svindel**

SAMSIK's rådgivningskontor kan kontaktes på: raadgivning@samsik.dk

Spørgsmål

Samsik.dk

Styrelsen for samfundssikkerhed

Styrelsen for samfundssikkerhed

CRESCENDO

Cyber preparedness and resilience of the energy sector in the Nordic region

CRESCENDO

Et EU-finansieret samarbejde om cybersikkerhed i energisektoren

Katrine Storm og Felicia Broby

Energistyrelsen

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

NCC CYBERSECURITY NATIONAL COORDINATION CENTRE NORWAY

NCC CYBERSECURITY NATIONAL COORDINATION CENTRE FINLAND

NTNU Norwegian University of Science and Technology

NORWEGIAN NATIONAL SECURITY AUTHORITY

TRAFICOM Finnish Transport and Communications Agency

Danish Energy Agency

The Research Council of Norway

Nordisk samarbejde – hvorfor?

- Der findes ikke et dansk energisystem
- Det nordiske elnet hænger sammen på tværs af grænser - det giver stabilitet og fælles ressourcer
- Men sammenkobling betyder også delt sårbarhed - det stopper ikke ved landegrænsen.
- Derfor er Norden ikke kun sårbart sammen - vi kan også løse det sammen



CRESCENDO

Om Crescendo

Fokus: cybersikkerhedsudfordringer på tværs af IT/OT-systemer

Temaer: sikkerhedstest, risikovurdering, trusselsmodellering.

Hvor er vi nu?

- 1. ansøgningsrunde (2025): ca. 1 mio. EUR fordelt på 10 projekter
- 2. ansøgningsrunde (2027): ca. 3 mio. EUR fordelt på min. 30 projekter
- Op til 200.000 EUR pr. projekt, 50% selvfinansiering påkrævet
- Konsortium på min. 2 virksomheder (1 energivirksomhed, 1 cybervirksomhed) - ejerskab indenfor EU/EEA
- Maks. 6 måneders projektperiode



Fokusområder i Crescendo

- **Risikovurdering**
- Hvordan vurderer vi konsekvenserne af cyberhændelser for elnettet?
- Hvilke modenhedsmodeller kan hjælpe organisationer med at måle deres beredskab?
- Hvordan kan vi tilpasse risikotilgange til både IT og OT?

- **Sikkerhedstest**
- Kan man skabe sikre måder at teste OT eller industrielle kontrolsystemer?
- Hvilke simuleringsværktøjer eller digitale tvillinger kan hjælpe os med at forstå cyber-fysiske trusler bedre?

- **Trusselsmodellering**
- Hvordan kan vi modellere hybride risici, der spreder sig mellem digitale og fysiske systemer?
- Hvordan håndterer vi menneskelige fejl og insidertrusler?
- Kan jeres værktøjer tilpasse sig nye sårbarheder og systemer?

De bedste projekter svarer ikke kun på disse spørgsmål – de leverer konkrete metoder, som sektoren kan tage i brug med det samme.

EKSEMPLER FRA RUNDE 1

Projekter der styrker norden

Defend Iceland (Island)

Etiske hackere tester islandske elproducenters systemer for sårbarheder uden at forstyrre driften. Allerede udvidet til Danmark.

Defendable / PORTRES (Norge)

Cybersikring af IT/OT systemer bag strøm og ladning i norske havne. Risikovurdering, trusselsmodellering og penetrationstest.

NC-Spectrum / Himinborg (Norge)

Nordisk koncept for OT-overvågning og respons for driftssystemer i elforsyningen. Security Operations Centres, koncept der kan kopieres af flere i sektoren.

Forbered jer til 2. ansøgningsrunde

Vi vil styrke cybersikkerheden i den nordiske energisektor gennem samarbejde og innovation på tværs af landegrænser



Cross-border af natur

Tip: Selv én partner fra et andet nordisk land styrker jeres ansøgning.

Bredt favnende

Tip: Fravælg jer ikke selv - er I i tvivl, så søg.

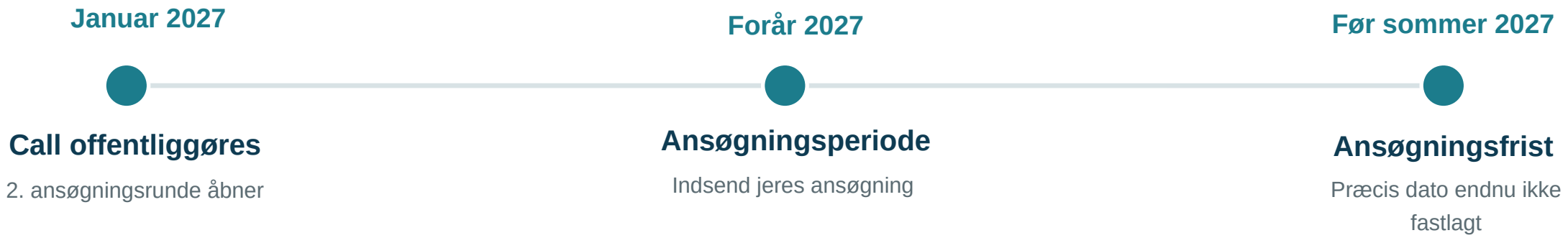
Samfundsværdi først

Tip: Vær konkret om, hvem der får gavn af det - ud over jer selv.

Ambitionen er bredere end det enkelte projekt: *resultater og metoder kan bruges af flere virksomheder i sektoren - ikke kun dem, der er testet.*

(Højest vægtede evalueringskriterium (Impact, 40%), når projekterne udvælges)

Tidslinje og netværksevent i København



Netværksevent i København d. 25. november.

- Mød fagfolk fra energisektoren og cybersikkerhedsbranchen
- Hør fra projekter, få ansøgningstips
- Relevante oplægsholdere om aktuelle cybertrusler specifikt i energisektoren

Contact@project-crescendo.eu
www.project-crescendo.eu

CRESCENDO


BIFROST connect
WHERE VPNS END, BIFROST CONNECT.
BIFROST
BIFROST
connect
REMOTE ACCESS AS IT SHOULD BE

Hvem

Made in Denmark
Hardware and Software
designed, coded, assembled in Denmark

Founded 2018

Built from real IT / OT support challenges

Portable and Battery Powered

Ideal for contingency / disaster recovery

No Cloud Data

Production data stays outside of any cloud

The tool to reach offline equipment

Bridging the gap between IT and OT





WHERE VPNS END

BIFROST connect

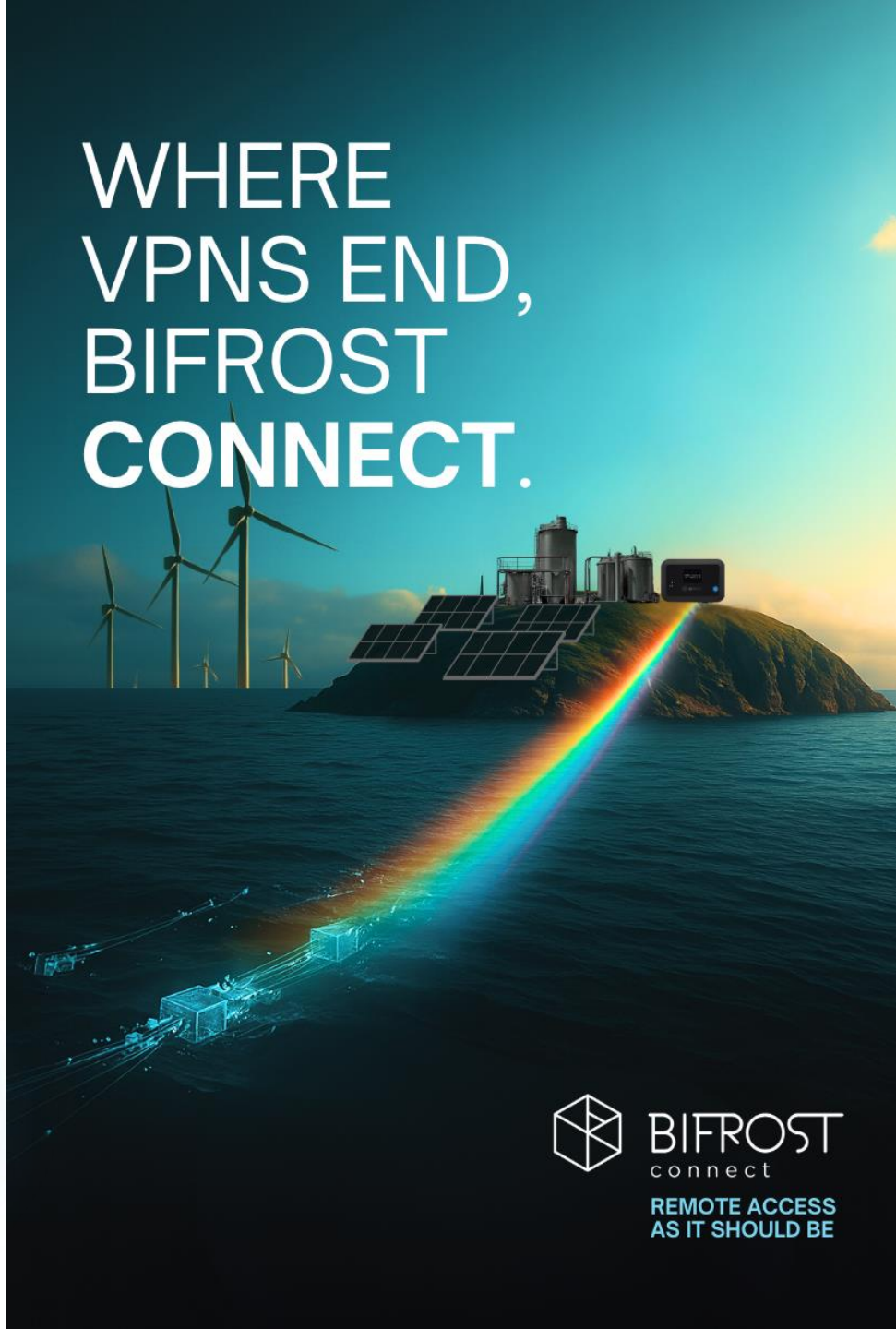
"Secure Remote Access" for mission critical IT / OT infrastructure.

Hvorfor

Fordi Verden er mere usikker og kravene til Cybersecurity stiger

- Kommissionering, Incident Response, 3rd Party Access
  - Men de kvalificerede personer er langt væk!
  - E.g. Beredskab / Ø-drift er påkrav – men hvordan?
- Netværk er isolerede eller offline
- Firewalls lukket, ingen OS eller permanent forbindelse
- Leverandører skal hurtigt ind, men sikkerhed og compliance må ikke kompromitteres





Hvor

















Hvad

Zero Trust-arkitektur til sikret intern og ekstern fjernadgang

- ✓Midlertidig adgang med lokal adgangsstyring og global kontrol
- ✓Zero Trust-alternativ til uofficielle work-arounds
- ✓Ingen efterladte forbindelser eller glemte åbne sessioner

Incident Response & Beredskab

- ✓Total isolation under hændelser (ø-drift) – kun godkendt tunnel til specifik enhed
- ✓4G-out-of-band adgang sikrer fjernsupport ved netværksnedbrud
- ✓Direkte adgang uden eksponering til internettet
- ✓Hurtigere fejlhåndtering end fysisk tilkald
- ✓Backup-løsning til kritisk udstyr, når primære værktøjer ikke slår til

Central styring & compliance

- ✓Én portal til opsætning, styring og adgangsrettigheder
- ✓Least-privilege og detaljeret audit trail
- ✓Globalt overblik, lokal kontrol og understøttelse af NIS2



MISSION:

Den foretrukne Ad Hoc løsning for tredje parts fjernadgang til IT og OT miljøer; navnlig indenfor kritisk infrastruktur”

NCC projekt

SECURE TRANSPORT AND NATIVE ENDPOINT CONTROL



Direct Native Access

"The World's Longest Virtual Arms"

KVM, serial terminal and SSH through one Bifrost Unit, down to pre-OS and BIOS level. The technician's computer never joins the OT network.



Direct Tunnel Access

"The World's Longest Cable"

An identity-bound IP tunnel from the installed app. Subnet mapping gives scoped access to multiple endpoints, for one or several technicians.



Clientless Tunnel Access

"The easiest way to give secure IP tunnel access"

Designed to give the technician's own software IP connections to the systems behind one Bifrost Unit, each scoped to IP address and port, with nothing to install.



Virtual Serial Access

SESSION GOVERNANCE: OPERATOR SIDE AND ST



SessionGuard

Designed to force a live stream of the technician's screen and keystrokes to recording the customer owns, in the browser and the app. The technician must accept it, and if the stream stops, so does the session.



SESSION GOVERNANCE: OPERATOR SIDE AND



SessionGuard

Designed to force a live stream of the technician's screen and keystrokes to recording the customer owns, in the browser and the app. The technician must accept it, and if the stream stops, so does the session.

SECURITY BY DESIGN

NETWORK

- Outbound only on port 443
- No open ports, no inbound traffic
- No lingering sessions
- Ethernet, WiFi, 4G/LTE or Starlink

ACCESS AND DATA

- Per-session MFA, per-person login
- End-to-end encrypted sessions
- We cannot decrypt: relays forward ciphertext only
- Immutable audit log: who, what, when

HARDWARE

- Hardened Linux, signed firmware
- No debug ports, revocable device keys
- 249 g, up to 2 hours in session on battery
- Attended unit: the session is approved on site

WHERE VPNS END

BIFROST connect


BIFROST
connect
WHERE
VPNS END,
BIFROST
CONNECT.
BIFROST
Kasper Holst Wochner
KHW@bifrostconnect.com
+4528732547
BIFROST
connect
REMOTE ACCESS
AS IT SHOULD BE

FORTIS

NCC-DK

FEDERATED ON-PREM TRUSTED INFRASTRUCTURE SYSTEM

Claus Amtrup Andersen
caa@cybercube.dk

Co-funded by the European Union

CyberCube HOSTING

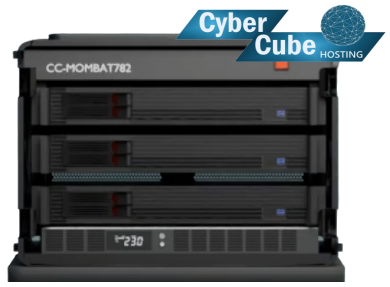
Hvordan er CyberCube blevet til?

2021 Energistyrelsens cyber- og informationssikkerhedsstrategi for el-, gas- og fjernvarmesektoren

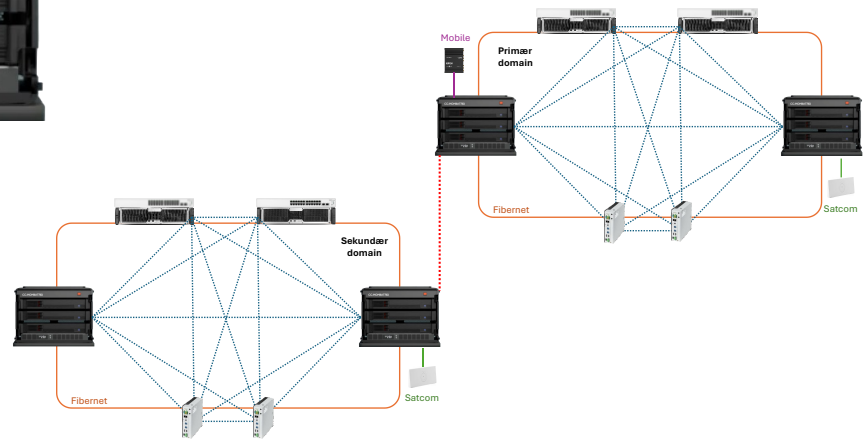
2023 EURISCO interne IT-hosting skulle sikres og vi opsatte derfor bla. følgende krav:

Offline-kapacitet i en online verden: IT systemer i Ø-drift

- UPS (15 min) og lille generator til nøddrift, minimalt effektforbrug
- Automatisk fail-over fra fiber til mobil og Starlink på MESH VPN netværk
- Kun mobile on-prem systemer (ikke mere cloud)
- Ingen vendor-lockin, kun open-source sw produkter
- Proxmox VE clustering, HA firewall, backup/recovery, 24/7 overvågning…



FEDERATED ON-PREM TRUSTED INFRASTRUCTURE SYSTEM



1994 … 202X

EURISCO arbejder med kritisk infrastruktur for energiselskaber

EURISCO RESEARCH & DEVELOPMENT

2025

EURISCO bygger en PoC for CyberCube

Og får tildelt Innoboost støtte til CyberCube MVP færdigudvikling

2026

CyberCube ApS etableres

Første kunde

Første system i drift

Cyber Cube HOSTING

NCC-DK støtter CyberCube FORTIS videreudvikling

Hvad er FORTIS? Og hvad skal det løse af problemstillinger?

FORTIS er et NCC-DK støttet projekt, som har til formål at styrke cybersikkerheden i kritiske sektorer

Gældende lovgivning
BEK260, CRA…
skal styrkes med
praktiske eksempler

'10-punktsplan'

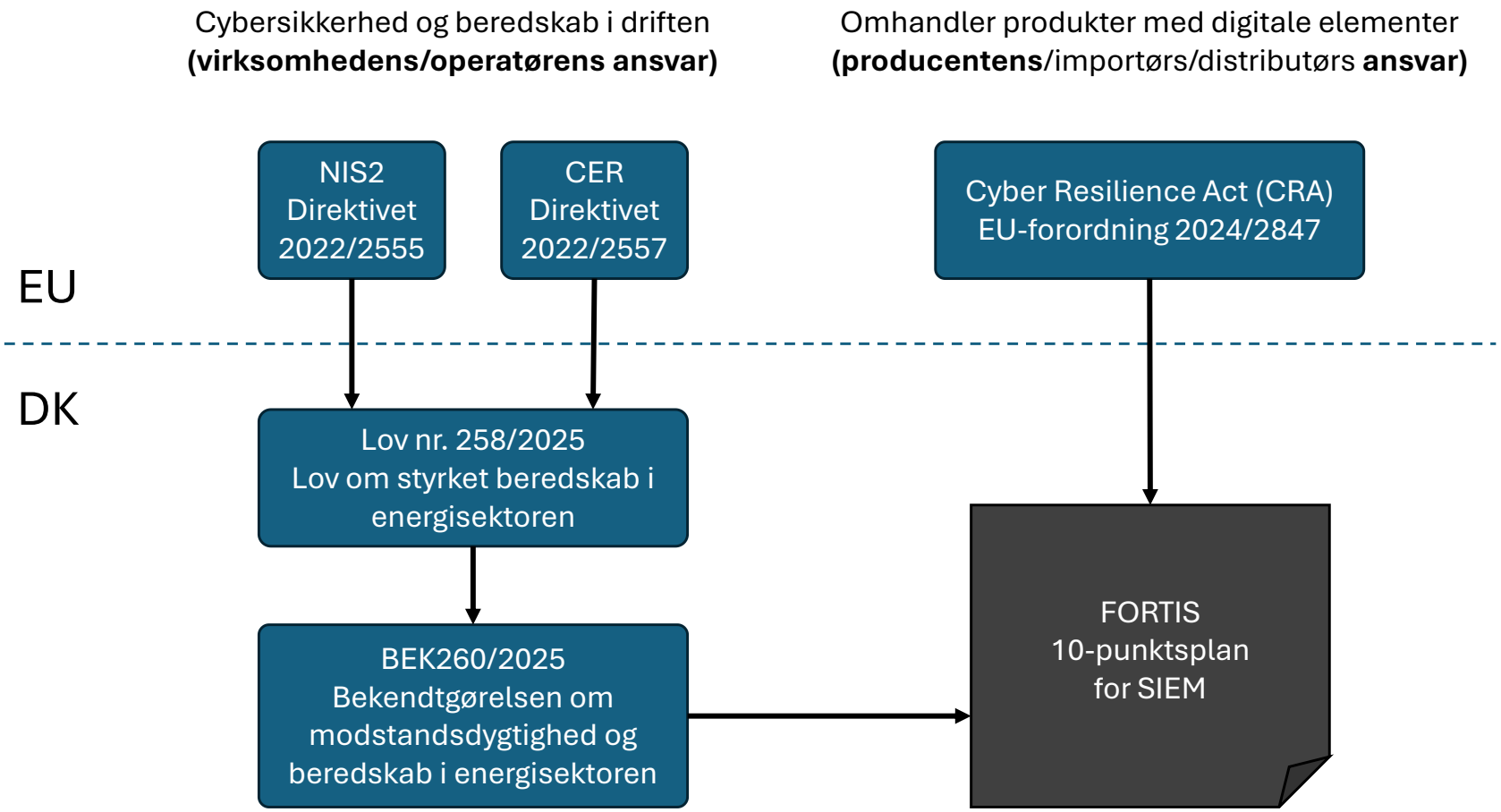
FORTIS

FEDERATED **O**N-P**R**EM **T**RUSTED
INFRASTRUCTURE **S**YSTEM

Styrke dansk suverænitet
indenfor kritiske sektorer
gennem brugen af
open-source produkter

Udvikle et koncept for on-prem
federering, som supplement til
cloud-løsninger

10-punkts plan for BEK260/CRA



Co-funded by
the European Union

CyberCube HOSTING

DRAFT

10-punkts plan for BEK260/CRA

1 Central logopsamling, korrelation og logintegritet

Systematisk opsamling fra alle pligtige kilder · korrelation på tværs af lokationer og forsyningsarter · tidssynkronisering af alle kilder · lagring adskilt fra kildesystemet og sikret mod manipulation · 13 måneders retention · dokumenteret geografisk placering af lagring.

2 Detektion, alarmering og eskalering i realtid

Detektionsregler på perimeter, interne segmenter og OT-grænseflader · klassificering af alarmniveau · definerede tærskelværdier der automatisk udløser alarm · alarm til navngiven modtager døgnet rundt med kvitteringskrav · eskaleringstrin koblet til beredskabsplanens kriterier for krisestab

3 Bevissikring, logudlevering og myndighedsrapportering

Bevissikret, tidsstemplet logmateriale med dokumenteret chain of custody · struktureret eksport til it-sikkerhedstjeneste inden for 24 timer · understøttelse af underretningsforløbet 24 t / 72 t / 1 måned · skabeloner med de indholdskrav, myndighederne stiller · sporing af hvilke frister der løber på en åben hændelse.

4 Identitets-, adgangs- og audit trail-overvågning

Uforanderligt spor pr. handling: bruger-ID, kildeadresse, tidsstempel, objekt og resultat · rettighedstildeling, -ændring og -fjernelse · privilegeret brug og servicekonti · inaktive konti · MFA-status og -omgåelse · fysiske adgange fra anlæggets adgangskontrolsystem · fjernadgange.

5 Asset Management, SBOM

Automatisk opdaget beholdning af servere, databaser, netværksudstyr, endpoints, virtuelle maskiner og software · kobling til kritikalitet, ansvarsplacering og afhængigheder

6 Konfigurations-, ændrings- og segmenteringsovervågning

Baseline pr. systemtype · detektion af afvigelse fra baseline · logning af hvem der ændrede hvad hvornår · kobling til godkendt ændringsanmodning · overvågning af segmenteringsudstyr og zoneovergange · detektion af nye eller uautoriserede hardwareaktiver på netværket.

7 Sårbarheds- (CVE) og patchmanagement

Kobling mellem aktivfortegnelse og sårbarhedsfeeds · elektronisk modtagelse af varsler · risikovurdering af egen eksponering pr. varsel · patchniveau pr. aktiv og afvigelse fra baseline · aktiver uden support (end-of-life) · måling af tid fra patch-frigivelse til installation · beslutningslog for sårbarheder, der bevidst ikke udbedres.

8 Backup og restore, beredskabsøvelser.

Overvågning af backupjob, backupintegritet og forsøg på sletning eller kryptering af backup · overvågning af redundans og alternative driftsformer. Periodisk verificering af genskabelse til baseline.

9 Intrusion detection and threat handling (CRA)

Kravene til selve produktet, beskyttelse af egne logdata mod manipulation · egen adgangskontrol og egen audit trail · nulstilling til oprindelig tilstand · begrænset angrebsflade · modstandsdygtighed mod DoS · sikker sletning af data.

