Jens Berthelsen

www.linkedin.com/in/bertelsenjens

Senior Cyber Security & Trust Advisor | ISO9001 & ISO27001 Lead Auditor - Dubex

TLF. 31560318

Mail jbe@dubex.dk

Jens Lindskov Vestergaard

www.linkedin.com/in/jens-l-vestergaard

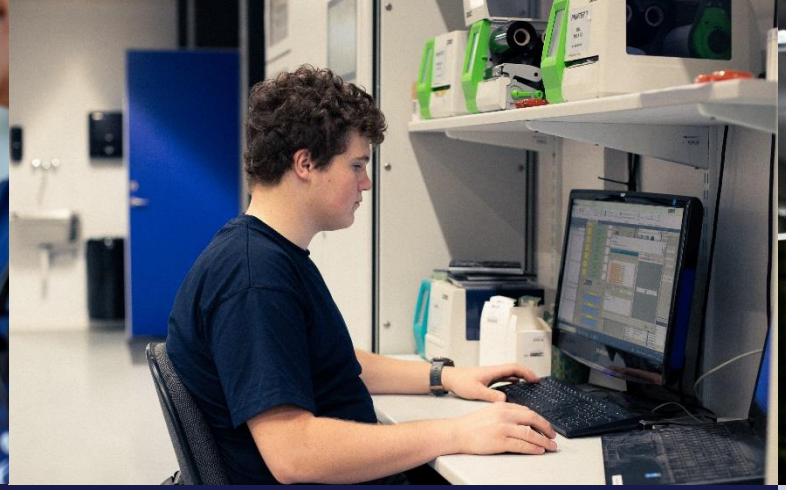
Afdelingsleder - Holtec

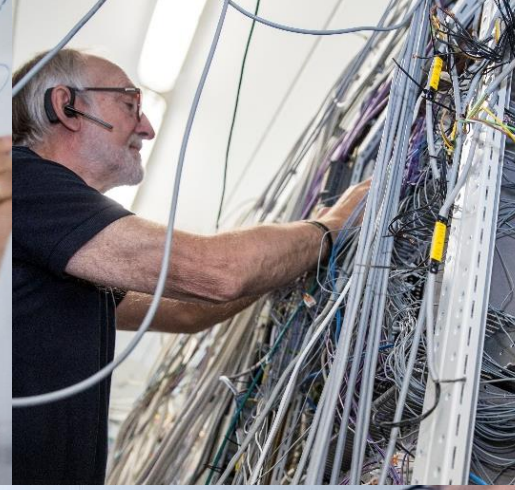
TLF. 91890572

Mail jlv@holtec.dk

Dubex:

HOLTEC.DK®

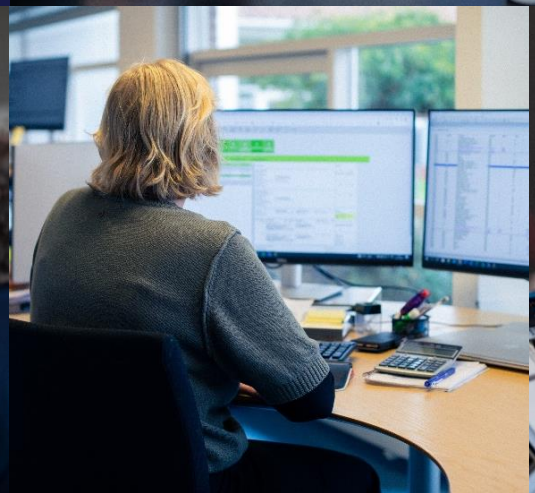
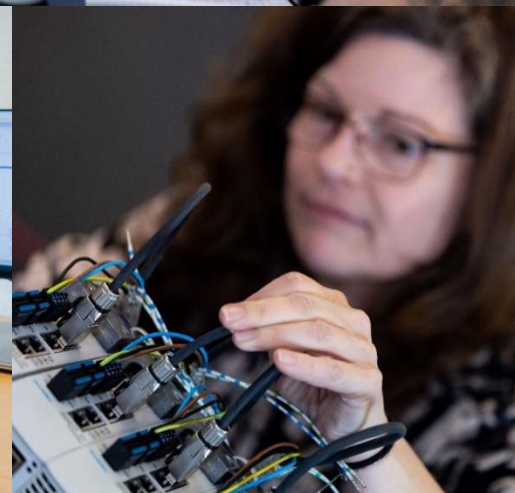