10 Sikker og redundant kommunikation (CRA)

Anvende sikret tale-, video- og tekstkommunikation · alternative kommunikationsformer under håndteringen af en hændelse · Politikker og procedurer for kryptografi

Co-funded by the European Union

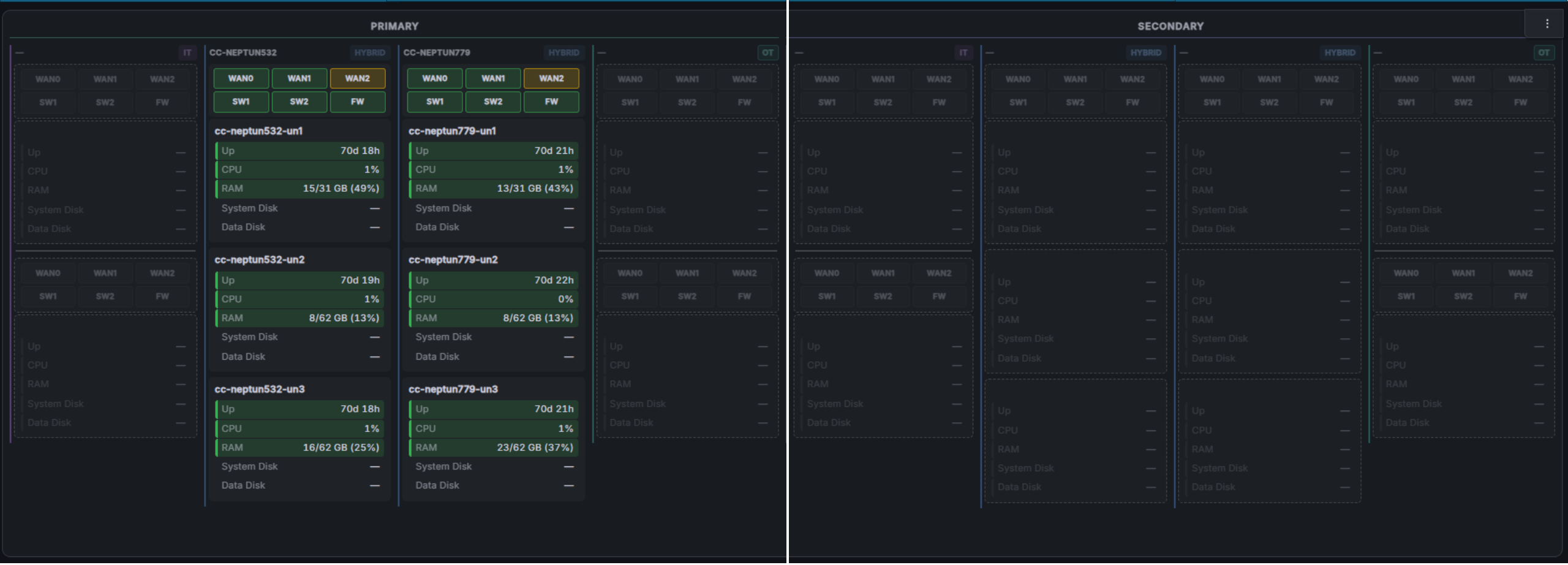
CyberCube HOSTING

DRAFT

10-punkts plan for BEK260/CRA

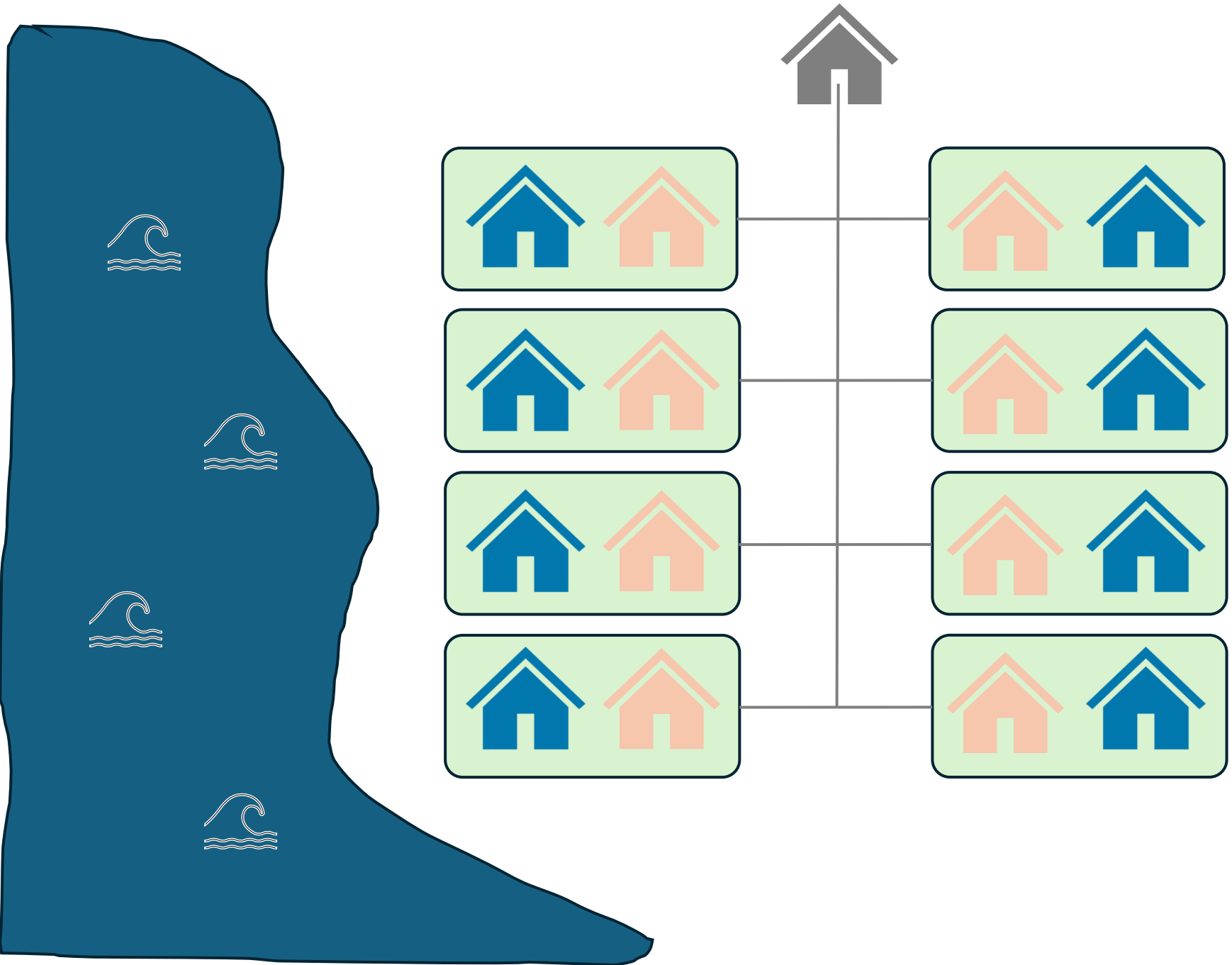
1	6
2	7
3	8
4	9
5	10

1	6
2	7
3	8
4	9
5	10



Co-funded by the European Union

CyberCube HOSTING



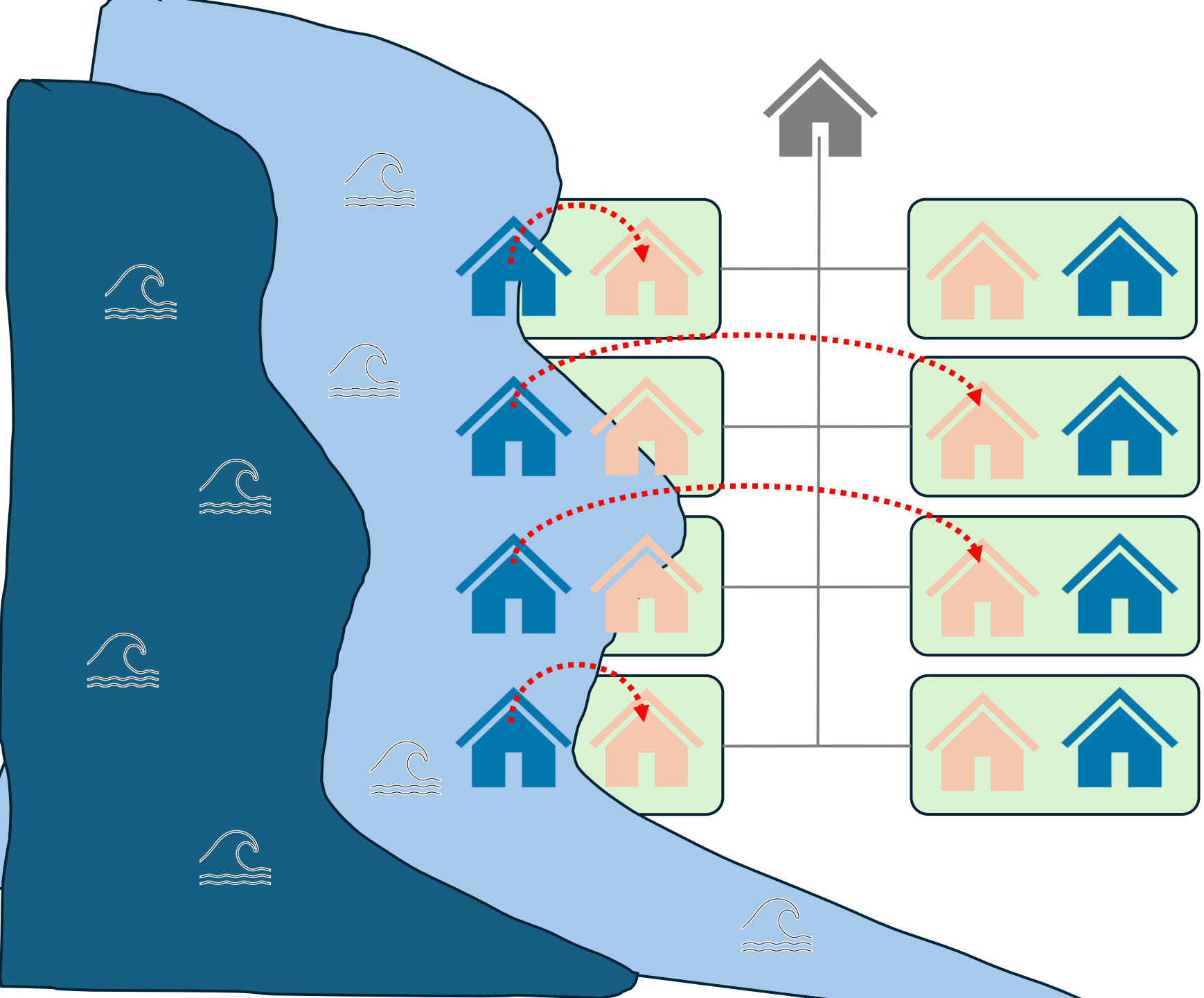
FEDERATED ON-PREM TRUSTED INFRASTRUCTURE SYSTEM

...flere selvstændige systemer eller organisationer samarbejder og stoler på hinandens identiteter

...data ligger lokalt og distribueret

...bygget til kritisk infrastruktur

CyberCube HOSTING





FEDERATED ON-PREM TRUSTED INFRASTRUCTURE SYSTEM

...flere selvstændige systemer eller organisationer samarbejder og stoler på hinandens identiteter

...data ligger lokalt og distribueret

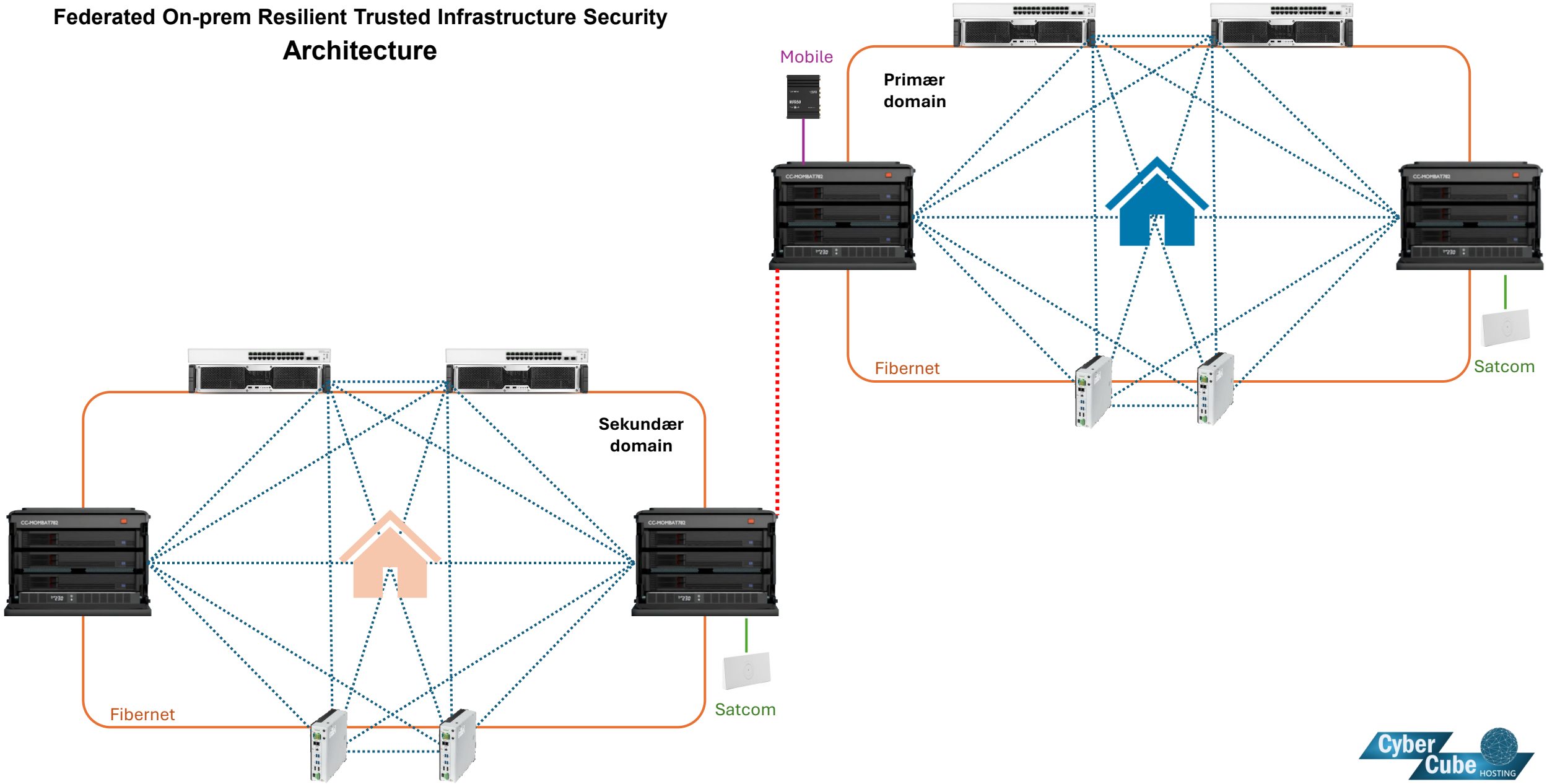
...bygget til kritisk infrastruktur

CyberCube HOSTING

FORTIS

Federated On-prem Resilient Trusted Infrastructure Security

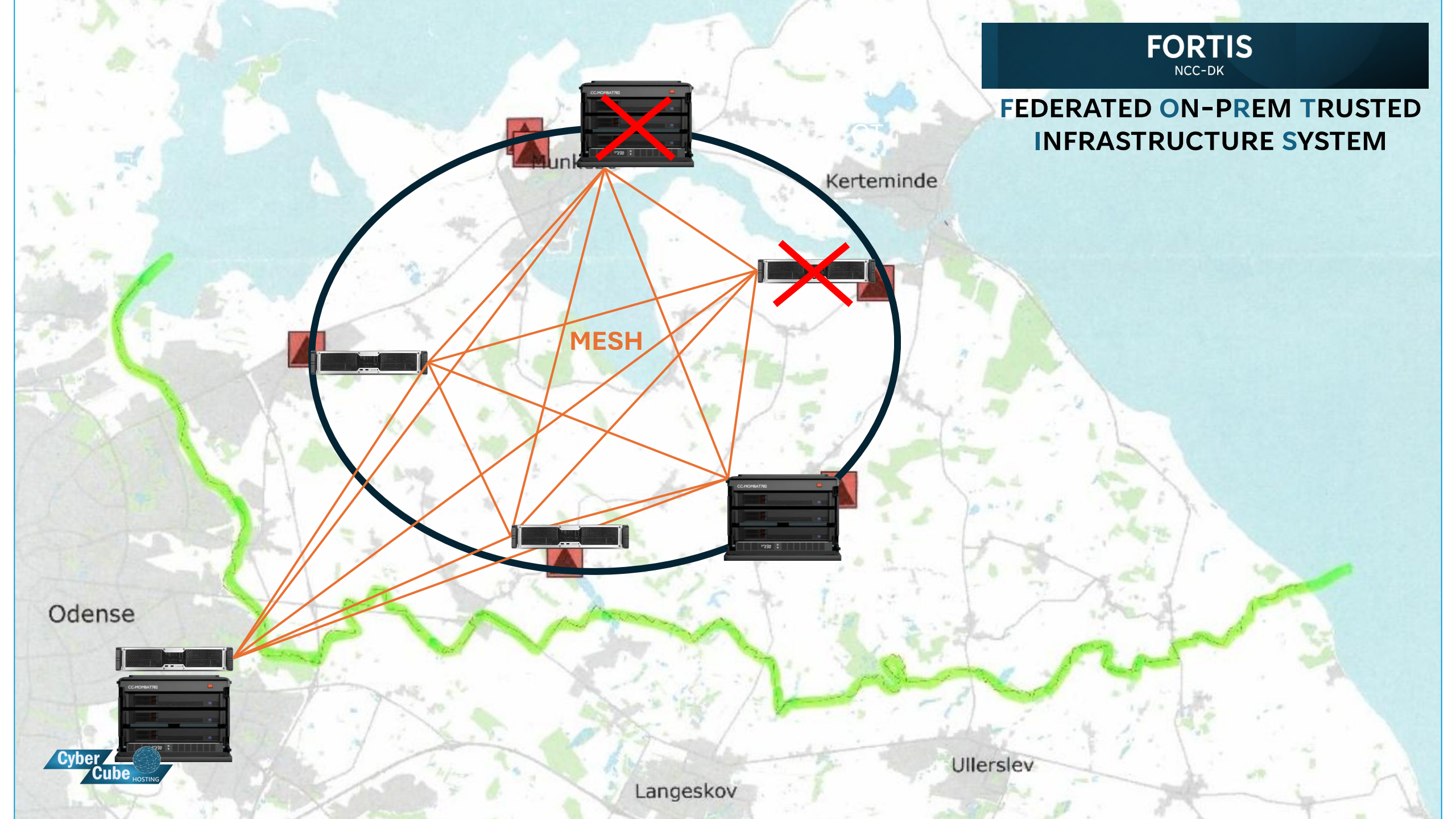
Architecture



CyberCube HOSTING

FORTIS
NCC-DK

FEDERATED ON-PREM TRUSTED INFRASTRUCTURE SYSTEM



open-source

PRODUKT teknologier

PROXMOX

ZITADEL

OpenBao

NGINX

OpenWrt

tailscale

ZABBIX

SigNoz

ANSIBLE

Nextcloud

wazuh.

CC-OT



CC-Hybrid



CC-IT



CyberCube HOSTING

Cyber Cube HOSTING

FORTIOR

FEDERATED ON-PREM TRUSTED INFRASTRUCTURE FOR OPERATIONAL RESILIENCE



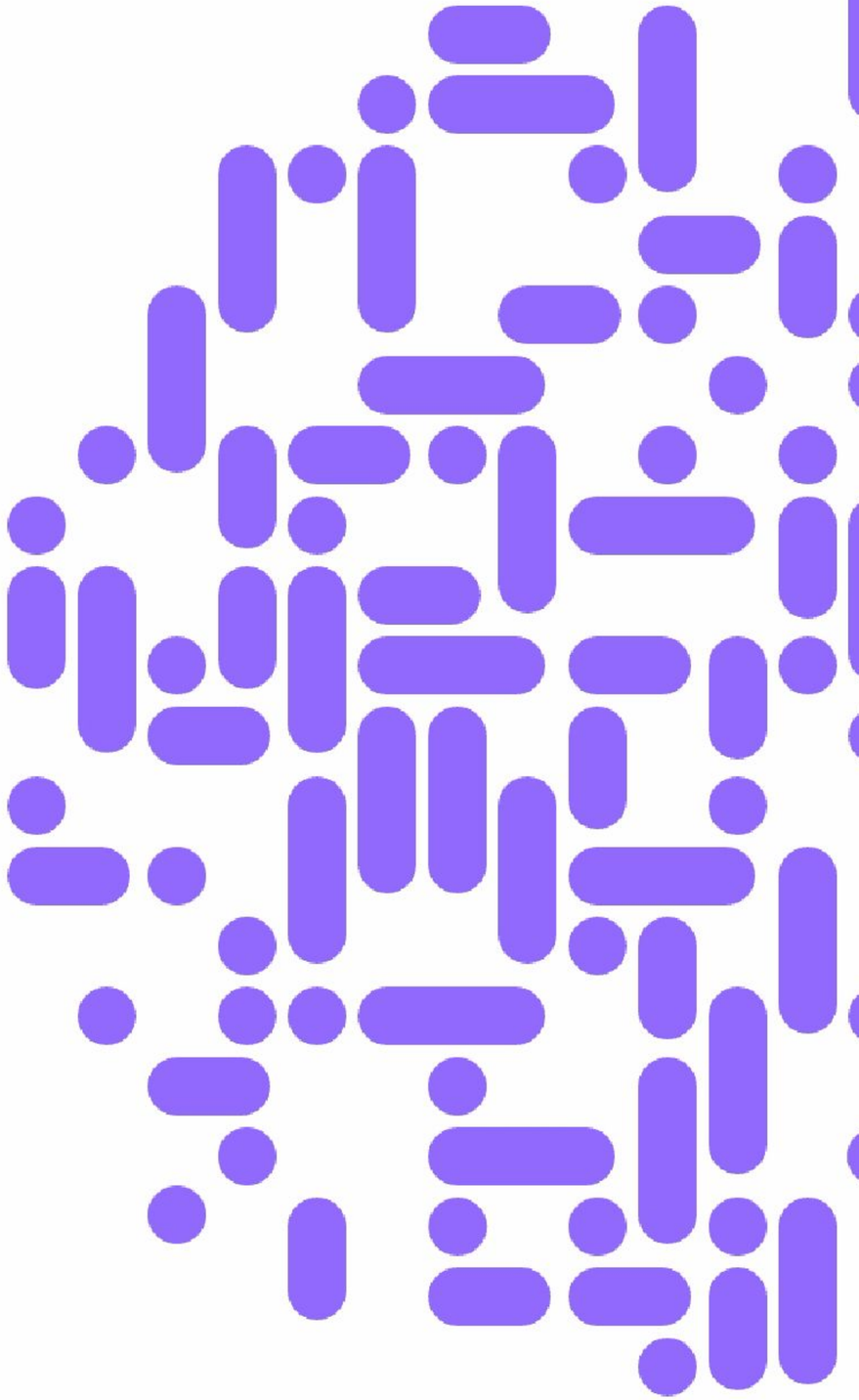
FORTIS er fundamentet for FORTIOR

Resiliate

NCC projekt:

Automatisk kortlægning og risikoanalyse af OT-leverandørkæder i kritisk infrastruktur

Lars Neupart
Lars@Resiliate.io
https://www.linkedin.com/in/larsneupart/



Resiliate

DanBAN
Danish Business Angels

Lars Neupart

3x founder & business angel, primarily in DanBAN

Founder of three tech startups:

1. Cyber / white hat hacking / pen-testing
   - Consulting services & software
2. GRC
   - software & consulting services
3. Resiliate - digital resilience & sovereignty
   - Software
   - Consulting partner ships



Resiliate

Agenda:

1. I dag: Resiliate og it-leverandør detektion & analyse
2. Projektet: OT-leverandør detektion & analyse
3. Hvordan kan I hjælpe / Call to action ?

Resiliate

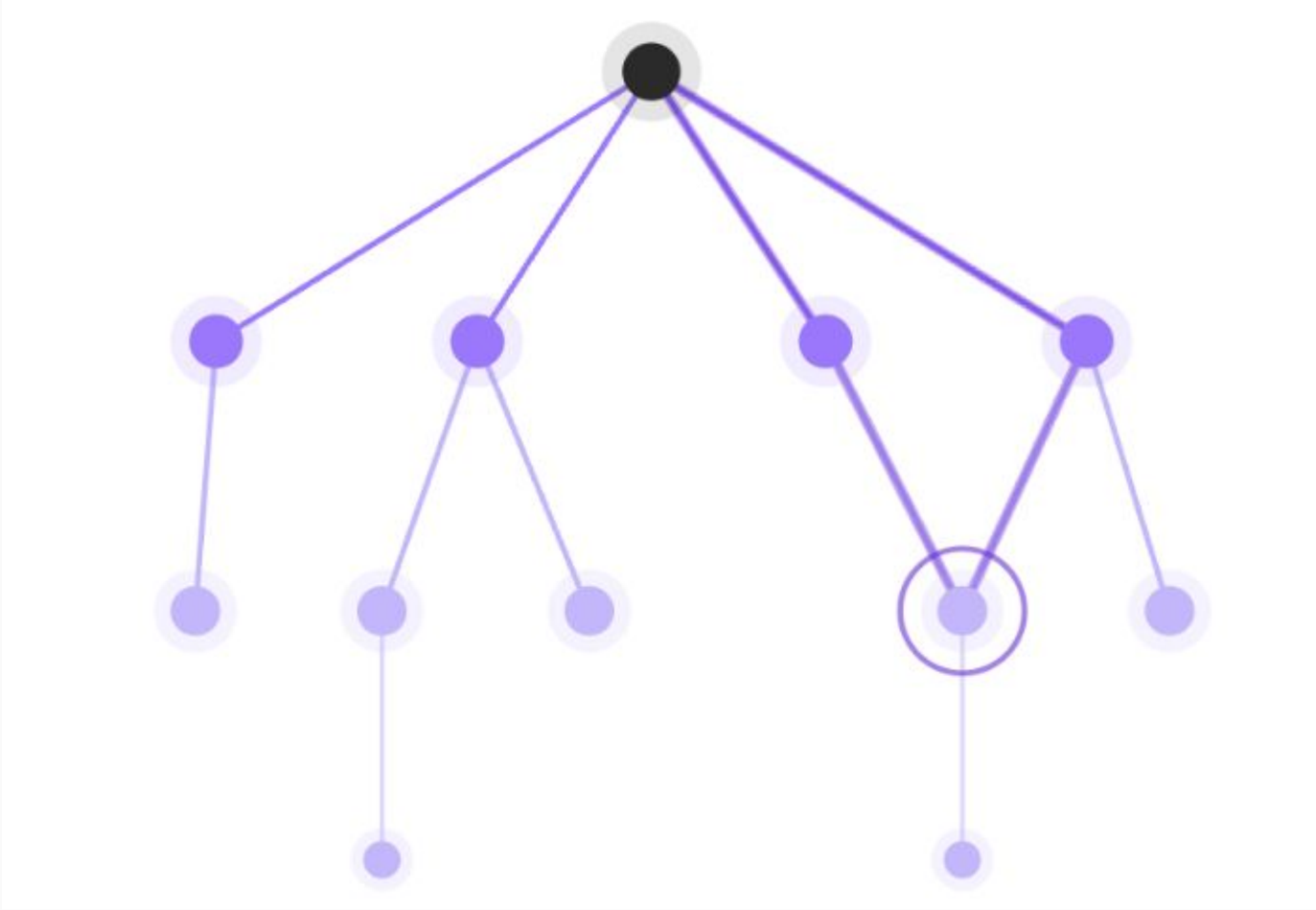
Jeres leverandører har leverandører!

Resiliate finder jeres skjulte it-leverandører, og analyserer resiliens og sandsynlighed for nedbrud på hver af dem.

Resiliate kortlægger og analyserer kontinuerligt **alle lag** af virksomheders it- & tech-leverandører, deres digitale og suverænitet. Plus Resiliate holder øje med relevante ændringer og hændelser, der kan påvirke jeres drift, og giver jer besked

Resiliate

I arver risiko fra virksomheder, I ikke kender navnet på



PROBLEM

Jeres leverandører har leverandører.

Virksomheder er ikke resiliente, når deres leverandører ikke er det.

De fleste virksomheder kan ikke nævne de it-leverandører, der gemmer sig to lag nede. Alligevel arver de risikoen for driftsforstyrrelser.

Resiliate

På hver node i netværket:

Vi måler sandsynligheden for nye nedbrud hos jeres it-leverandører - og deres leverandører.

Og giver jer besked om ændringer & væsentlige begivenheder

Resiliate

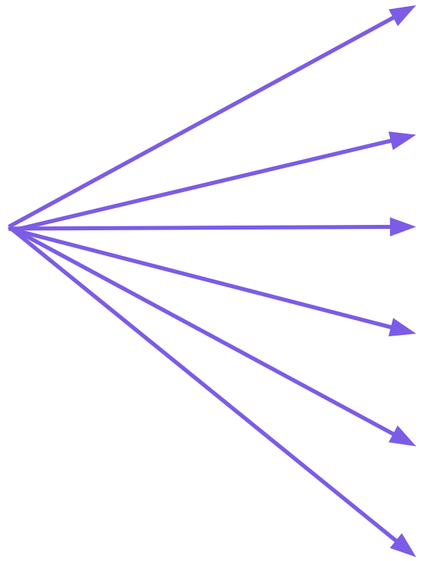
Eksempel på “IT vendor map”.
Bemærk antal underleveramdører



Resiliate

Eksempler på indhold i leverandør-analyse

(“vendor due diligence”)



Vercel Inc. Critical

United States · owned by Independent (United States) · vercel.com · 2 services in use · 59 sub-vendors · assessed 7 Sep 2026

Vercel provides the developer tools and cloud infrastructure to build, scale, and secure a faster, more personalized web. The company offers a Frontend Cloud platform that enables developers to deploy web applications with AI...

More

Overview | Disruption Prediction | Vendors | Services | Insights | Compliance | Financials

Digital Sovereignty	Digital Resilience	Financial Resilience
75%	9.0	7.0

Follow Vercel Inc. Get an email when the analysis changes.

Disruption Prediction
Likelihood of an outage or degradation in the next 6 months →

Vendors
59 sub-vendors →

Services
Personal Data Processing · Vercel
2 in use →

Insights
Sub-vendor breakdown and resilience scores →

Compliance
GDPR, NIS2, HIPAA +11
No gaps →

Financials
Revenue, workforce, and resilience factors
7.0 of 10 →

View the Vercel Inc. Trust Page →

Resiliate

Sandsynlighed for nedbrud

Disruption prediction

Anthropic, PBC has a 100% probability of disruption in the next 6 months.

How it's calculated

Here's what's at stake for your business.

Based on 553 tracked disruptions - 184 critical, 369 major.

- Sep 3 Elevated errors for multiple models
- Sep 3 Elevated errors for Claude Sonnet 5
- Sep 2 Elevated errors for Claude Sonnet 5
- Sep 2 Delays in credit purchases
- Sep 1 Degraded performance on platform.claude.com and Claude for Microsoft Office 365

See the full disruption history →

All systems operational · Live · checked 09:54 PM Status page

Where disruptions concentrate · 6 services

- Claude 69% · 537 disruptions · last Sep 2026
- Claude Code 8% · 51 disruptions · last Sep 2026
- claude.ai 7% · 50 disruptions · last Sep 2026
- Claude Cowork 7% · 45 disruptions · last Sep 2026
- Claude API (api.anthropic.com) 7% · 44 disruptions · last Sep 2026
- Claude Console (platform.claude.com) 2% · 16 disruptions · last Aug 2026

Red = at least one full outage; orange = degradations only.

Resiliate

Agenda:

1. I dag: Resiliate og it-leverandør detektion & analyse
2. **Projektet: OT-leverandør detektion & analyse**
3. Hvordan kan I hjælpe / Call to action ?

Resiliate

Projektet skal udvikle disse moduler/funktioner:

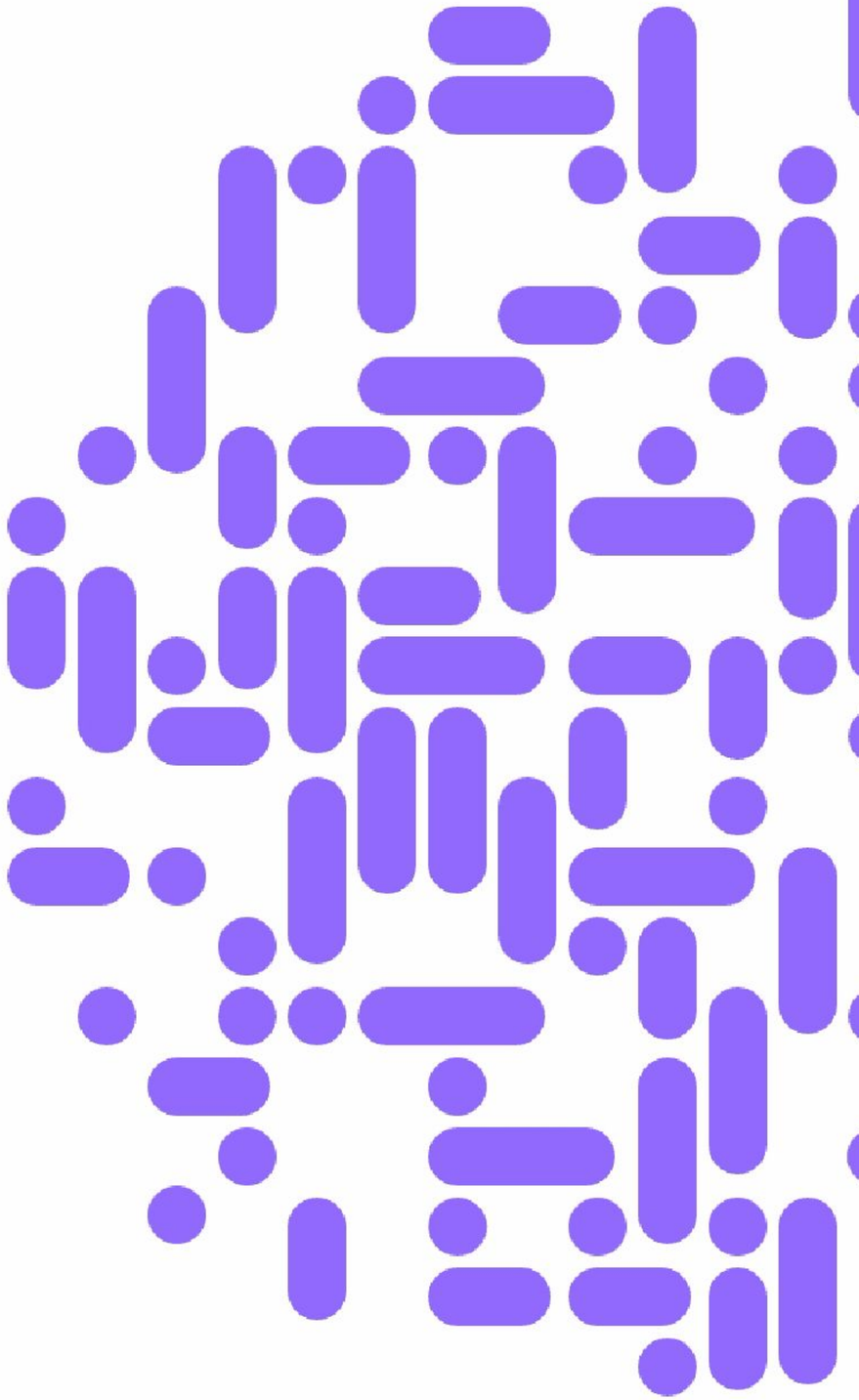
1. Automatiseret OT Vendor Detection
2. IT/OT Dependency Mapping
3. Disruption Prediction Algorithm for kritisk infrastruktur

STØTTET AF:



Resiliate

Kender I de ~~skjulte it leverandører~~, OT-leverandører, der kan udløse jeres næste nedbrud?



Resiliate

Agenda:

1. I dag: Resiliate og it-leverandør detektion & analyse
2. Projektet: OT-leverandør detektion & analyse
3. **Hvordan kan I hjælpe / Call to action ?**

Resiliate

Åben diskussion:

Hvad er forskellene i IT og OT miljøer set i et resiliens / robustheds-perspektiv?

Giver “disruption prediction” mening i OT-sammenhæng?

Opfordring:

Arbejder du med OT? Bliv test-partner.

Test-partnerne skal bruge lidt tid med os og give feed back mod til gengæld at få nogle risikoanalyser af deres OT-leverandører

Kontakt Lars Neupart:

Lars@Resiliate.io

https://www.linkedin.com/in/larsneupart/

Resiliate

How to Resiliate?

1: Scan QR-koden (eller gå på Resiliate.io)
2: Opret konto med arbejds-email
3: Se jeres leverandør-analyser og afhængigheder

SCAN QR



Kvantesikker OT

KVANTECOMPUTERE OG SIKKERHED

Benjamin Salling Hvass · Alexandra Instituttet · 2026

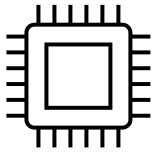
Alexandra giver
danske virksomheder
digital konkurrencekraft
gennem nyeste it-viden



Hvorfor

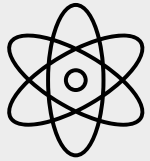
Kort fortalt

Klassiske computere

Problem →  → Løsning

…regner i 1 milliard år…

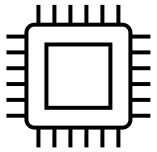
Kvantecomputere

Problem →  → Løsning

…regner i 10 sekunder…

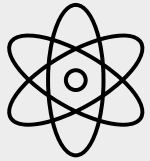
Kort fortalt

Klassiske computere

Klassisk kryptografi →  → Brudt

…regner i 1 milliard år…

Kvantecomputere

Klassisk kryptografi →  → Brudt

…regner i 10 sekunder…

Kryptografi beskytter to ting



Kun de rette kan læse data

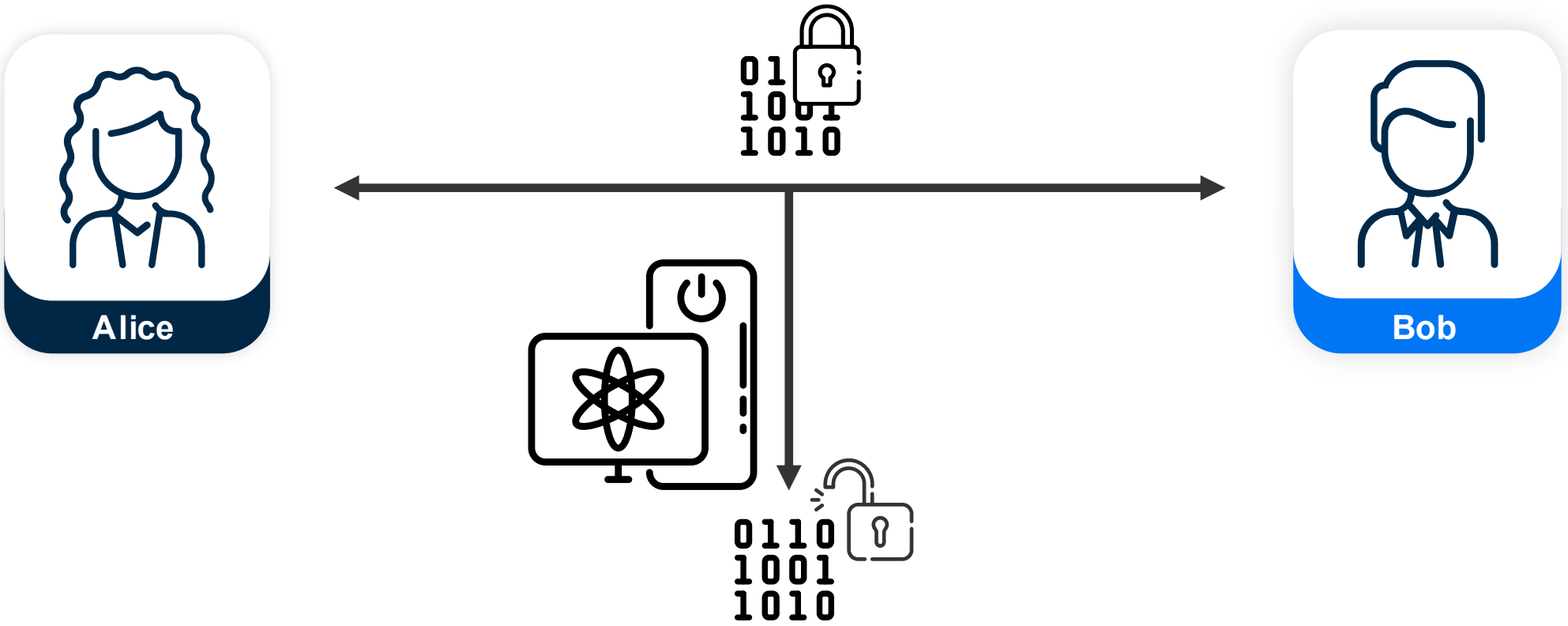
Nøgleudveksling:
Diffie-Hellman, ECDH, RSA



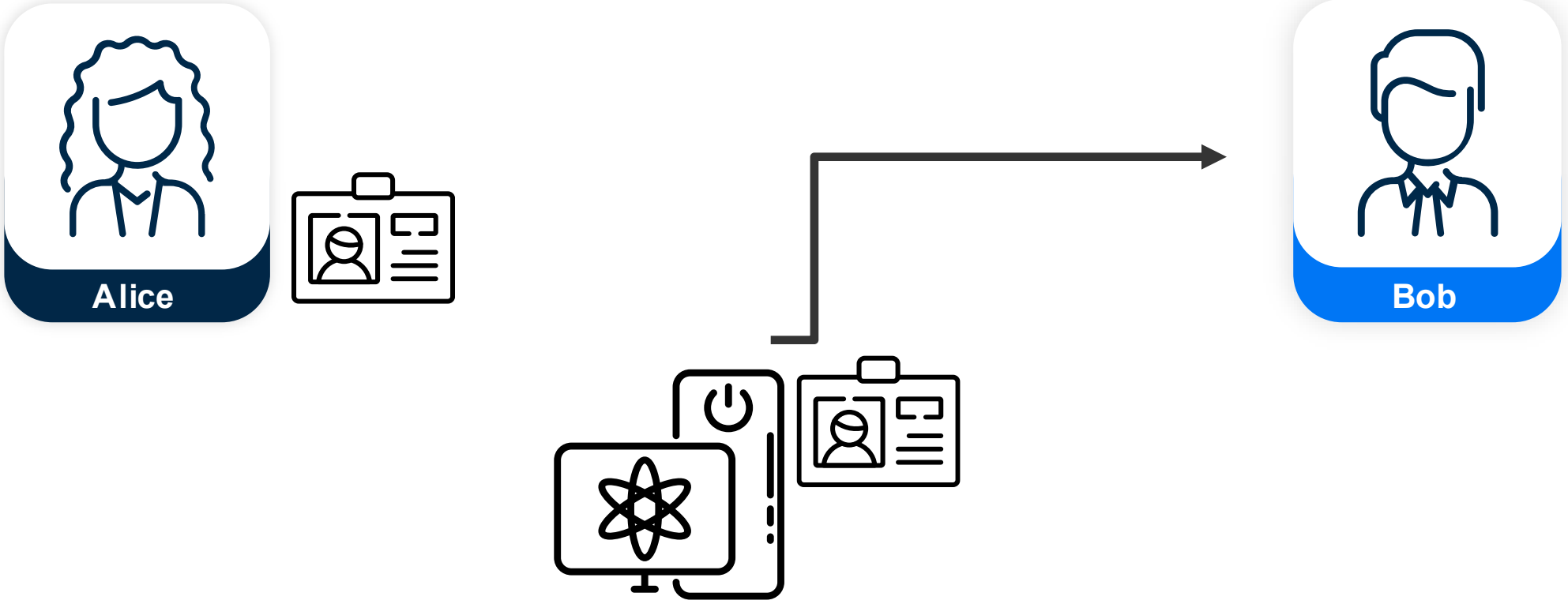
Data er uændret og kommer fra den rette afsender

Digitale signaturer og certifikater:
RSA, ECDSA, EdDSA

Indhent nu, dekryptér senere

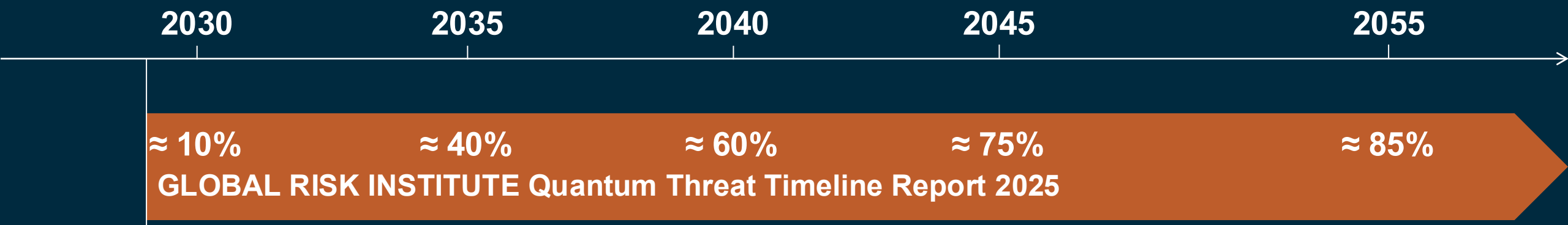


Truslen mod autentifikation



Hvornår

Hvornår kommer kvantecomputeren?

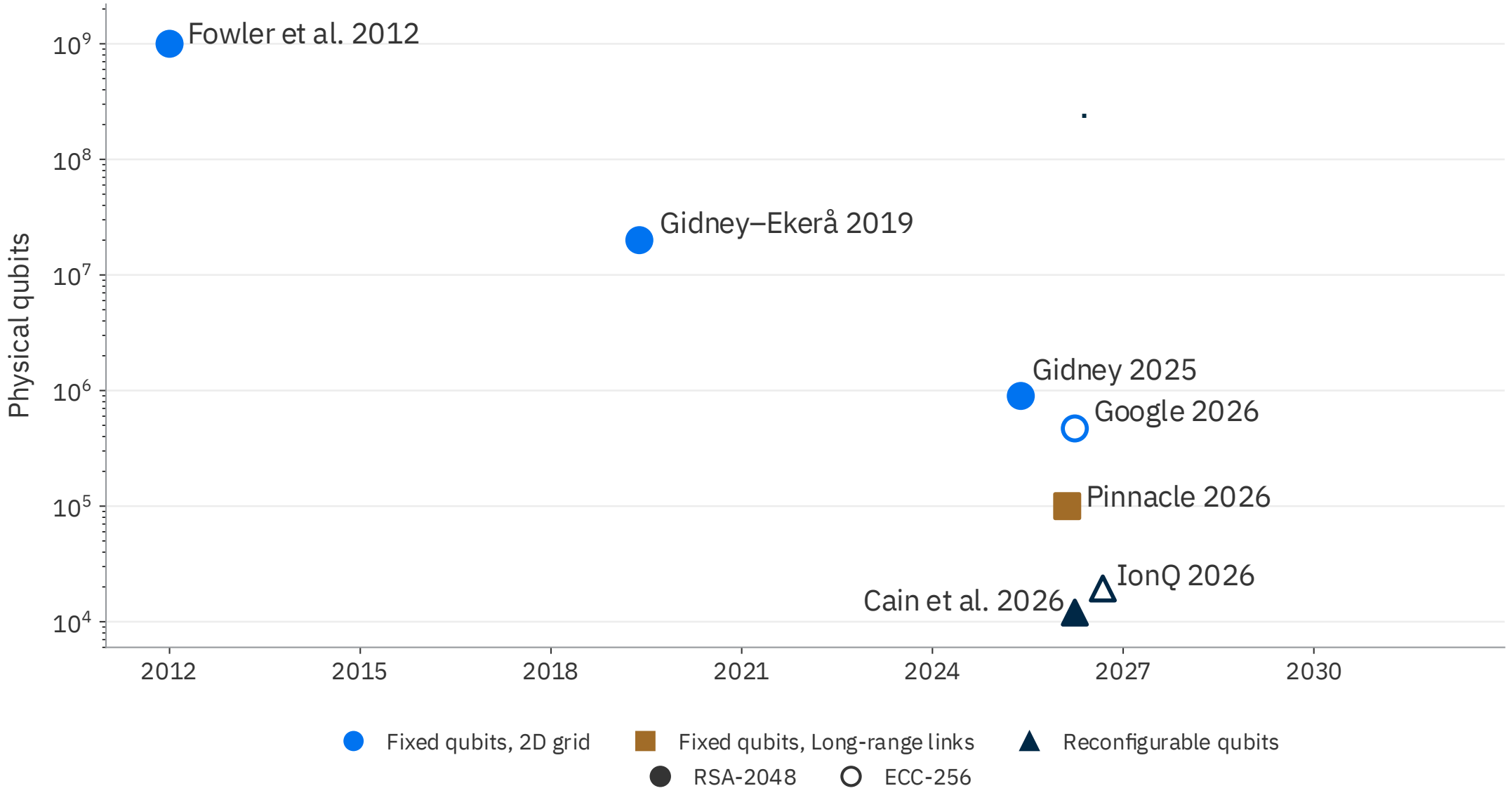


BSI
Status Rapport 2025

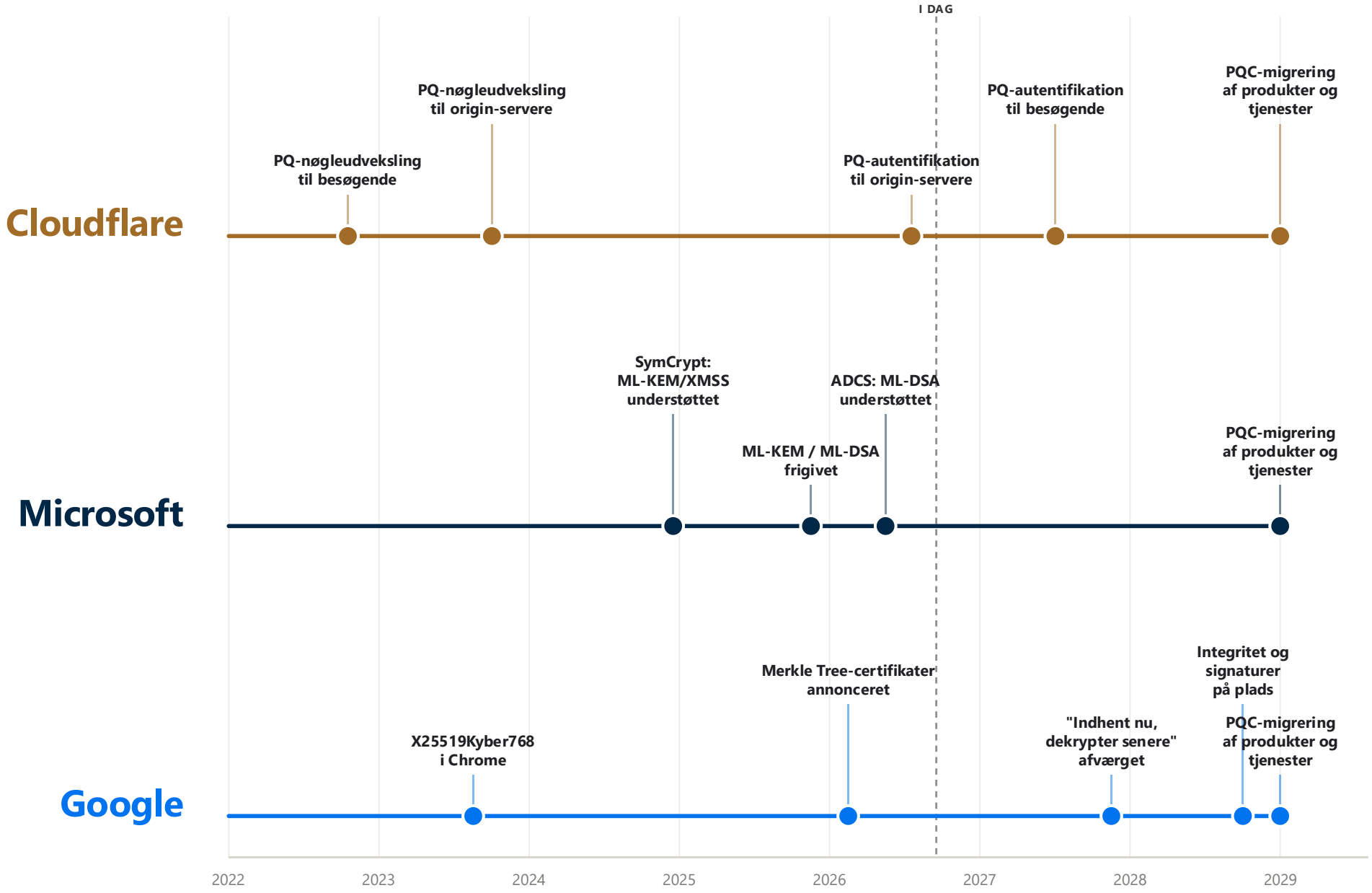
Status of Quantum computer development
"Our conservative estimate is that cryptographically relevant quantum computers are likely to be available within 15 years." "possible disruptive results in this context could accelerate the development to below a decade."