HOLTEC.DK®

Din professionelle partner i industriel automation og IT



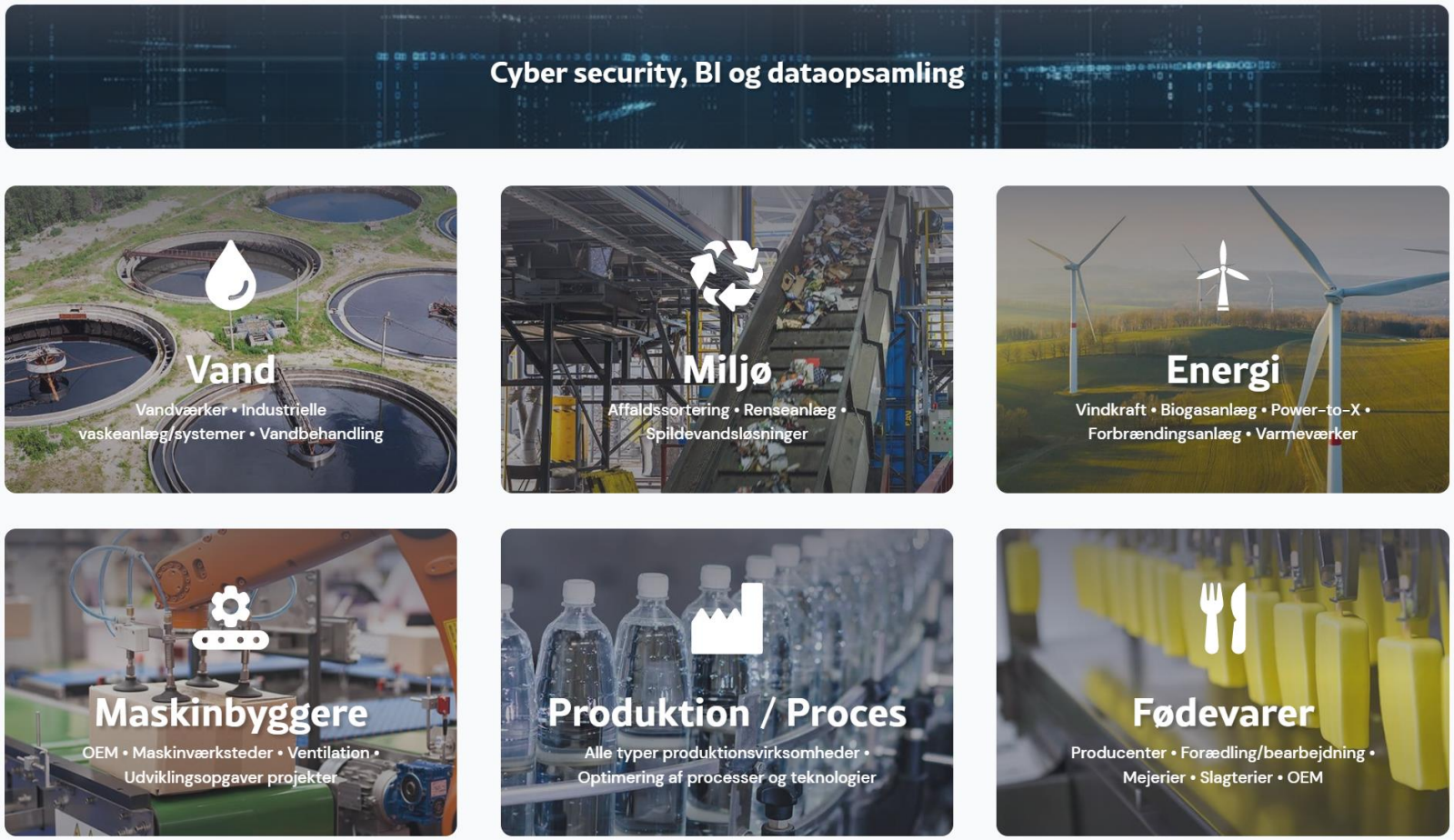
HOLTEC gruppen

- VI HAR 10 AFDELINGER I DANMARK

HOLTEC i tal

8	35	110	1000	3000
Lokationer fordelt i Danmark	Års erfaring på automations-markedet	Medarbejdere med erfaring, viden og analytiske evner	Projektportefølje årligt	Tavler produceret årligt

Brancher og fokusområder



HOLTEC.DK®

Dubex:

28 YEARS OF CYBER DEFENCE

- ✓ Largest dedicated Cyber Defence Center in DK
- ✓ Both Danish and English service support
- ✓ Log monitoring and analysis since 1999
- ✓ Dubex Managed SIEM
- ✓ Incident Response - 16 years of experience

Dubex Service Areas

Cyber Risk Advisory
Risk Insights & Advice

- Risk and maturity assessments
- Risk management
- Compliance advisory Crisis management
- Supply chain management
- Internal auditing

Incident Response
React & Mitigate

- Incident Response Team
- Incident coordination and management
- Attack Mitigation, and recovery
- Forensics Analysis
- Incident Reports

Cyber Defence Center
Detect & Respond

- Managed SIEM & MDR
- Managed EDR
- Managed NDR
- Dark Web Monitoring
- Threat Alert
- Brand Protection