DEADLINE 2029
GOOGLE og
MICROSOFT

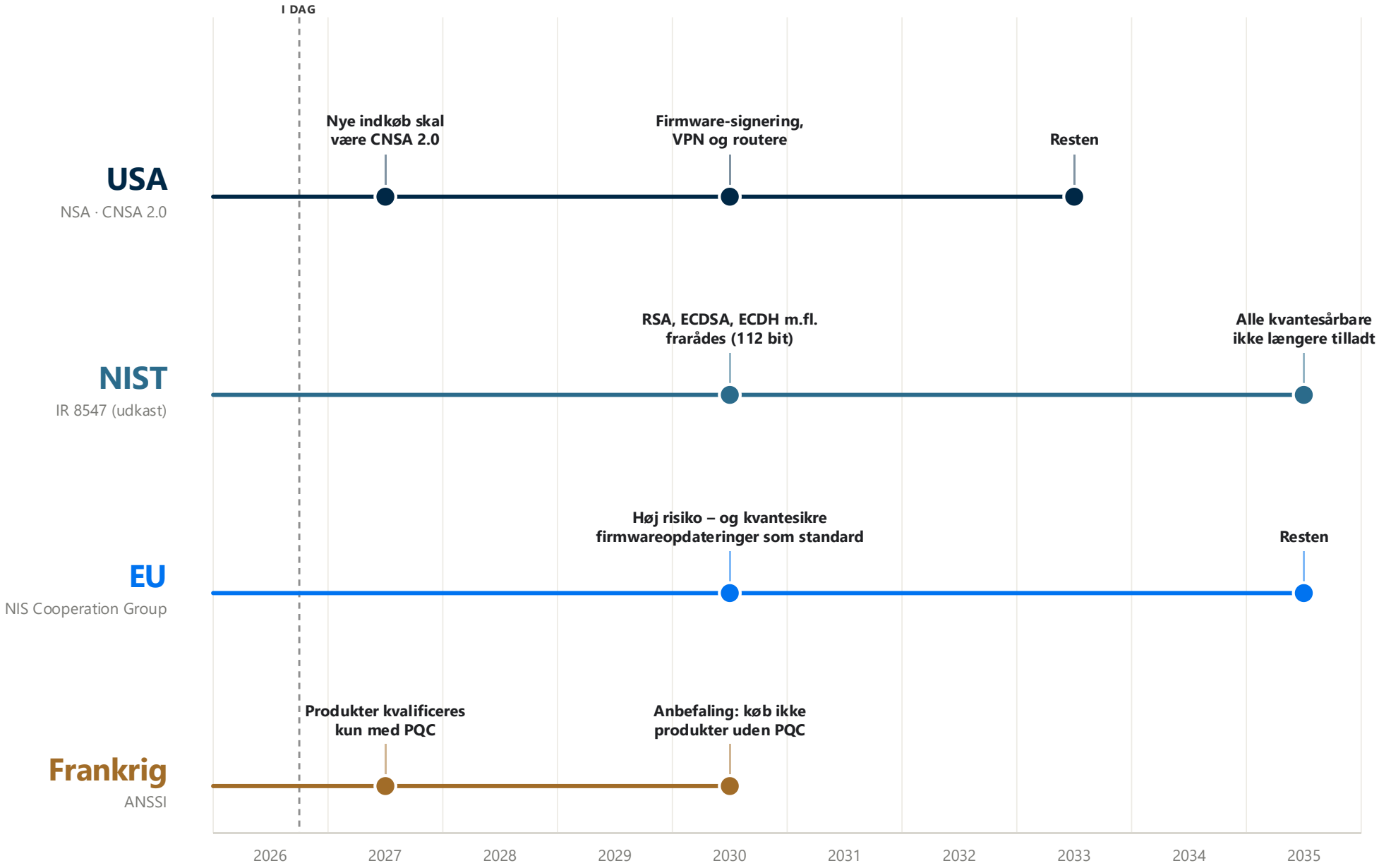
(c) Alexandra Instituttet



(C) ALEXANDRA INSTITUTTET



(C) ALEXANDRA INSTITUTTET



(C) ALEXANDRA INSTITUTTET

OT

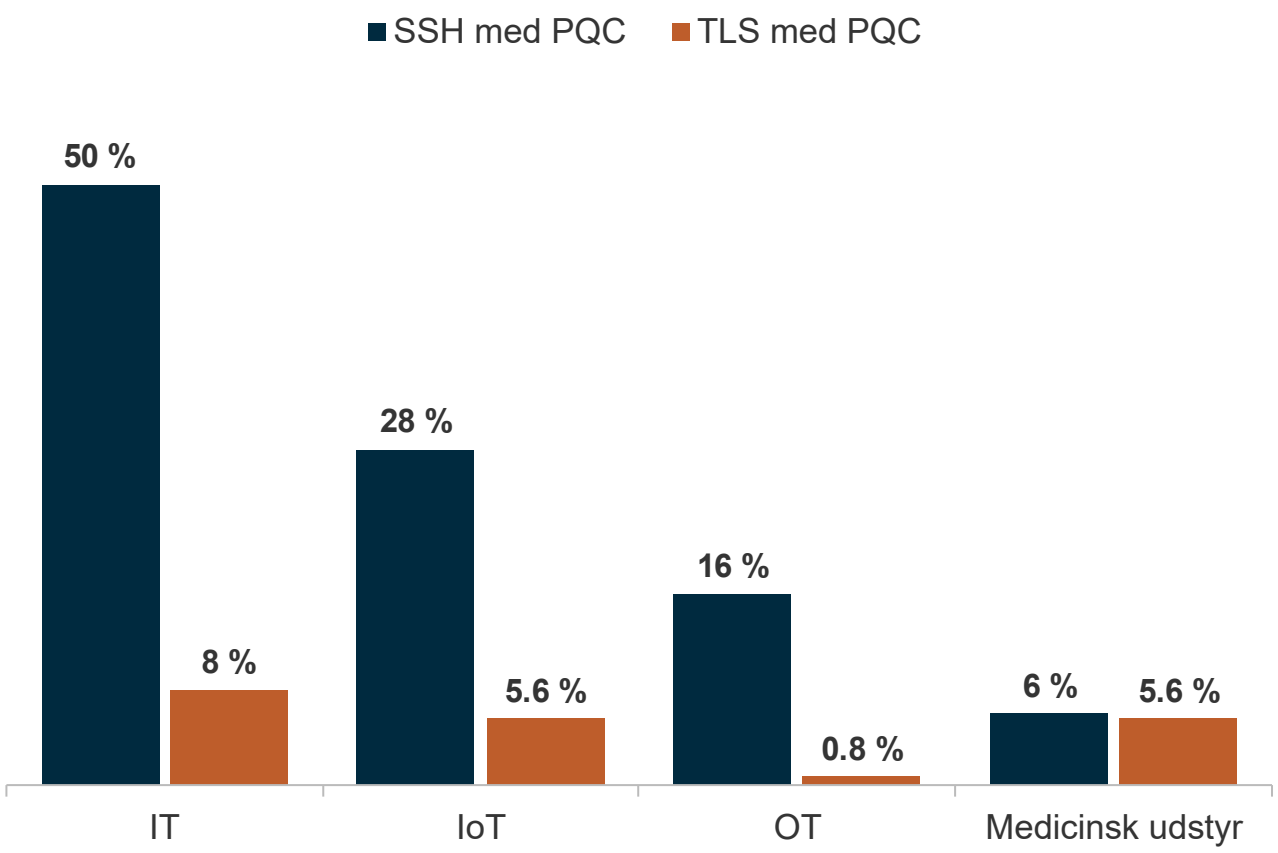


Fjernadgang og udstyr med lang levetid

	Fjernadgang VPN · jump-server · SSH · RDP	**Udstyr med lang levetid** RTU'er · målere · relæer · sensorer · IoT
Specielt sårbart	• Nøgleudvekslingen i VPN og SSH • Certifikater og nøgler bag VPN, RDP og SSH	• Firmware-signaturer • Lang levetid • Svære at opdatere • Små enheder
Status	• PQC-nøgleudveksling er bredt understøttet • Nogle steder er PQC-certifikater understøttet	• Få leverandører tilbyder PQC
Gør nu	• **Tjek hvad der kan gøres i dag** • **Kan nøgleudveksling opgraderes?** • **Kan PQC-certifikater understøttes?**	• **Beskyt forbindelsen foran enheden med en gateway** • **Stil krav til næste udbud**

(C) ALEXANDRA INSTITUTTET

OT halter efter IT



Andel af enheder i virksomhedsnetværk, der understøtter kvantesikker nøgleudveksling. Kilde: Forescout Research – Vedere Labs, juni 2026.

16 %

af OT-enhederne understøtter PQC i SSH – mod 50 % i IT. I TLS er det under 1 %.

2 ud af 3

OT-enheder i virksomhedsnetværk har kritisk risiko og understøtter ikke PQC.

(C) ALEXANDRA INSTITUTTET

Hvordan

Opdater software og biblioteker, eller ræk ud til leverandører

Kvantesikker kryptografi findes allerede

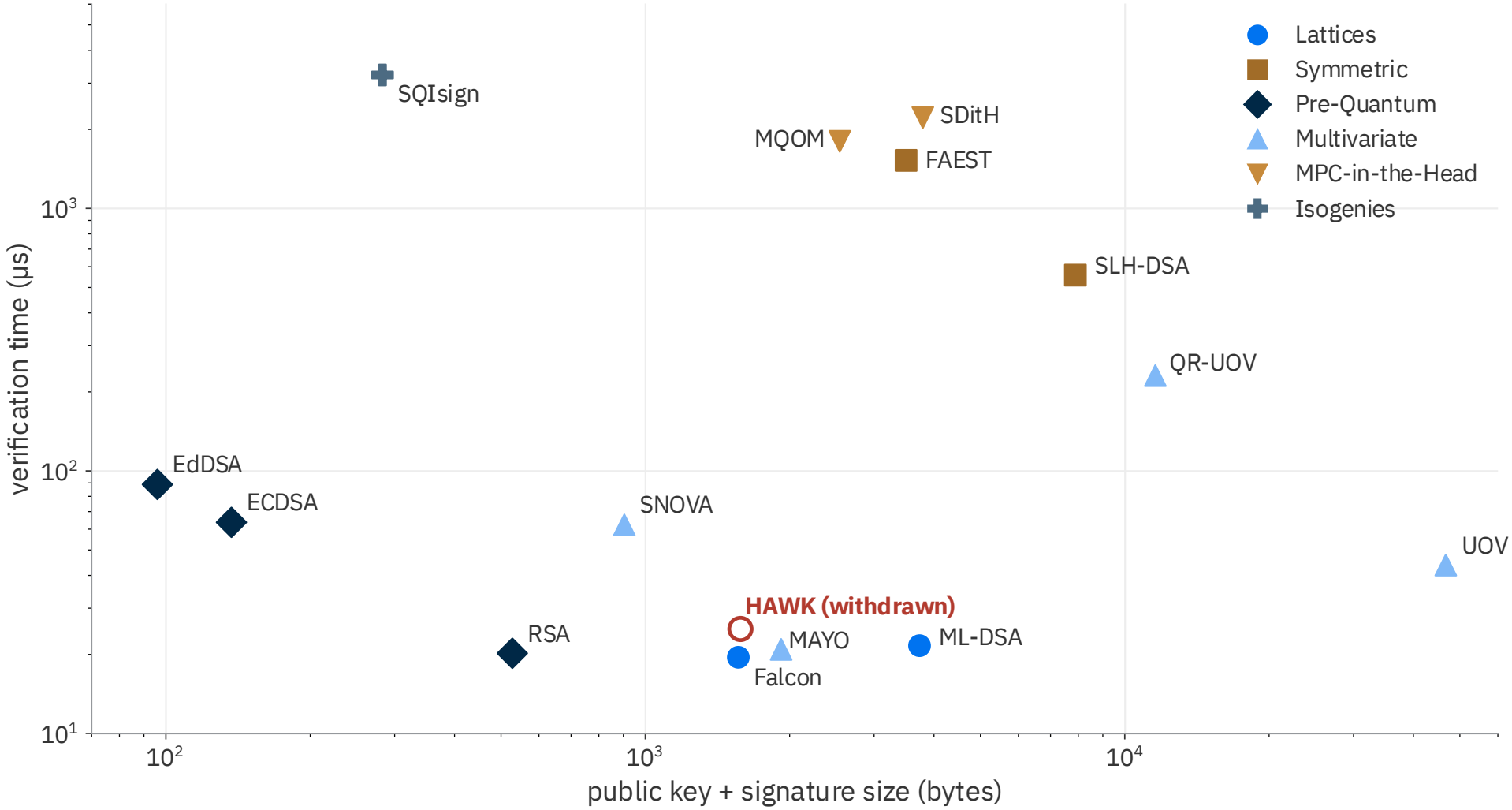
Samme hardware.
Kører på klassiske computere.

Standardiseret.
ML-KEM til nøgleudveksling, og ML-DSA til signature. Evt. suppleret af SLH-DSA, FN-DSA, XMSS/LMS til signaturer.

Hybrid.
Klassisk og kvantesikker sammen, fx X25519MLKEM768. Giver den kombinerede sikkerhed.

Større og tungere.
Ingen kvantesikker signatur er lige så lille og hurtig som ECDSA.

Kvantesikker kryptografi findes allerede



NIST Round 3 signature candidates, lowest security parameter set per scheme. Source: pqshield.github.io/nist-sigs-zoo (data/schemes/.yaml).*

Første skridt

1

Forankr

Nedsæt en arbejdsgruppe eller forankr truslen i eksisterende grupper

2

Kortlæg

Start ved IT/OT-grænsen, firmware-signering og certifikater.

3

Prioritér

Vægt integritet højest. Se på fysisk konsekvens, levetid, og om enheden overhovedet kan opdateres.

4

Planlæg

Læg migrationen ind i planlagte stop.

Skitser et internt roadmap hvor milepæle og systemer er tænkt ind.

Brug det, I allerede gør: risikovurderinger, asset-registre og NIS2-arbejdet. Kvantetruslen er en ny trussel i en kendt proces.

(C) ALEXANDRA INSTITUTTET

Cisco: kvantesikker kommunikation

Cisco Quantum-Safe Communications Roadmap

NIST Post-Quantum Cryptography (PQC) algorithms implemented across these platforms/protocols

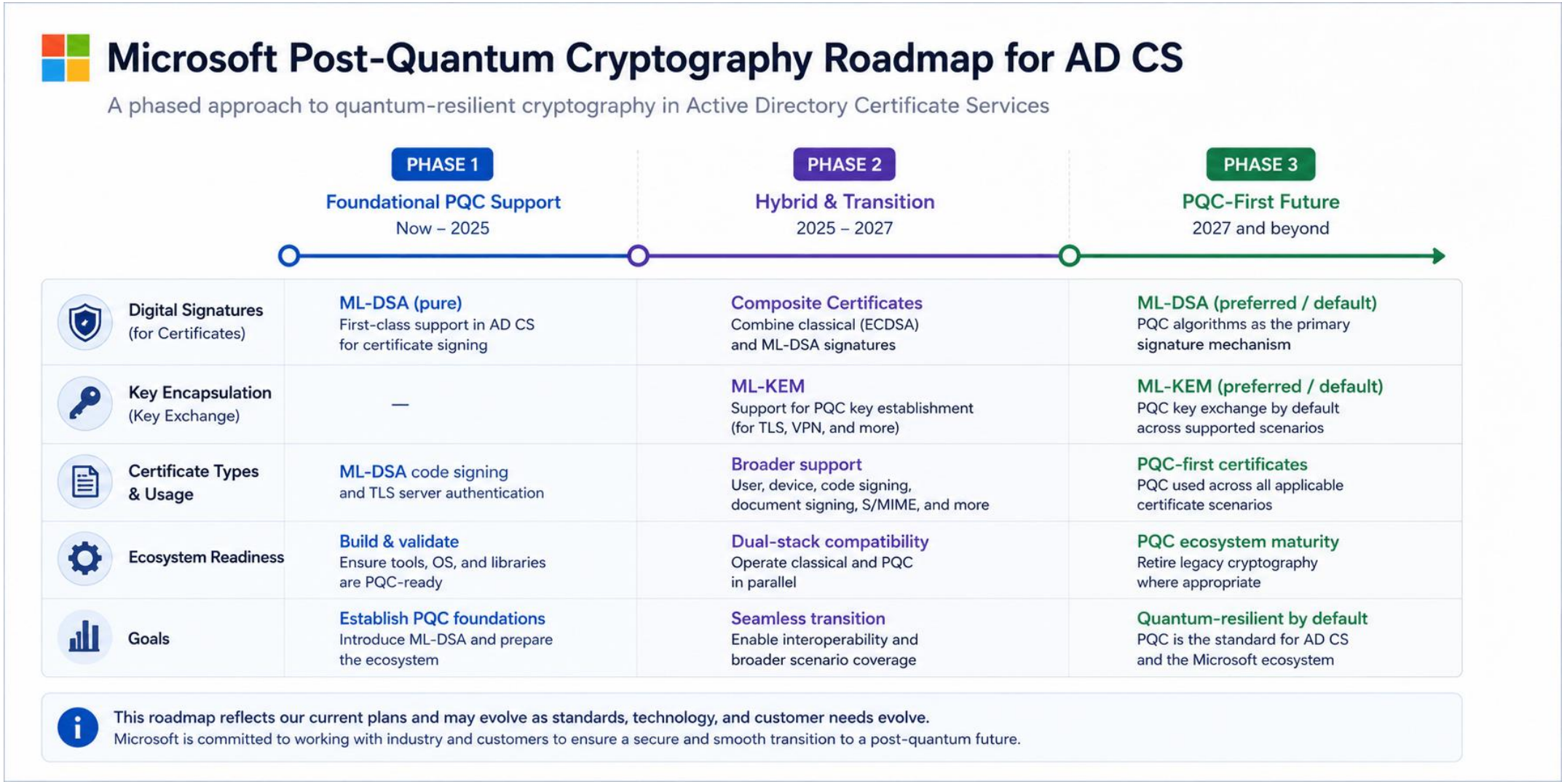
Portfolio	Protocols planned by December 2026	Protocols planned by June 2027
Enterprise Routing (IOS-XE)	IKEv2 IPsec, DMVPN, FlexVPN, SD-WAN IPsec, MACsec, SSH, TLS	TLS, DTLS, Authentication capabilities
Enterprise Switching (IOS-XE)	IPsec, MACsec, SSH, TLS	Additional TLS use cases
Wireless (IOS-XE)	TLS 1.3 updates for: RadSec, TACAS, LDAP Over-The-Air (OTA) Support for PQC with introduction of security profiles (Security profile 16 and 18 support)	dTLS updates for: RadSec, TACAS, LDAP, CAPWAP, VxLAN
IoT (IOS-XE)	IKEv2 IPsec, MACsec, SSH, TLS	
Data Center Networking (NX - OS)	SSH	MACsec, TLS*
Data Center Networking (Nexus Dashboard)		SSH, TLS*
Data Center Networking (ACI)		SSH, TLS - HTTPS/API* SSH - Device Access* , TLS - Internal/External communication*
Service Provider (IOS - XR)	MACsec, SSH, TLS	
Firewalls		IPSec, SSH and TLS Decryption
Secure Client		IPsec
Catalyst Center		TLS, SSH and SFTP (Hybrid)
Webex	TLS and MLS for Webex App and Devices supporting end-to-end encrypted meetings	
Meraki Dashboard		TLS implemented in Secure OS, NGINX, and Envoy Gateway; hybrid configuration for secure management communications
Splunk	Hybrid PQC capabilities for all DoD IL5 authorized Splunk cloud offerings	
ThousandEyes		TLS for agent communications and APIs/application access, PQC-enabled signing for all ThousandEyes Agents
Identity Services Engine		RADIUS, EAP, TACACS, HTTPS (critical services), LDAPS, IPsec, SSH
Duo		TLS with fallback options to support systems that are not yet updated in customer environments

© 2026 Cisco and/or its affiliates. All rights reserved.

*July/Aug 2027 depending on software release schedule.

This roadmap may change without notice. Last updated Aug 11, 2026.

Microsoft: kvantesikre certifikater i AD CS



Stil krav i næste udbud

1. **Kryptoagilitet**
   algoritmer skiftes via konfiguration – ikke ny hardware
2. **Kvantesikre firmware-signaturer**
   fx LMS/XMSS eller ML-DSA – og tillidsankre, der kan opdateres i felten
3. **Åbenhed**
   hvilke kryptobiblioteker og algoritmer er indbygget (CBOM)?
4. **Plads til større nøgler**
   buffere og protokoller skal kunne rumme PQC-størrelser
5. **Roadmap med forpligtende datoer**
   hvornår kommer ML-KEM, ML-DSA og hybrid?

(C) ALEXANDRA INSTITUTTET

Til diskussion

1. Hvem har fjernadgang til jeres anlæg i dag og hvordan er den forbindelse beskyttet?
2. Hvilke af jeres systemer vil stadig være i drift i 2035?
3. Ser I andre steder hvor OT er særligt udsat overfor kvantetruslen?
4. Hvilke eksisterende processer kan kvantetruslen indtænkes i? Kortlægning, SBOMs, risikovurdering, etc.
5. Hvad ville det kræve at skrive krav om kvantesikkerhed ind i jeres næste udbud?

(C) ALEXANDRA INSTITUTTET

Kontakt

Benjamin Salling Hvass

Senior Security Architect
benjamin.hvass@alexandra.dk

iDMZ, Virtual Patching & OT IPS



Henrik V. Meyer, hmeyer@fortinet.com
Sales Engineer - OT SME

HOW CYBER CRIMINALS THINK

© Fortinet Inc. All Rights Reserved.

1. Find a target

© Fortinet Inc. All Rights Reserved.

2. Hack the target

© Fortinet Inc. All Rights Reserved.

3. Abuse the target

© Fortinet Inc. All Rights Reserved.

4. Sell the target

© Fortinet Inc. All Rights Reserved.

WHAT IS A TARGET?

© Fortinet Inc. All Rights Reserved.

YOU ARE THE TARGET

© Fortinet Inc. All Rights Reserved.

hmeyer@fortinet.com
linkedin.com/in/meyerhenrik



© Fortinet Inc. All Rights Reserved.

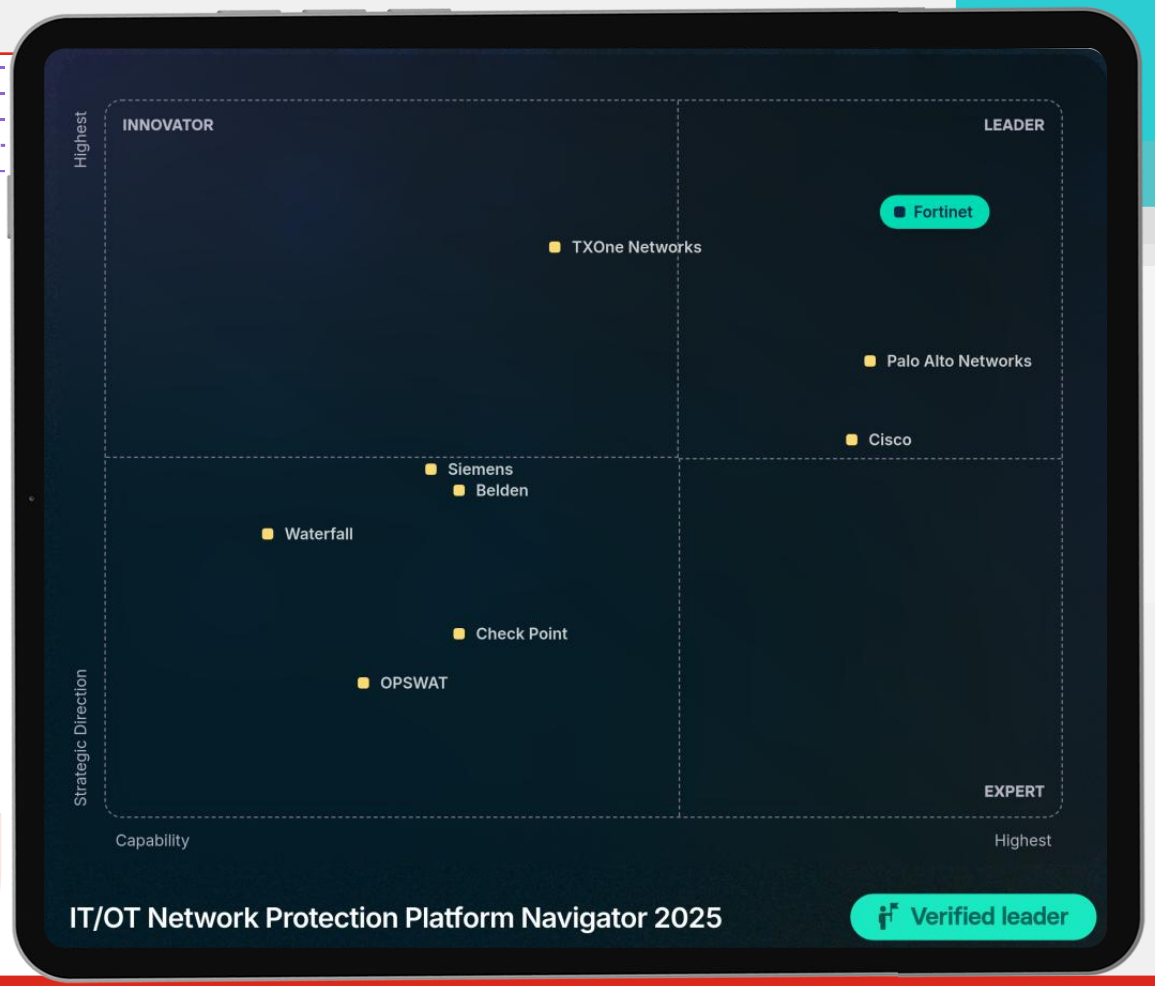
3Y Leader in the IT/OT Network Protection Platform Navigator 2025

Independent Confirmation of Platform Leadership

Fortinet IT/OT Security Platform identified as a Navigator Leader for three consecutive years

Fortinet is a leader for the 3rd successive year. The OT Security Platform consists of over 20 products in 3 solution pillars: secure networking, zero trust/SASE, and security operations. In addition, the technology integration offered through the OT Security Platform extends beyond Fortinet solutions to third-party technologies, delivering a comprehensive and centralised OT service. Fortinet has also built strong relationships with leading channel partners and OEMs

Westlands Advisory, Industrial Cybersecurity Industry Analysis 2025

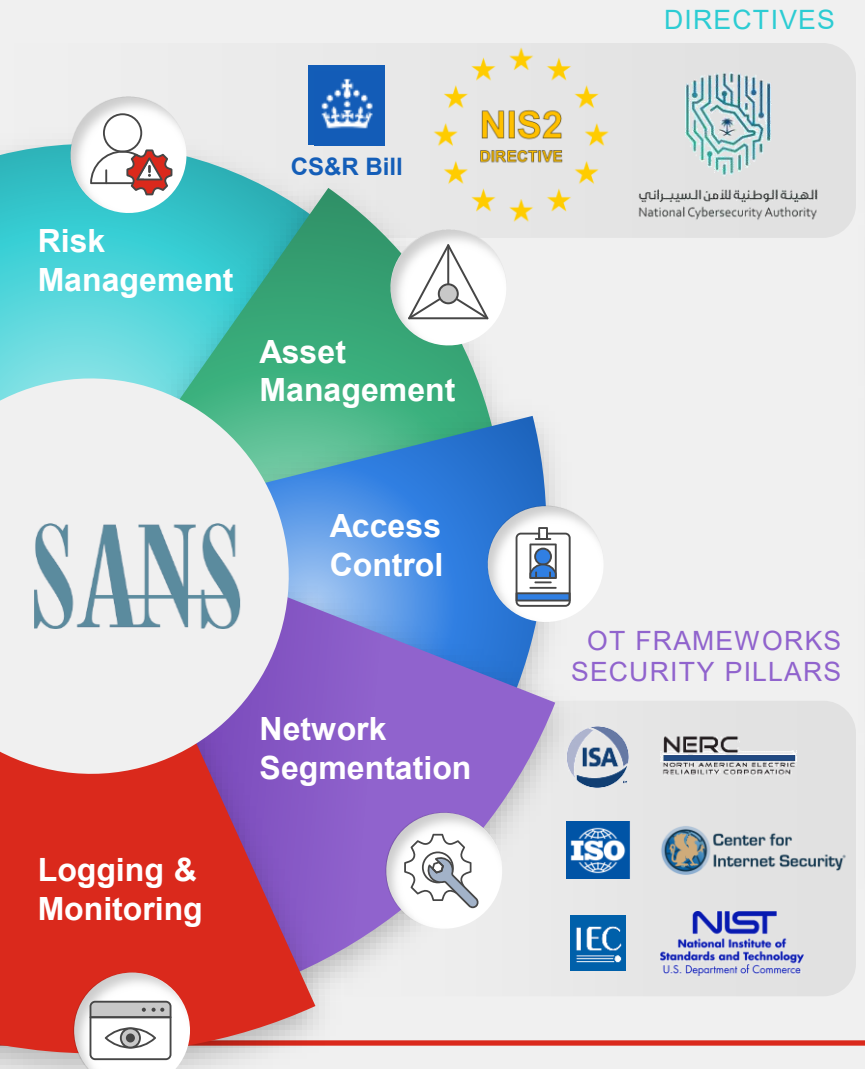


Westlands Advisory confirms Fortinet as a leader in IT/OT Security Platforms

© Fortinet Inc. All Rights Reserved.

Technology Mapping for Compliance

Supporting People and Process with technology



Asset Management	SIEM	NAC	NGFW	API	
Access Control to Networks & Assets	NGFW	NAC	FAC	Client	Tokens
Segmentation, Protection & Response	NGFW	Switch	WIFI	XDR	Tokens
Events, Alerts and Incident Detection	SOAR	SIEM	Analyzer	SandBox	Deception
Risk Management	Manager	SIEM	Analyzer		

SINGLE PANE MANAGEMENT

THREAT INTELLIGENCE

INTEROPERABILITY

Compliance emerges naturally from well-operated security programs

© Fortinet Inc. All Rights Reserved.

NIS2 – Artikel 21

(89) Væsentlige og vigtige enheder bør indføre en bred vifte af grundlæggende cyberhygiejnepraksisser såsom »zero trust«-principper, softwareopdateringer, enhedskonfiguration, netværkssegmentering, identitets- og adgangsstyring eller brugerbevidsthed, arrangere kurser for deres personale og højne bevidstheden om cybertrusler, phishing og social engineering-teknikker. Disse enheder bør desuden evaluere deres egne cybersikkerhedskapaciteter og, hvor det er hensigtsmæssigt, stræbe efter at integrere cybersikkerhedsforstærkende teknologier, såsom systemer baseret på kunstig intelligens eller maskinlæring, for at forstærke deres kapaciteter og sikkerheden i net- og informationssystemerne.

Reference: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A32022L2555

© Fortinet Inc. All Rights Reserved.

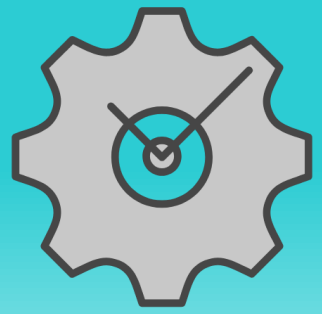
Recommended Best Practices for Safeguarding OT



Segmentation



Visibility & Compensating Controls



SOC & Incident Response



Platform Approach



OT threat intelligence

© Fortinet Inc. All Rights Reserved.

OT CPS Secured Networking and Process Integrity

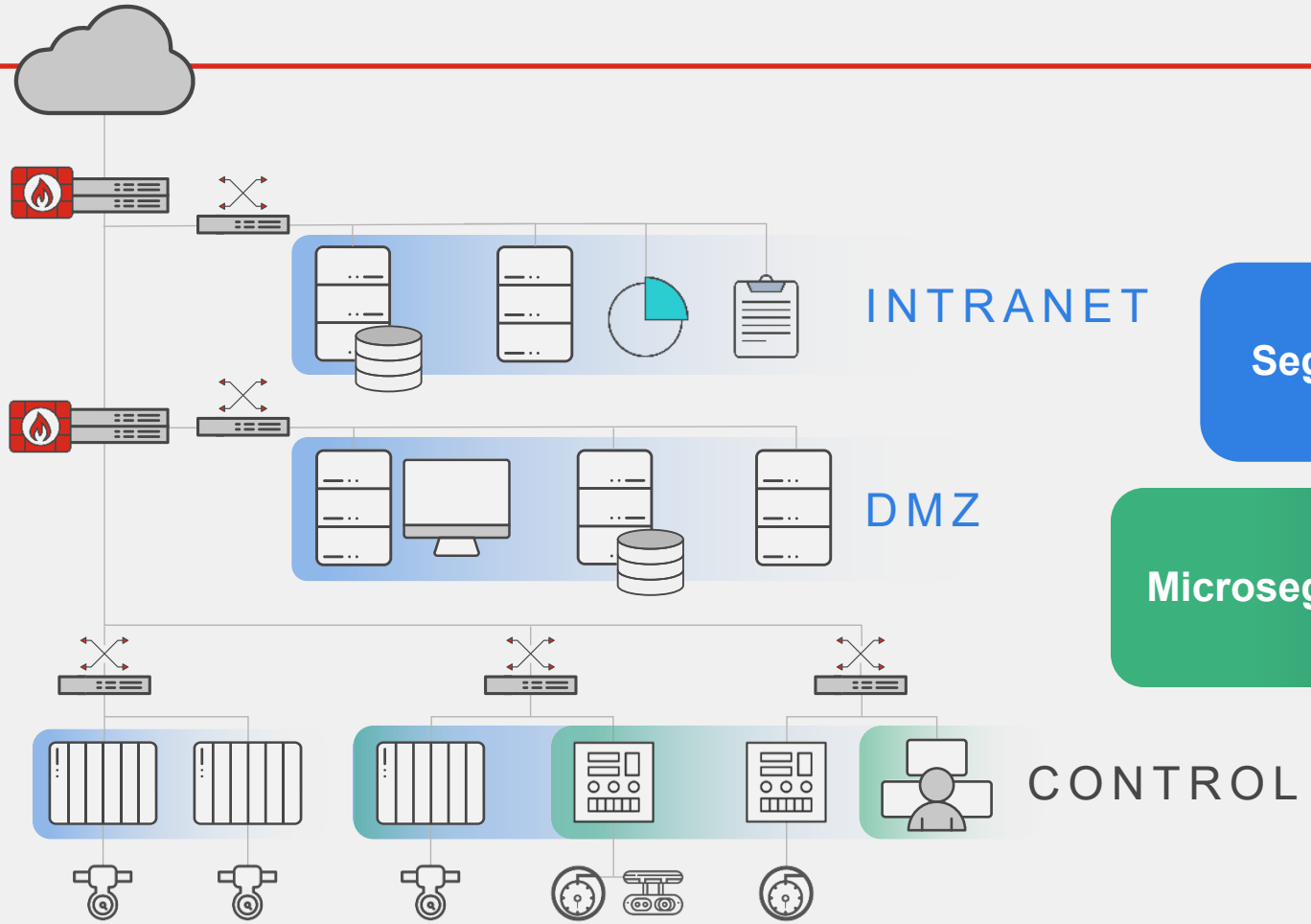
Protecting processes and safety systems

Asset-aware
segmentation

Enforcement
close to OT assets

Built-in blast
radius reduction

Protection of Level 0 and Level 1
devices and control logic integrity



Secured networking contains threats. Process integrity at Level 0 and 1 protects Safety

© Fortinet Inc. All Rights Reserved.

The FortiGuard OT Security Service

+3,500	+1,600	~800	+2,100
Protocol Rules	OT App Detection Rules	IPS Rules	OT Virtual Patch Rules

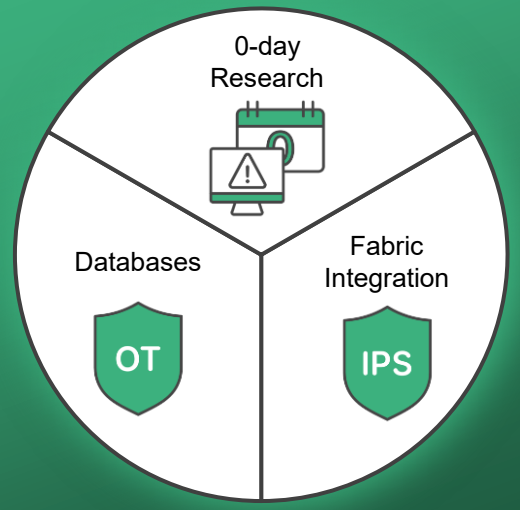
OT Protocols

Allen Bradley DF-1
DNP3
Ether-S-Bus
EtherCAT
EtherNet-IP/CIP
FL-NET
GE EGD
IEC 60870-5-104
IEC 61850
IEC Synchrophasor
KNXnet/IP
LonTalk
Mitsubishi MELSEC
MMS
Modbus RTU
Modbus TCP/IP
OCPP
OPC
OPC UA
Profinet CBA
Profinet IO
Rockwell FactoryTalk
SafetyNET
SECS-II/GEM
SEL Fast Nessage
Schnedier UMAS
Siemens S7
Siemens S7 Plus
Siemens SIMATIC CAMP
TRDP
Triconex TSAA
Triconex TriStation
WITSML

…and many, many more

AI-Powered Security

FortiGuard Labs Threat Intelligence



OT Vulnerabilities

ABB
ETIC
Advantech
Fuji
AVEVA
GE
B&R Automation
Iconics
Contec
Inductive Automation
Delta IA
InHand Networks
DUT CCE
KeySight
Eaton
Korenix
Moxa
Ricon
mySCADA
Rockwell
OAS
Schneider
Omron
SEL
Osprey
Siemens
Pepperl+Fuchs
Sierra Wireless
PnP SCADA
WECON
PTC
Wibu Systems

Integrations | OS | NGFW | SD-WAN | NDR | Deception | Sandbox | NAC

© Fortinet Inc. All Rights Reserved.

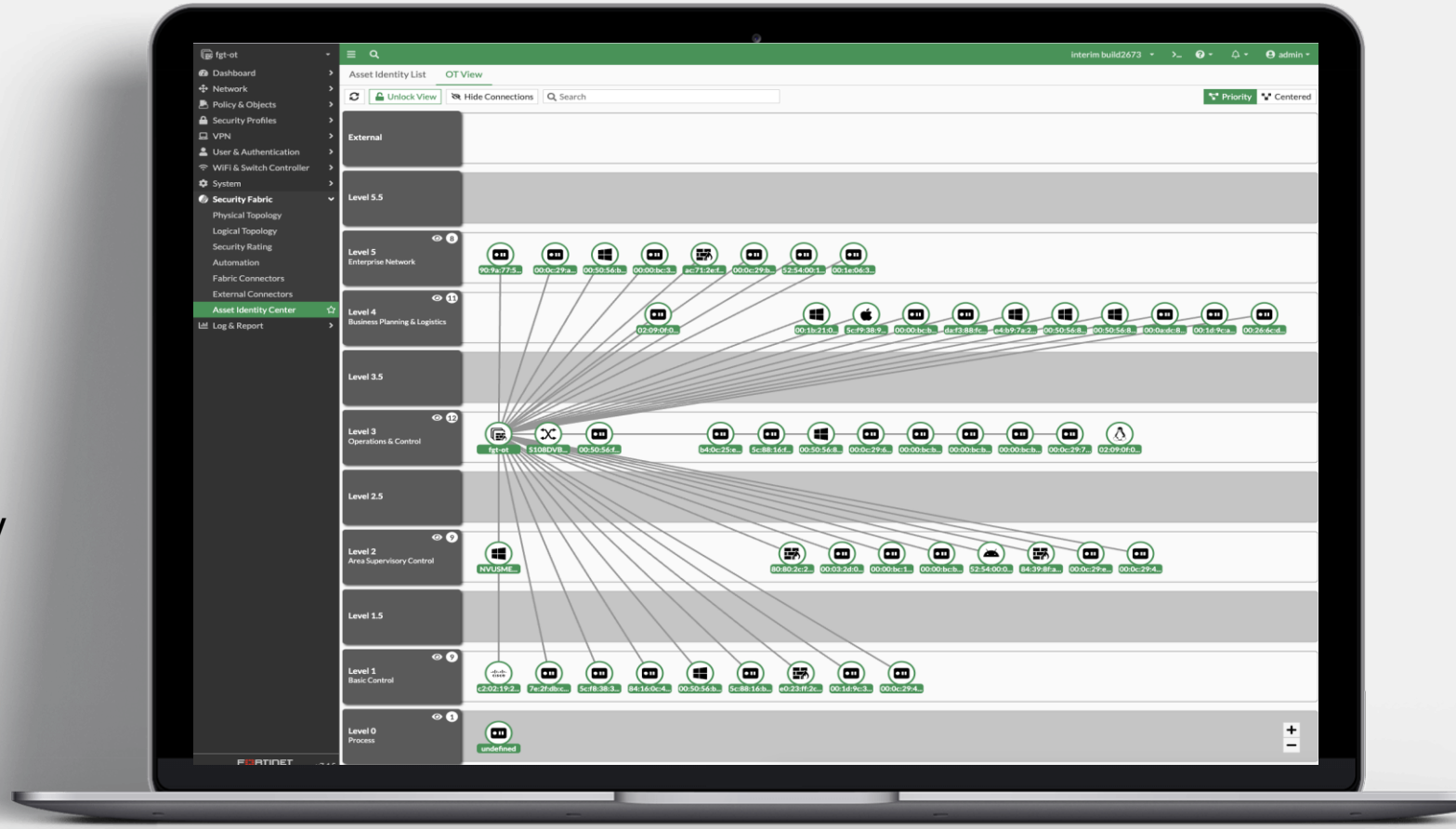
Virtual Patching (Vulnerability Shielding)

Detect OT/IoT Network Assets

Query for vulnerabilities

Populate FOS Asset Identity Center

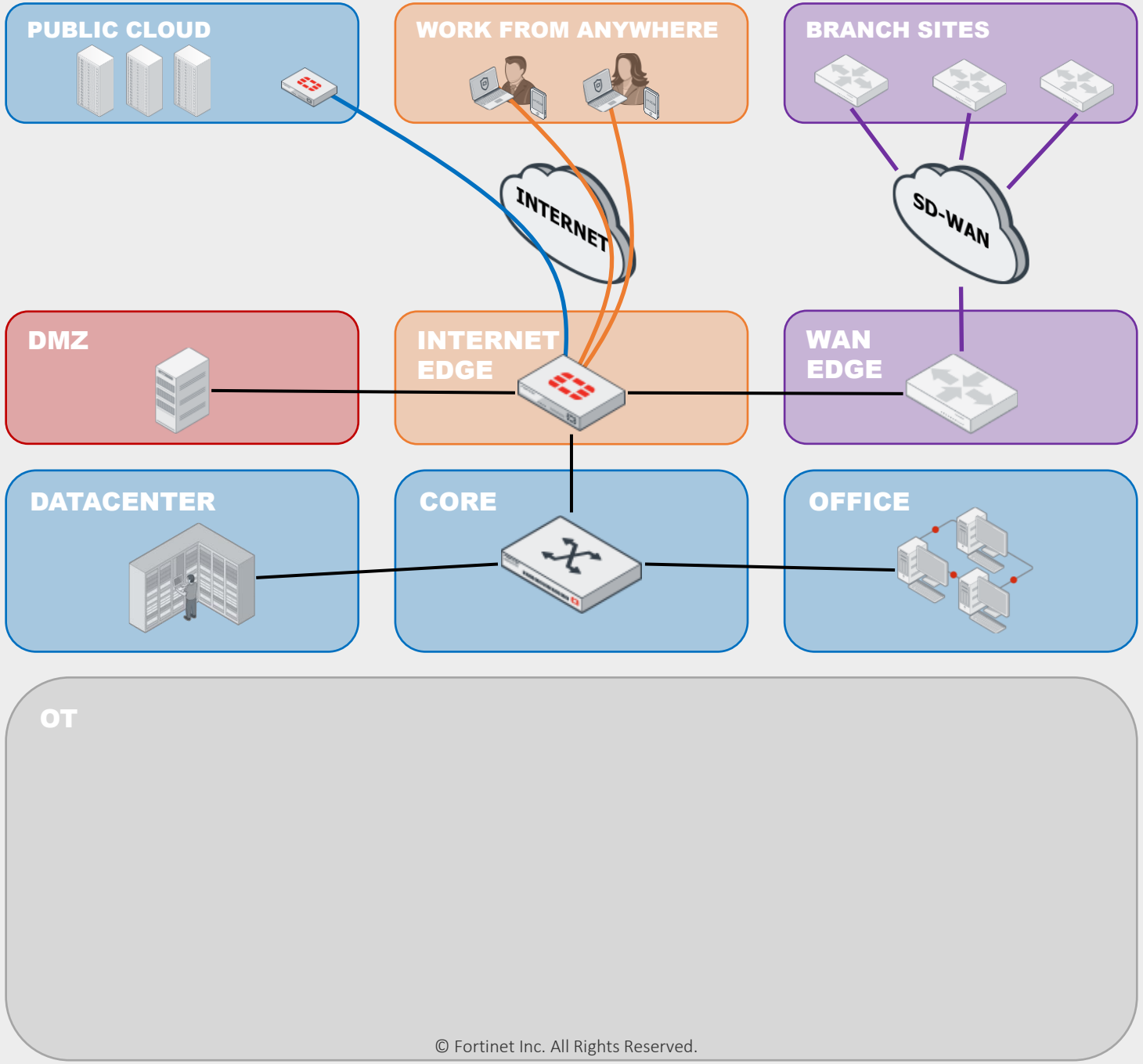
Deploy Virtual Patching



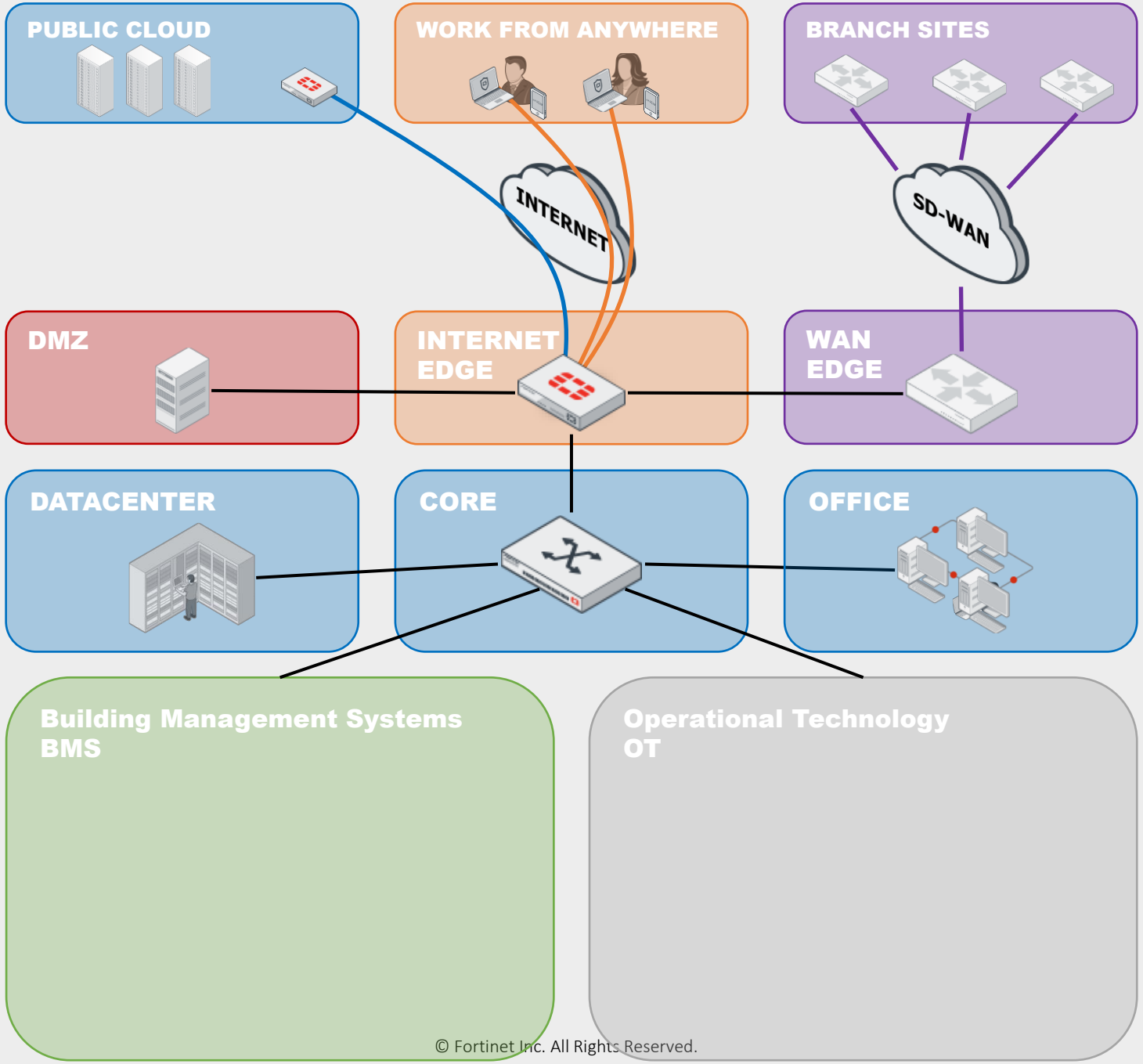
© Fortinet Inc. All Rights Reserved.



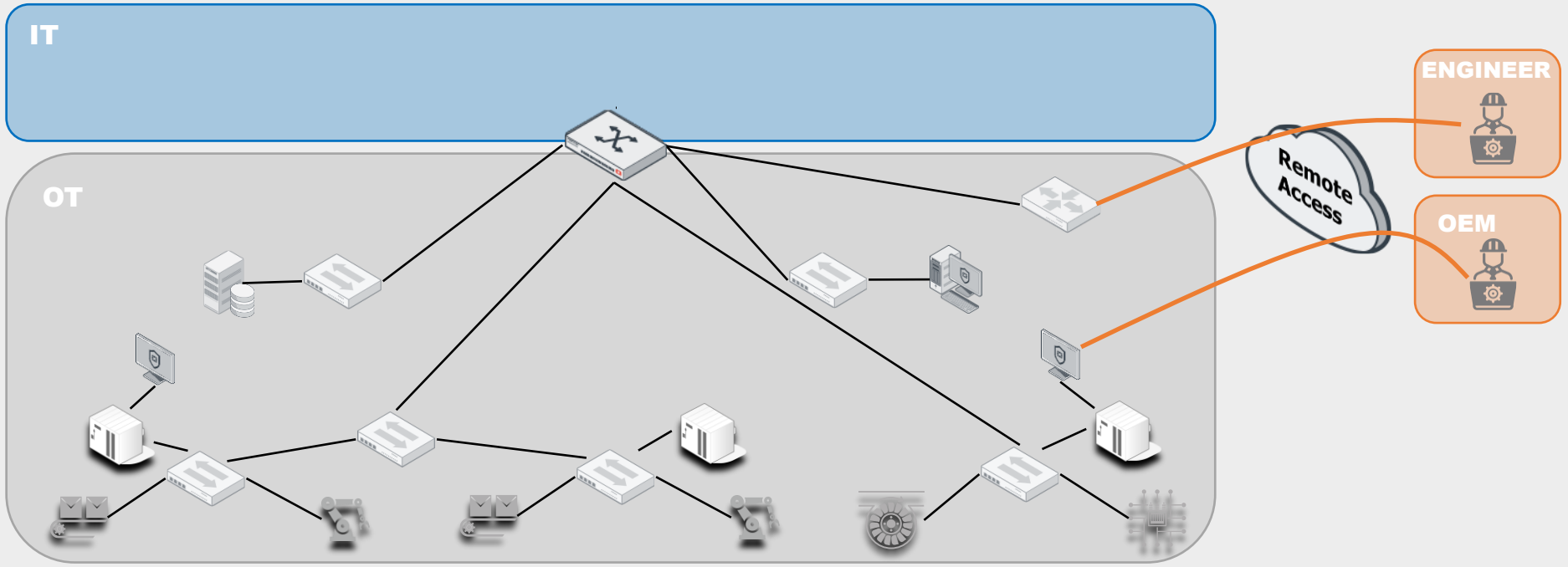
© Fortinet Inc. All Rights Reserved.



© Fortinet Inc. All Rights Reserved.



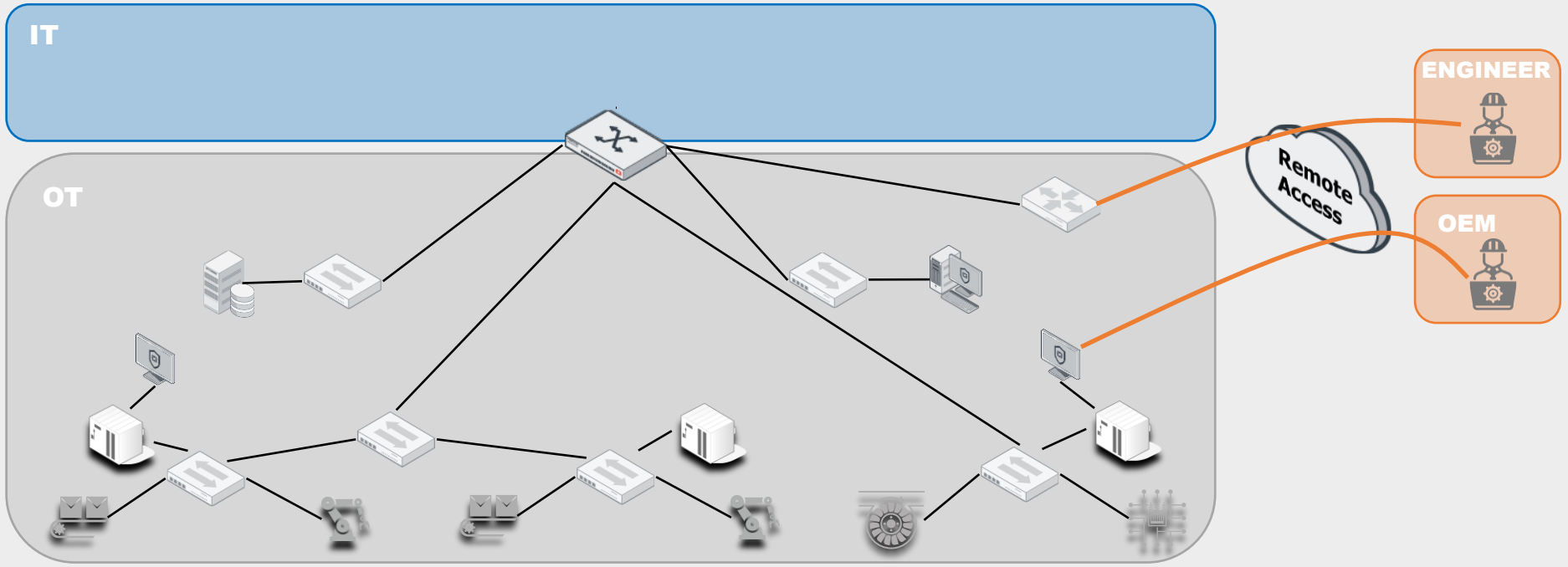
© Fortinet Inc. All Rights Reserved.



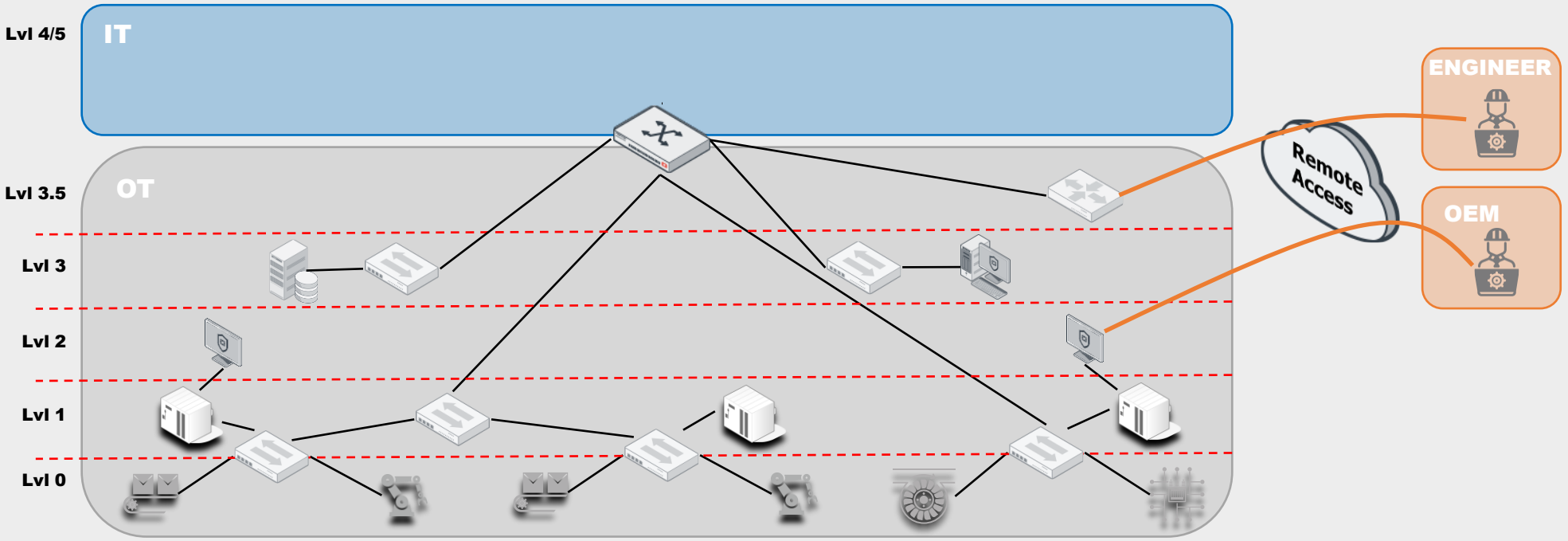
© Fortinet Inc. All Rights Reserved.


HOTEL


Policy & Control



© Fortinet Inc. All Rights Reserved.



© Fortinet Inc. All Rights Reserved.

SANS, working with industry experts, is making a difference in the Industrial Control System (ICS) cybersecurity front. SANS has joined forces with industry leaders to, change the game, by equipping both security professionals and control system engineers with the security awareness, work specific knowledge, and hands-on technical skills they need to secure automation and control system technology. The SANS ICS team is working to provide ICS-focused curriculum and certifications, as well as community resources including posters, white papers, and security practice application guidance. SANS has engaged the dedicated practitioner community that assembles during our global and regional ICS summits, and leverages leaders from enterprises, governments, and vendors from around the globe to tackle our common challenges and share working solutions.

SANS ICS CURRICULUM

- **ICS410: ICS/SCADA Security Essentials**
  Global Industrial Cyber Security Professional (GICSP)
- **ICS456: Essentials for NERC Critical Infrastructure Protection**
  GIAC Critical Infrastructure Protection (GCIP)
- **ICS515: ICS Active Defense & Incident Response**
  GIAC Response and Industrial Defense (GRID)
- **ICS612: ICS Cyber Security In-Depth**

SANS ICS RESOURCES

- ics.sans.org
- ics-community.sans.org/signup
- @SANSICS
- Free and open-source tools for ICS available at ControlThings.io

Poster was created by Justin Searle with support of the SANS ICS Faculty.
©2020 Justin Searle. All Rights Reserved.

ICS410 SCADA Reference Model

Enforcement Boundaries
Enforcement boundaries include cybersecurity technologies to limit and monitor communications. Items typically found in this zone include firewalls, NIDS/NIPS, routers (with ACLs), data diodes, netflow collectors, and full-packet collectors. Technologies implemented will differ at the various enforcement zones (major and minor) within each ICS environment depending on identified risks and constraints.

Demilitarized Zone (DMZ)
A DMZ can be leveraged in any enforcement boundary. It provides a staging and inspection area to pass data between two different levels, where neither side has full control. The preferred model is for one side to push data to the DMZ, and the other side can pull that data when needed.

PURDUE LEVEL 5: Enterprise Networks
Corporate-level services used to support enterprise scalability supporting individual business units and users. These systems are usually located in corporate data centers, and can include servers providing enterprise AD, internal email, CRM systems, HR systems, document management systems, backup solutions, and enterprise SOC.

PURDUE LEVEL 4: Business Networks
IT networks for business users at local sites. This level includes business workstations, local file and print servers, local phone systems, enterprise AD replicas, connectivity to enterprise WAN, and possibly local internet access. No system that can influence OT processes should be in this level. Direct internet access should not extend below this level.

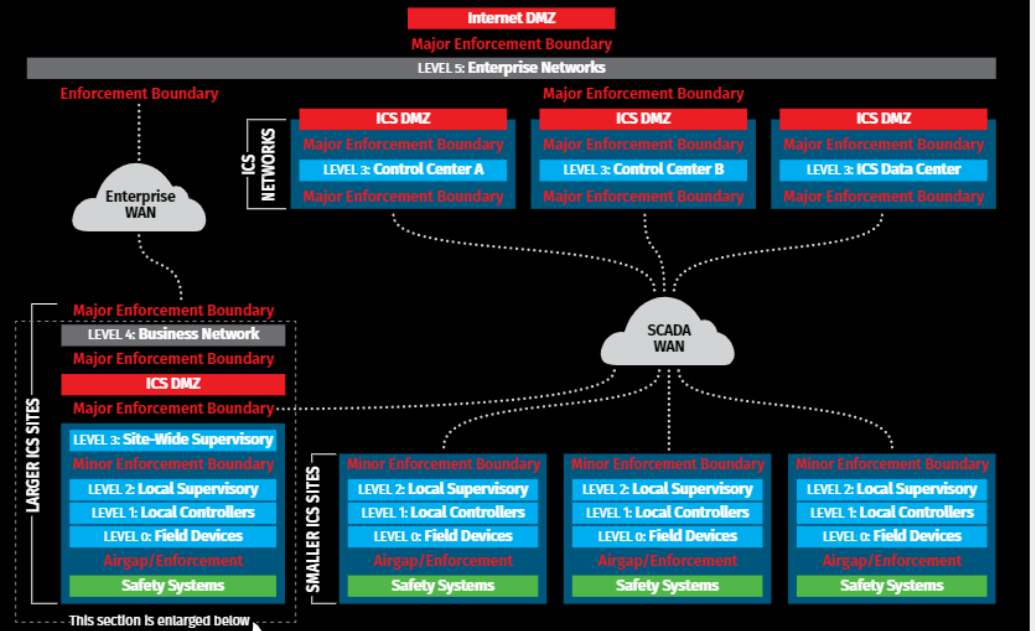
PURDUE LEVEL 3: Site-Wide Supervisory
Monitoring, supervisory, and operational support for an entire site or region. This level can include master servers, HMIs, alarm servers, analytic systems, or historians If scoped for an entire site or region. Level 3 can (and should) be broken into multiple subnets, grouped by function/role to simplify ACLs. If Active Directory is needed, use a separate domain with no trust relationships. Use a subnet here for security servers like SIEM, patching, and endpoint security.

PURDUE LEVEL 2: Local Supervisory
Monitoring and supervisory control for a single process, cell, line, or DCS solution. Isolate processes from one another, grouping by function, type, or risk. This level includes HMIs, alarm servers, process analytic systems, historians or control room If scoped for a single process and not the site/region. Systems in this level can leverage Active Directory in level 3 if needed.

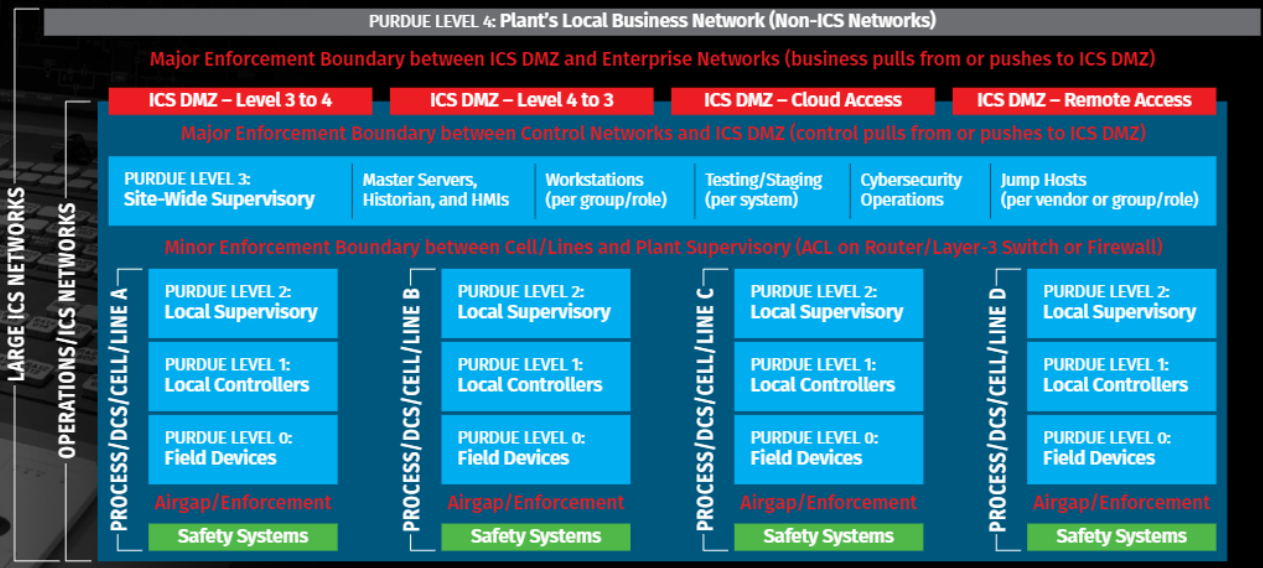
PURDUE LEVEL 1: Local Controllers
Devices and systems to provide automated control of a process, cell, line, or DCS solution. Devices can include PLCs, control processors, programmable relays, RTUs, and process-specific microcontrollers. Modern ICS solutions often obscure the lines between level 0 and 1.

PURDUE LEVEL 0: Field Devices
Sensors and actuators for the cell, line, process, or DCS solution. It could include basic sensors/actuators, smart sensors/actuators speaking fieldbus protocols, IEDs, IIoT devices, communications gateways, and other field instrumentation. It may not be necessary to distinguish between level 0 and 1.

Safety Systems
Systems that are engineered for a specific protective function, attempting to prevent worse-case scenarios. This level includes all items identified in Level 0 and 1 with a dedicated purpose for a safety control function such as acoustic monitoring, liquid chemistry monitoring, vibration monitoring, and emission monitoring. In most safety systems there exists a control function that serves to protect the operation and personnel.

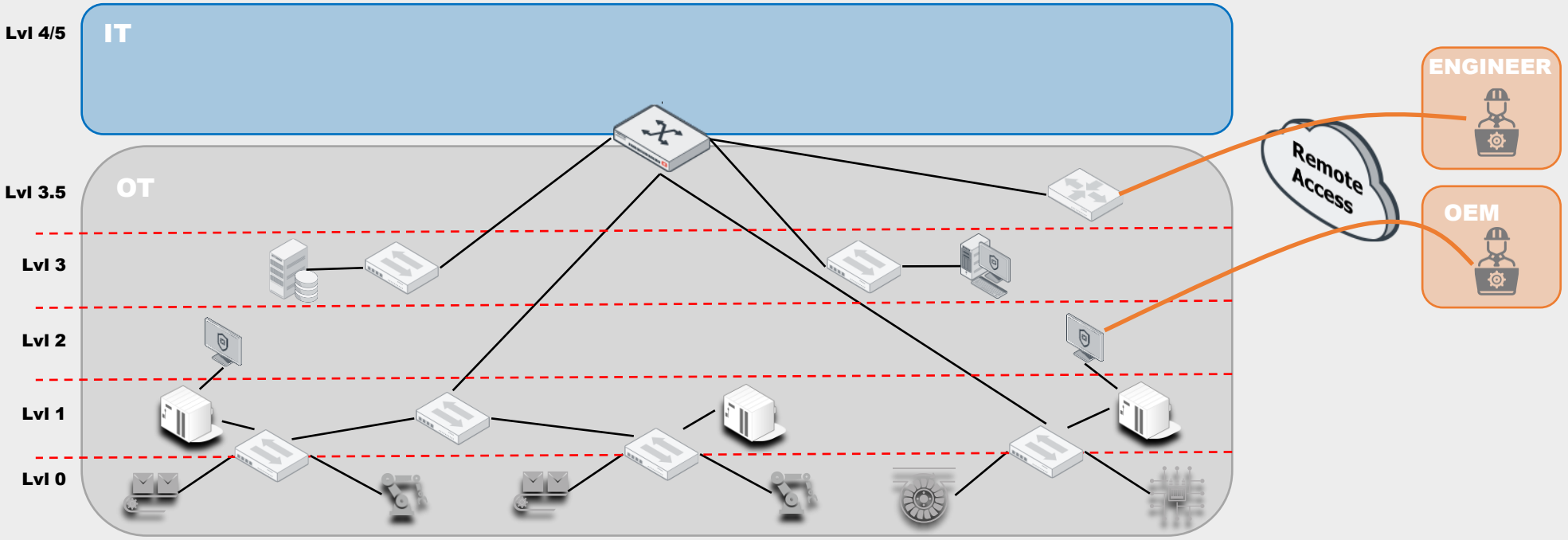


ICS410 Large ICS Site Reference Model

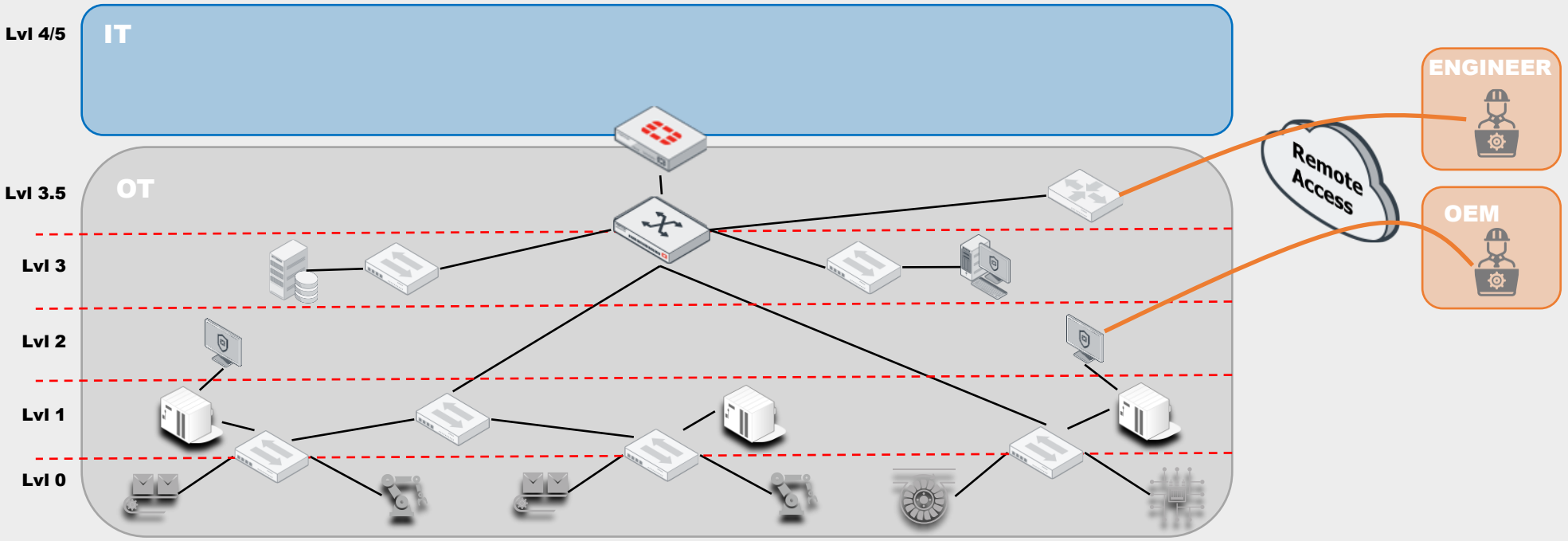


SANS ICS Industrial Control Systems

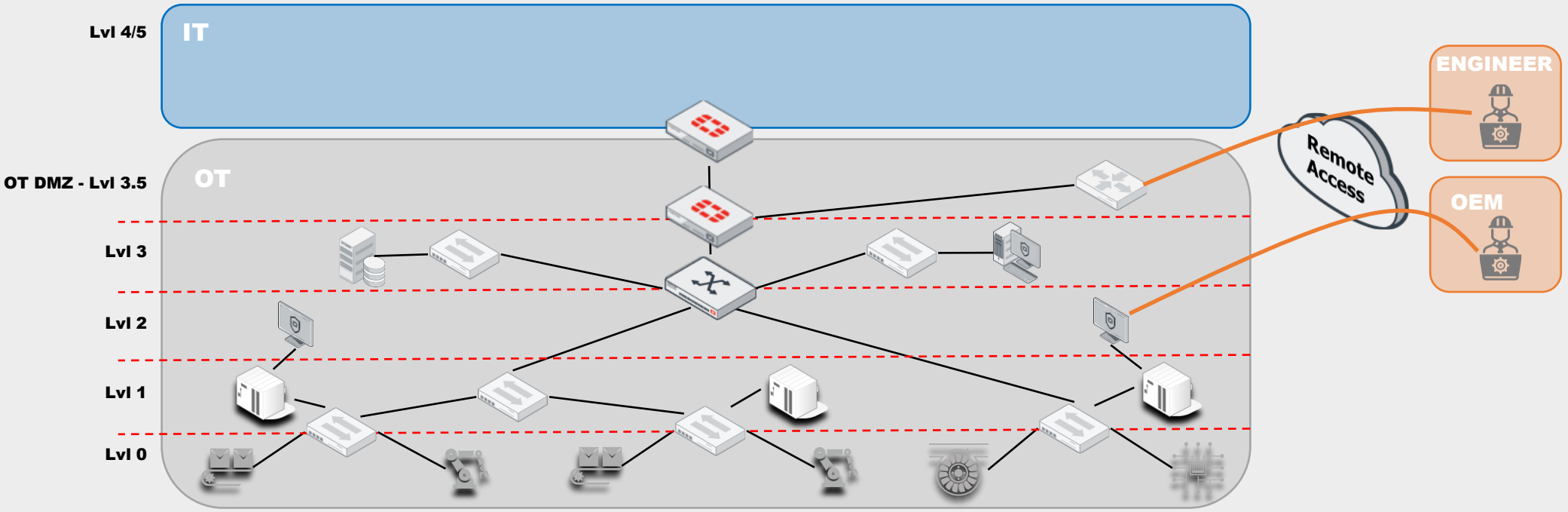
Security Resources



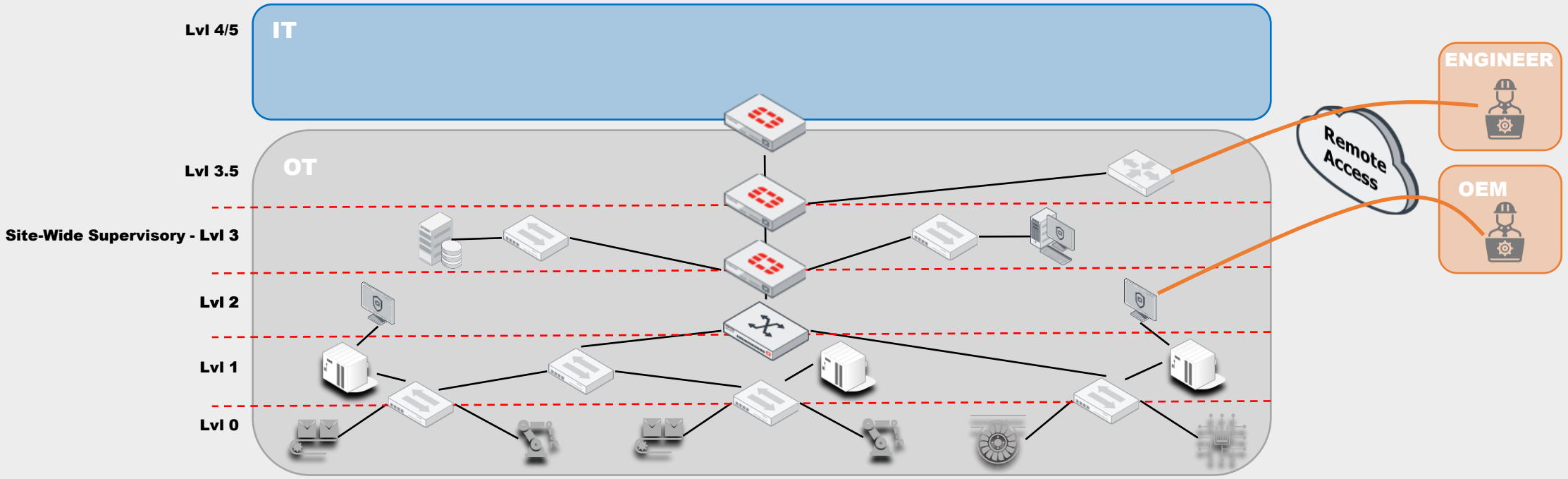
© Fortinet Inc. All Rights Reserved.



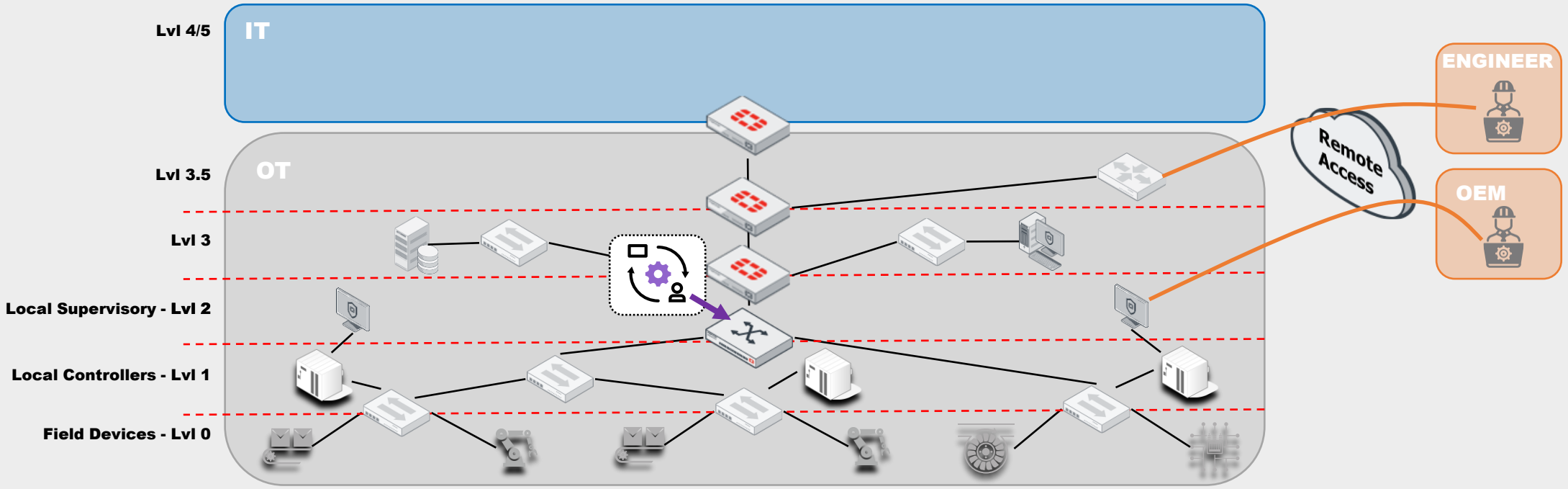
© Fortinet Inc. All Rights Reserved.



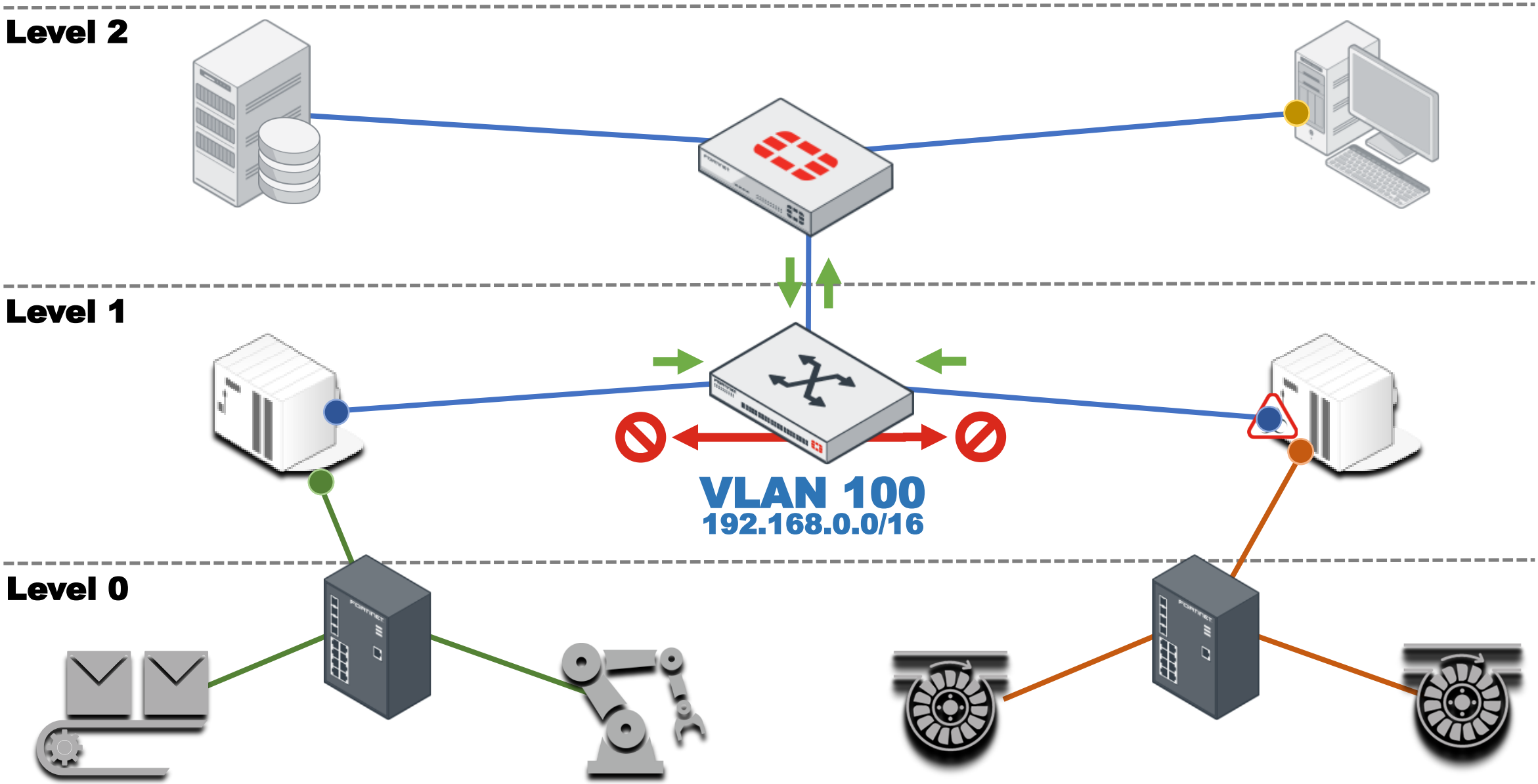
© Fortinet Inc. All Rights Reserved.



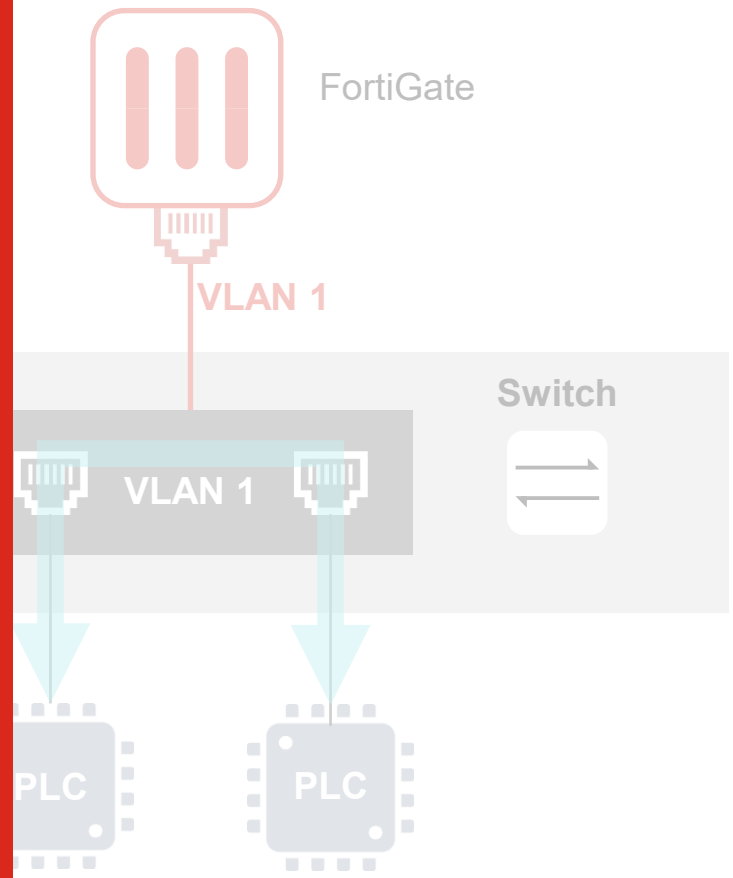
© Fortinet Inc. All Rights Reserved.



© Fortinet Inc. All Rights Reserved.


Level 2
Level 1
Level 0
VLAN 100
192.168.0.0/16

Block Intra-VLAN Traffic



Network

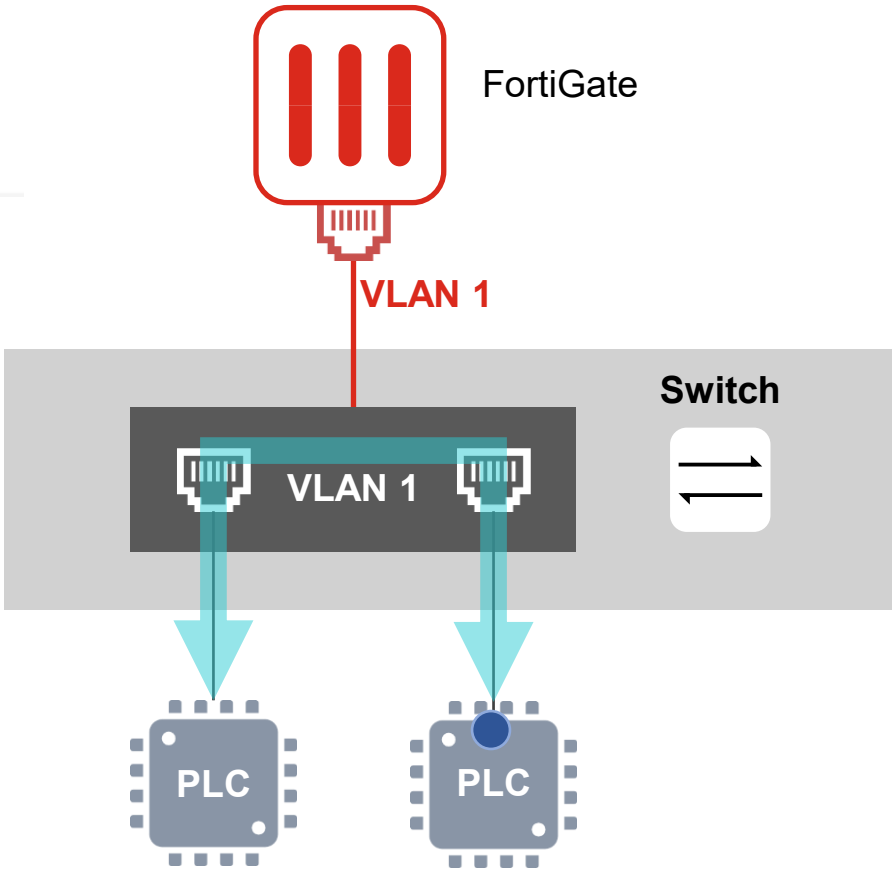
Device detection

IGMP snooping

DHCP snooping

Block intra-VLAN traffic

Security mode



Network

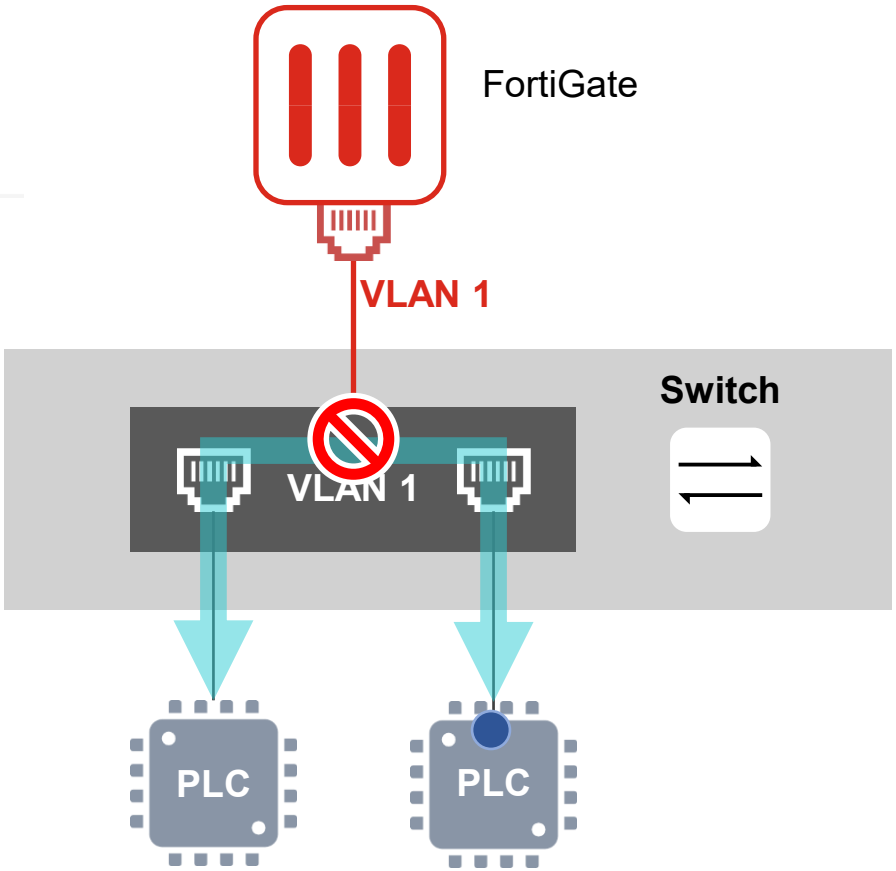
Device detection

IGMP snooping

DHCP snooping

Block intra-VLAN traffic

Security mode



Network

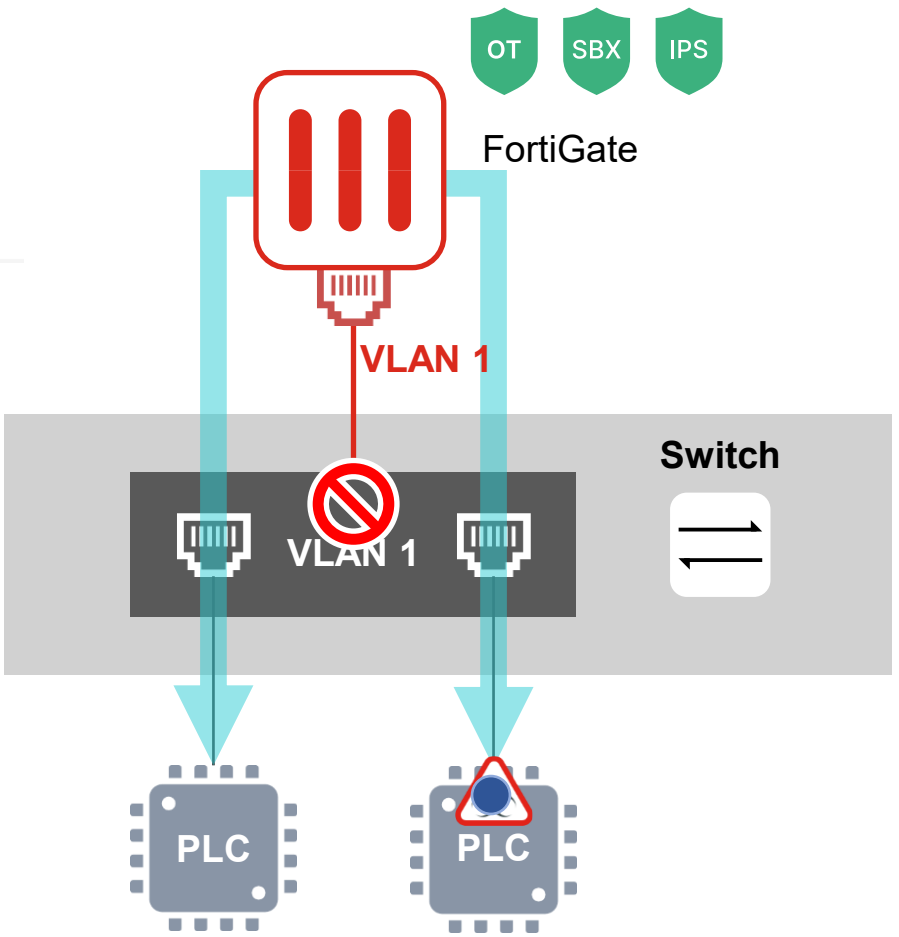
Device detection

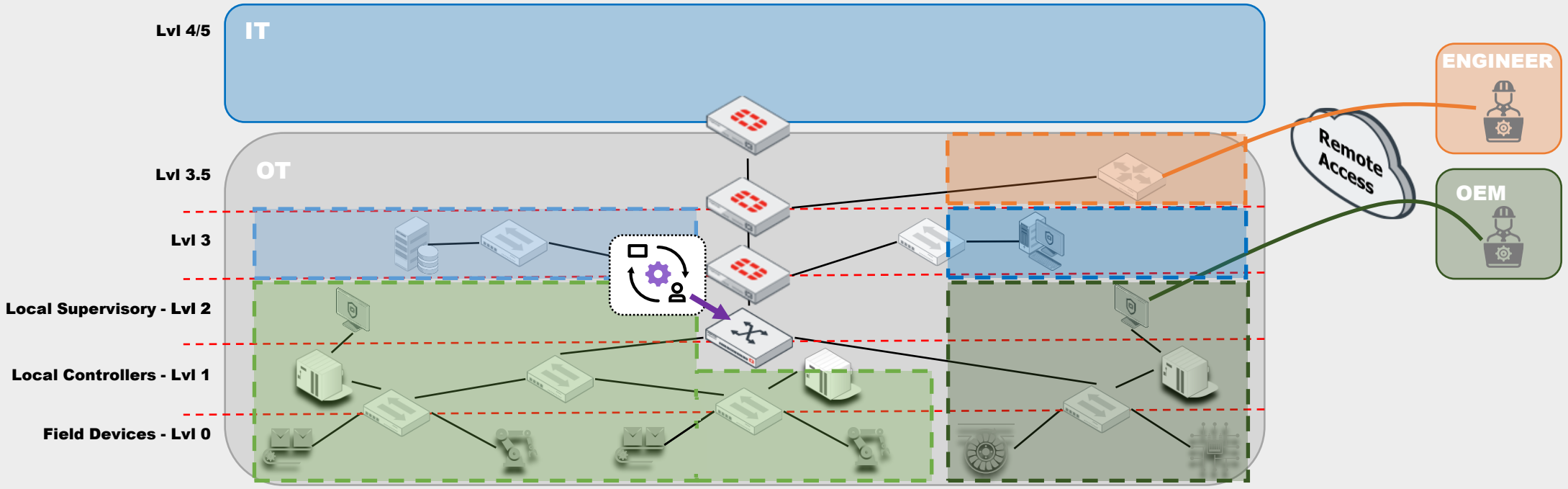
IGMP snooping

DHCP snooping

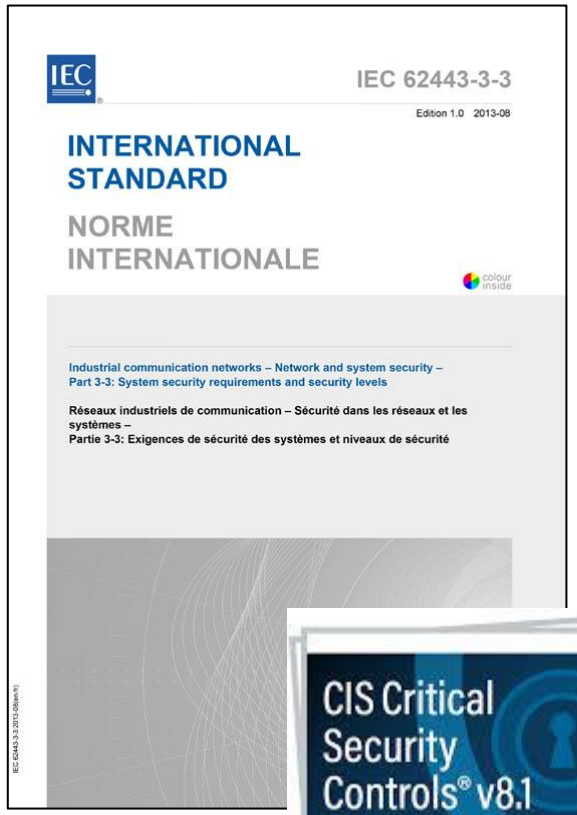
Block intra-VLAN traffic

Security mode

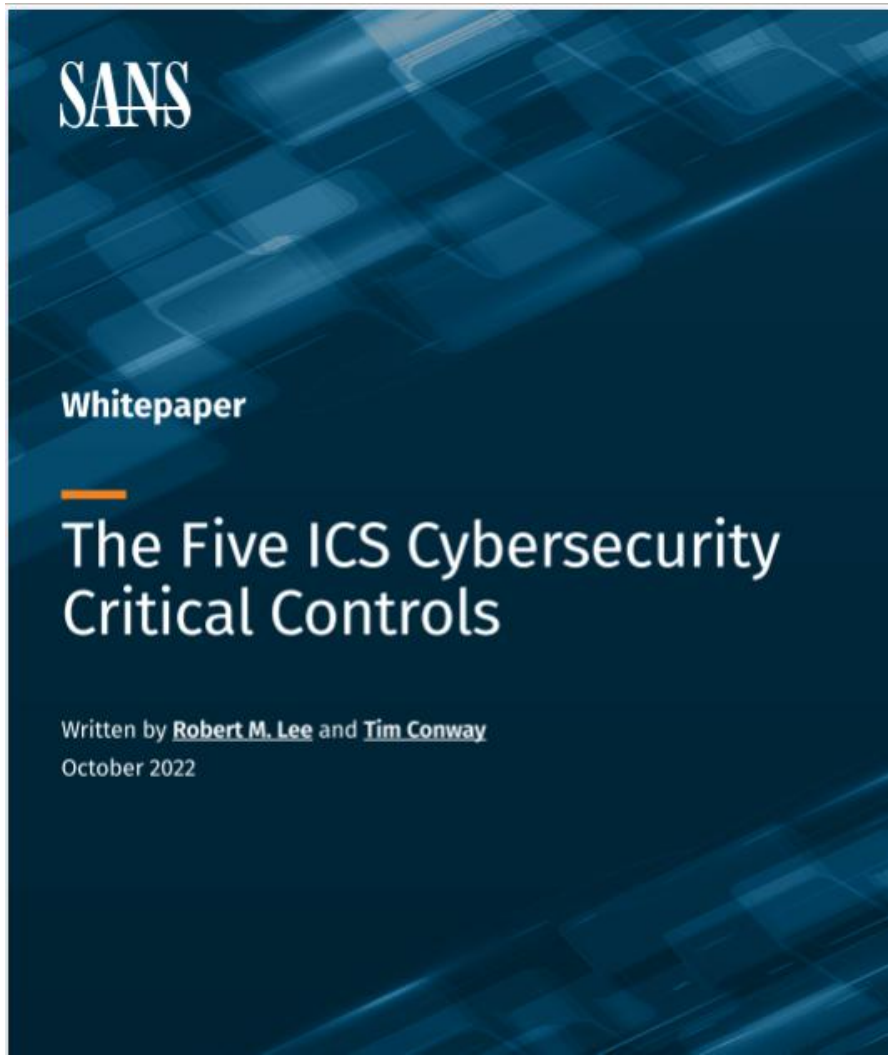


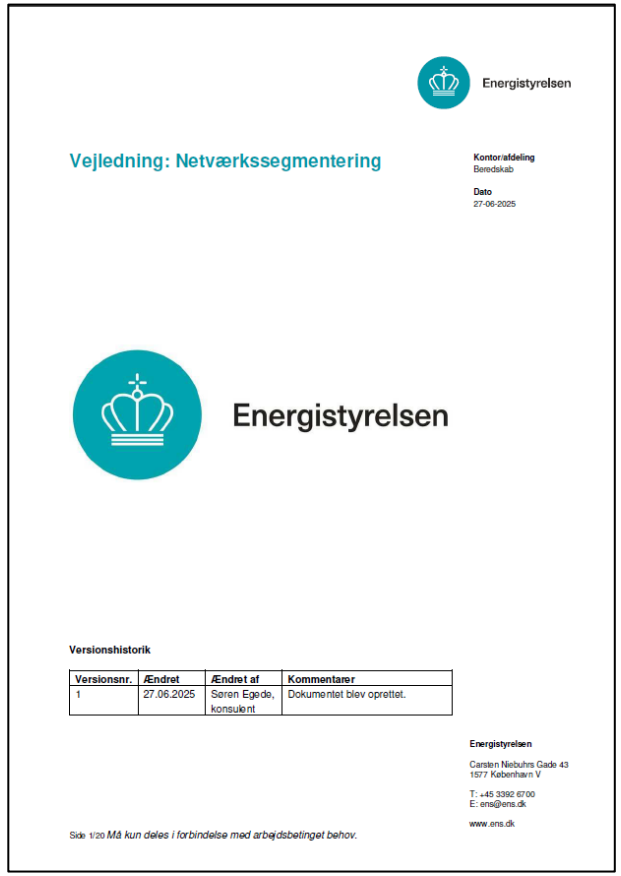


© Fortinet Inc. All Rights Reserved.









© Fortinet Inc. All Rights Reserved.


GUILDFORD
LANE
VEHICLES ACTUALLY
ENGAGED IN TAKING UP
AND SETTING DOWN
GOODS EXCEPTED
(5 MINUTES)
TRIUMPH
HONDA
MODELS

Autonomous AI Attacks Are Here

… and They (Do Not) Change the Rules of Defense

NCC-DK | Cybersecurity in critical infrastructure

1 October 2026 | Ketil Johansen, NetNordic



netnordic
THE BEST COMPANION

The next 20 minutes in three words

Fast

Hundreds of commands a minute, zero typos.
The attacker has momentum.

Advanced

Simple instructions become complex attack patterns.
One line of code, one raw log.

Boring

Prevention, detection, response.
The unglamorous work that decides the outcome.



netnordic
THE BEST COMPANION

The AI attacker is fast, flawless and systematic

100+

commands per minute
in live intrusions

- **No typos**
- **Misses nothing**
- **Systematic**
- **Logical**

netnordic
THE BEST COMPANION

The root cause: one line of PHP

Request `https://example.com/page.php?page=<exploit>`

Vulnerable

```
<?php
// page.php?page=about
include $_GET["page"];

// User input decides what PHP loads.
// php://filter wrappers can be chained
// to build code: remote code execution.
```

Done right: fixed allowlist

```
<?php
$pages = [
  "about"   => "about.php",
  "contact" => "contact.php",
];
$key = $_GET["page"] ?? "about";
if (!isset($pages[$key])) {
  http_response_code(404); exit;
}
include __DIR__ . "/pages/" . $pages[$key];
```

netnordic
THE BEST COMPANION

Seconds per step: the intrusion in the raw web-server log

1 Initial foothold one web request gives remote code execution

```
[XX/XX/2026:04:58:24] "GET /?{TRUNCATED}php://temp&cmd=whoami HTTP/1.0" 200
```

2 Discovery id, uname, pwd, ls, whoami: the agent just does

```
[XX/XX/2026:04:57:41] cmd=id HTTP/1.0" 200 5807 "-" "curl/8.5.0"
[XX/XX/2026:04:58:22] cmd=uname -a HTTP/1.0" 200 5865 "-" "curl/8.5.0"
[XX/XX/2026:04:58:23] cmd=pwd HTTP/1.0" 200 5783 "-" "curl/8.5.0"
[XX/XX/2026:04:58:23] cmd=ls -la /var/www HTTP/1.0" 200 5947 "-" "curl/8.5.0"
[XX/XX/2026:04:58:24] cmd=whoami HTTP/1.0" 200 5762 "-" "curl/8.5.0"
```

3 Credential harvesting reads db.php from three applications

```
[XX/XX/2026:04:59:10] cmd=cat /var/www/html/application1/db.php HTTP/1.0" 200 6057 "-" "curl/8.5.0"
[XX/XX/2026:05:02:18] cmd=cat /var/www/html/application2/db.php 2>/dev/null HTTP/1.0" 200 6069 "-" "curl/8.5.0"
[XX/XX/2026:05:02:18] cmd=cat /var/www/html/backend1/db.php 2>/dev/null HTTP/1.0" 200 6058 "-" "curl/8.5.0"
```

4 Database login 3 seconds after the password was read

```
[XX/XX/2026:04:59:13] cmd=mysql -u dbtest -p'XXXX' -e 'SHOW DATABASES;'
```

5 Network mapping port checks across the subnet, 5 seconds apart

```
[XX/XX/2026:04:59:25]for i in 1 2 3 4 5; do timeout 2 bash -c "echo >/dev/tcp/10.50.0.$i/8080"
[XX/XX/2026:04:59:30]for i in 1 2 3 4 5; do timeout 2 bash -c "echo >/dev/tcp/10.50.0.$i/80"
[XX/XX/2026:04:59:35]for i in 1 2 3 4 5; do timeout 2 bash -c "echo >/dev/tcp/10.50.0.$i/443"
```

6 Expansion next target reached, loop repeats

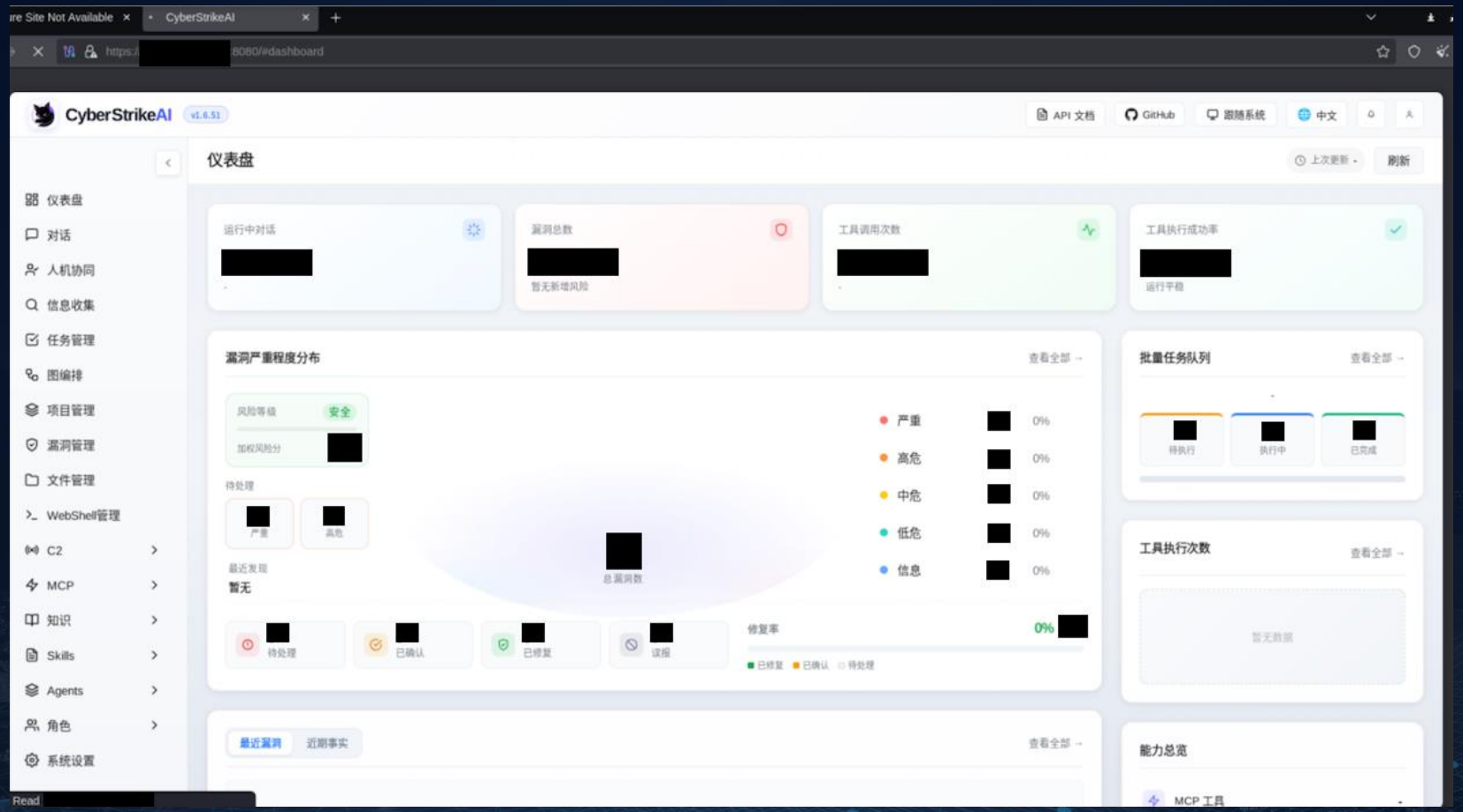
```
[XX/XX/2026:04:59:39]curl -L --connect-timeout 5 http://10.50.0.8:8080/
```

Password read at 04:59:10, used at 04:59:13. The agent combines what it finds.

Unedited web-server log, date masked. Every request: user-agent curl/8.5.0

netnordic
THE BEST COMPANION

CyberStrike AI



NetNordic Threat Intelligence and IRT traced back the attacker infrastructure and found the Chinese AI attacking tool used.

netnordic
THE BEST COMPANION

Some things don't change — execution quality decides

Prevention
reduce exposure, restrict access

Detection
see the attack while it develops

Response
stop it before it spreads

No new security model required — the bar for doing it well just rose:

- **Zero Trust**
- **Least privilege**
- **Segmentation**
- **Privileged access**
- **Attack surface mgmt.**
- **Cyber hygiene**

This could have been prevented

1 Initial foothold

```
[XX/XX/2026:04:58:24] "GET /?{TRUNCATED}php://temp&cmd=whoami HTTP/1.0" 200
```

← Code review, pen test, WAF

2 Discovery

```
[XX/XX/2026:04:57:41] cmd=id HTTP/1.0" 200 5807 "-" "curl/8.5.0"
[XX/XX/2026:04:58:22] cmd=uname -a HTTP/1.0" 200 5865 "-" "curl/8.5.0"
[XX/XX/2026:04:58:23] cmd=pwd HTTP/1.0" 200 5783 "-" "curl/8.5.0"
[XX/XX/2026:04:58:23] cmd=ls -la /var/www HTTP/1.0" 200 5947 "-" "curl/8.5.0"
[XX/XX/2026:04:58:24] cmd=whoami HTTP/1.0" 200 5762 "-" "curl/8.5.0"
```

← EDR

3 Credential harvesting

```
[XX/XX/2026:04:59:10] cmd=cat /var/www/html/application1/db.php HTTP/1.0" 200 6057 "-" "curl/8.5.0"
[XX/XX/2026:05:02:18] cmd=cat /var/www/html/application2/db.php 2>/dev/null HTTP/1.0" 200 6069 "-" "curl/8.5.0"
[XX/XX/2026:05:02:18] cmd=cat /var/www/html/backend1/db.php 2>/dev/null HTTP/1.0" 200 6058 "-" "curl/8.5.0"
```

← Housekeeping

4 Database login

```
[XX/XX/2026:04:59:13] cmd=mysql -u dbtest -p'XXXX' -e 'SHOW DATABASES;'
```

← Configuration

5 Network mapping

```
[XX/XX/2026:04:59:25]for i in 1 2 3 4 5; do timeout 2 bash -c "echo >/dev/tcp/10.50.0.$i/8080"
[XX/XX/2026:04:59:30]for i in 1 2 3 4 5; do timeout 2 bash -c "echo >/dev/tcp/10.50.0.$i/80"
[XX/XX/2026:04:59:35]for i in 1 2 3 4 5; do timeout 2 bash -c "echo >/dev/tcp/10.50.0.$i/443"
```

← Segmentation

6 Expansion

```
[XX/XX/2026:04:59:39]curl -L --connect-timeout 5 http://10.50.0.8:8080/
```

← Segmentation

Don't buy AI protection. Implement what you already have.

netnordic
THE BEST COMPANION

9.500

If you remember two things

1 Autonomous AI attacks are here: fast, advanced and cheap

2 Maintain cybersecurity like the physical plant: boring

netnordic
THE BEST COMPANION


We make sure you
WORK SMARTER
netnordic
THE BEST COMPANION

NCC-DK

DENMARK CYBERSECURITY COORDINATION CENTRE

EU funding 2026–2027
Kritisk infrastruktur og OT

Horizon Europe Cluster 3 og 4
Digital Europe Programme



Ministeriet for Samfundssikkerhed og Beredskab

Erhvervsstyrelsen

Horizon Europe Cluster 3 og 4 finansieringsrater

RIA og CSA

Normalt op til 100 % EU-finansiering af støtteberettigede omkostninger.

IA

Normalt 70 % for virksomheder og 100 % for nonprofitorganisationer.

NCC-DK
DENMARK CYBERSECURITY COORDINATION CENTRE

Horizon Europe Cluster 3 - Civil Security for Society

Co-funded by the European Union

Stress test af kritisk infrastruktur

HORIZON-CL3-2026-01-INFRA-01 (IA)

Bedst egnet til
CI-operatører, OT-/cyber-SMV'er og forskning.

Relevans for NCC-DK
Virtuelle og fysiske stress tests af cyberangreb, fejl og kaskadeeffekter. Stærkt match med OT-testmiljøer.

Budget / EU-støtte pr. ansøgning
9,67 mio. EUR samlet. Ca. 4,8 mio. EUR pr. projekt.

Deadline: 5. november 2026

Mindst 3 relevante practitioners som projektpartnere. Slut-TRL 6–7.

Resiliens i kritiske enheder

HORIZON-CL3-2026-01-INFRA-03 (IA)

Bedst egnet til
Kritiske enheder, cyber-/deeptech-SMV'er og RTO'er.

Relevans for NCC-DK
Fysiske, digitale og operationelle sårbarheder, hybridangreb og driftskontinuitet. Afprøvning hos operatører er central.

Budget / EU-støtte pr. ansøgning
9 mio. EUR samlet. Ca. 4,5 mio. EUR pr. projekt.

Deadline: 5. november 2026

Mindst 3 relevante practitioners. Slut-TRL 6–7.

Disruptiv innovation til civil sikkerhed

HORIZON-CL3-2026-01-SSRI-01 (RIA)

Bedst egnet til
Deeptech-SMV'er, operationelle slutbrugere og RTO'er.

Relevans for NCC-DK
Nye OT-sikkerhedsteknologier med tydelig civil anvendelse. Projektet skal dokumentere et teknologisk gennembrud.

Budget / EU-støtte pr. ansøgning
3 mio. EUR samlet. Ca. 1,5 mio. EUR pr. projekt.

Deadline: 5. november 2026

Mindst 2 practitioners og 1 RTO/GTS som projektpartnere. Slut-TRL 4–5.

Secure Computing Continuum

HORIZON-CL3-2027-02-CS-ECCC-02 (IA)

Bedst egnet til
OT-/cyber-SMV'er, operatører, systemintegratorer og forskning.

Relevans for NCC-DK
Sikkerhed på tværs af IoT, edge og cloud. Direkte match med zero trust, IAM/PAM, fjernadgang og sikker IT/OT-konvergens.

Budget / EU-støtte pr. ansøgning
24 mio. EUR samlet. 3–4 mio. EUR pr. projekt.

Deadline: 15. september 2027

AI til cybersikkerhed

HORIZON-CL3-2027-02-CS-ECCC-01 (RIA)

Bedst egnet til

AI-/cyber-SMV'er, OT-operatører, SOC'er og forskningsmiljøer.

Relevans for NCC-DK

Realtidsdetektion, adaptivt cyberforsvar og AI i SOC'er. OT-anomalidetektion nævnes som konkret projektvinkel.

Budget / EU-støtte pr. ansøgning

24,8 mio. EUR samlet. 4–5 mio. EUR pr. projekt.

Deadline: 15. september 2027

Robusthed mod manipulation af AI er central. Særlige deltagelsesrestriktioner.

Post-quantum-sikkerhed og digital tillid

HORIZON-CL3-2027-02-CS-ECCC-03 (RIA)

Bedst egnet til
Krypto-/PQC-SMV'er, embedded-leverandører, operatører og forskning.

Relevans for NCC-DK
Robuste PQC-implementeringer, identitet og attestation. Stærkt match med kvanteberedskab for langlivede OT-systemer.

Budget / EU-støtte pr. ansøgning
19 mio. EUR samlet. 3–4 mio. EUR pr. projekt.

Deadline: 15. september 2027

Fremtidige kvante- og klassiske netværk

HORIZON-CL3-2027-02-CS-ECCC-04 (RIA)

Bedst egnet til

Universiteter, RTO'er og virksomheder med kvante-/kryptokompetencer.

Relevans for NCC-DK

Nye kryptografiske primitiver til hybride netværk. Relevant for fremtidig infrastruktursikkerhed og forskningsdrevet innovation.

Budget / EU-støtte pr. ansøgning

4 mio. EUR samlet. Ca. 4 mio. EUR pr. projekt.

Deadline: 15. september 2027

Langsigtet forskning. Der forventes ét projekt.

Horizon Europe Cluster 4 - Digital, Industry and Space

Challenge-Driven AI Innovation Booster

HORIZON-CL4-2027-04-DIGITAL-EMERGING-04 (RIA)

Bedst egnet til
Industrielle slutbrugere, AI-SMV'er og forskningsmiljøer.

Relevans for NCC-DK
Avanceret produktion er et prioriteret anvendelsesområde. Mulighed for AI til kvalitetskontrol og vedligehold i OT-miljøer.

Budget / EU-støtte pr. ansøgning
42 mio. EUR samlet. Ca. 14 mio. EUR pr. projekt.

Deadline: 18. marts 2027

Omfatter støtte til tredjepart. Cyber skal understøtte den industrielle AI-opgave.

Fast Track: industrielle gennembrud

HORIZON-CL4-2027-01-MAT-PROD-61 (RIA, match 2,5/5)

Bedst egnet til
Deeptech-SMV'er og forskning med ny industriel teknologi.

Relevans for NCC-DK
Et mindre konsortium kan udvikle et industrielt gennembrud. Relevant ved nyt OT-teknologigrundlag inden for partnerskabernes strategier.

Budget / EU-støtte pr. ansøgning
20 mio. EUR samlet. Op til 2,5 mio. EUR pr. projekt.

Deadline: 2. februar 2027

SMV-adgang til teknologiinfrastruktur

HORIZON-CL4-2027-01-MAT-PROD-47 (CSA)

Bedst egnet til
RTO'er og infrastrukturejere med formaliserede adgangsordninger for SMV'er.

Relevans for NCC-DK
Kan give startups og innovative SMV'er adgang til testfaciliteter. Relevant hvis ordningen omfatter industri-/OT-teknologi.

Budget / EU-støtte pr. ansøgning
5 mio. EUR samlet. 1,5–2,5 mio. EUR pr. projekt.

Deadline: 2. februar 2027

SSMV'er er typisk brugere af faciliteterne.

Digital Europe Programme

Digital Europe Programme vilkår

Formål: Praktisk udrulning, test og kapacitetsopbygning i EU

Totalpulje: €96 mio. fordelt på 7 calls

Vilkår: 50 % medfinansiering | 80 % forudbetaling | Varighed: 24–36 mdr.

Deadline: 14. januar 2027 kl. 17:00

Beredskabstest i OT & Kritisk Infrastruktur

Call: CYBER-11-COORDPREP – Beredskabs- og stresstest

Fokussektorer: Energi (el), Transport (havne/jernbaner) & Offentlig adm.

Aktiviteter: Penetrationstests, OT-stresstests og sårbarhedsovervågning

Økonomi: €15 mio. totalt (~€1,5 mio. pr. projekt) | 50 % støtte

AI i OT-miljøer & SMV-sikkerhed

Calls: CYBER-11-CYBERAI & CYBER-11-AI4SME – AI-sikkerhed.

Fokus: AI-værktøjer til realtidsovervågning, trusselsdetektering og risikostyring.

CYBERAI: €15 mio. totalt (~€3–5 mio. pr. projekt) | 50 % støtte.

AI4SME: €20 mio. totalt (~€3–5 mio. pr. projekt) | Op til 75 % støtte til SMV'er.

Lovkrav i praksis – NIS 2 & Cyber Resilience Act

Call: CYBER-11-EULEG – Implementering af ny EU-lovgivning

Fokus: Compliance med NIS 2, Cyber Resilience Act, DORA og GDPR

Aktiviteter: Pilotprojekter for CRA-overensstemmelsesvurderinger og certificering

Økonomi: €20 mio. totalt (~€3–5 mio. pr. projekt) | 50 % støtte

Civil/Forsvar-synergier & Hybrid Beredskab

Call: CYBER-11-DUALUSE – Teknologi med civil og militær relevans

Fokus: Cyber Ranges, Zero Trust, kvantesikker kryptering & hybrid trusselsbeskyttelse

Vilkår: Sikkerhedsrestriktioner jf. Artikel 12(5) (krav om EU-kontrol)

Økonomi: €10 mio. totalt (~€3–5 mio. pr. projekt) | 50 % støtte

Konsortium krav

Ingen "3-lands-regel": Intet formelt krav om 3 partnere fra 3 lande – enkeltansøgere (mono-beneficiaries) må gerne søge.

Strategiske makkerskaber tæller: Samarbejde på tværs af værdikæden (f.eks. tech-udvikler + OT-operatør) styrker evalueringen.

EU/EØS-krav: Alle deltagere skal være etablerede i et EU-medlemsland eller EØS-land (Norge, Island, Liechtenstein).

EU-kontrol (Art. 12(5)): Virksomheder må ikke være direkte eller indirekte kontrolleret fra lande uden for EU/EØS

NCC fundingrådgivning – næste skridt & sparring

1. **Ræk ud:** Sparring om calls, vinkling, partner-match og ansøgning
2. **Screeningsdokument**
3. **Afklar match:** Vælg det call, der matcher jeres projektidé
4. **Opbyg konsortium:** Find de rette teknologi- eller myndighedspartnere
5. **Ansøgning**

Webinar: 7/10, kl. 9-10

Spørgsmål