Offensive Security
Hack & Identify

- Penetration Testing
- Purple Team
- Assumed Breach
- Vulnerability management
- Phishing
- Attack surface mapping

As a Service
Cybersecurity advice

- CISO as a Service
- Security Architect as a Service
- SME as a service

Security Operations
Operate & Support

- Product support
- Product Consultancy
- Product Management support
  - CyberArk, Check Point, SentinelOne, F5, Symantec, InfoBlox

Cybersikkerhed i CTS

Dubex:

HOLTEC.DK®

NIS2 og CTS

- Risikostyring og robusthed
- Incident management
- Forretningkontinuitet
- Ledelsesansvar

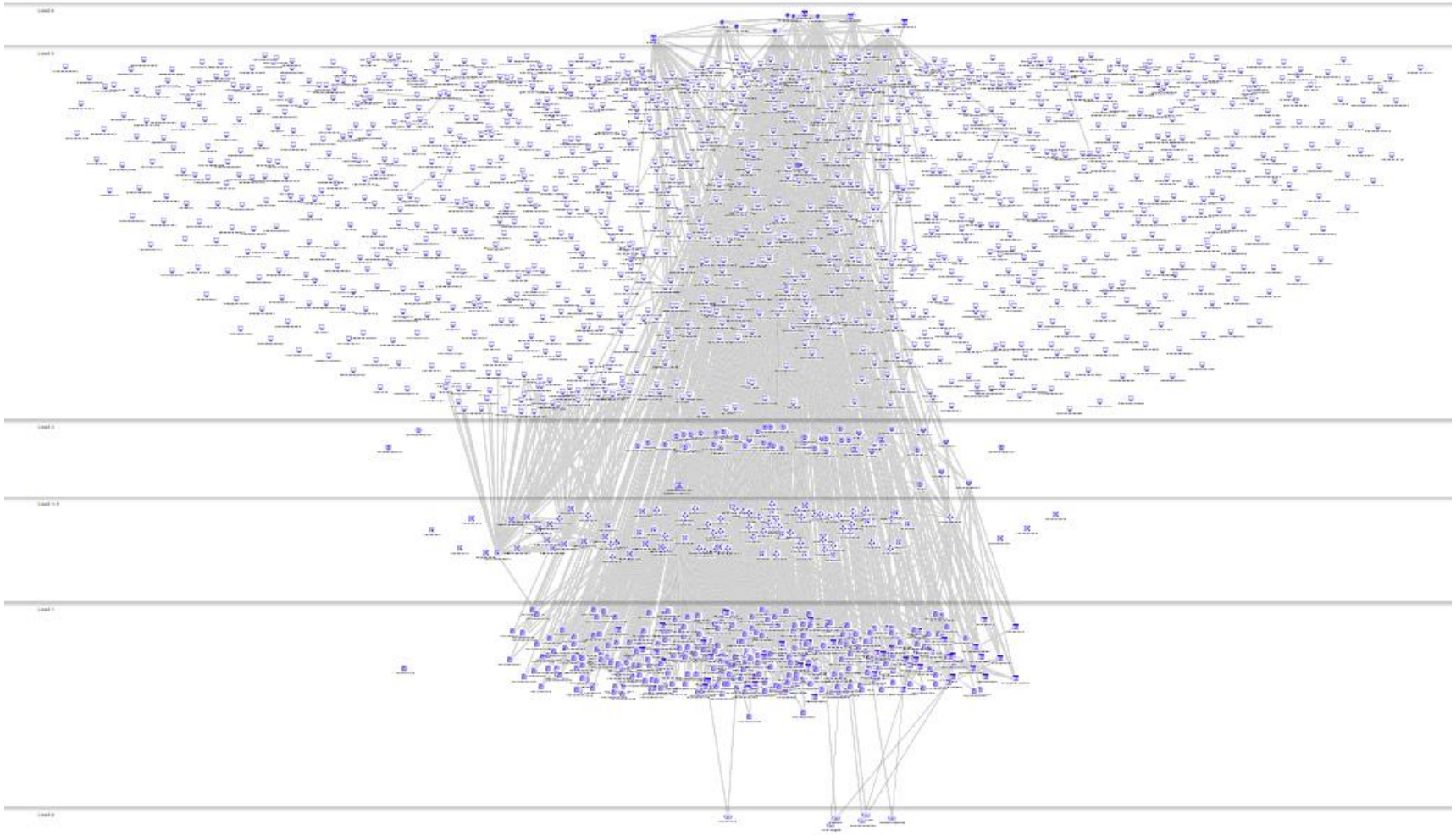
Roadmap til cybersikkerhed

- Asset inventory
- Risk assessment
- Security program
- Service provider management
- Network security
- Software updates
- Device security
- System/network access control
- Network documentation
- Physical security
- System backup/restore
- Change management
- Training
- System security verification
- Processes

Dubex:

HOLTEC.DK®

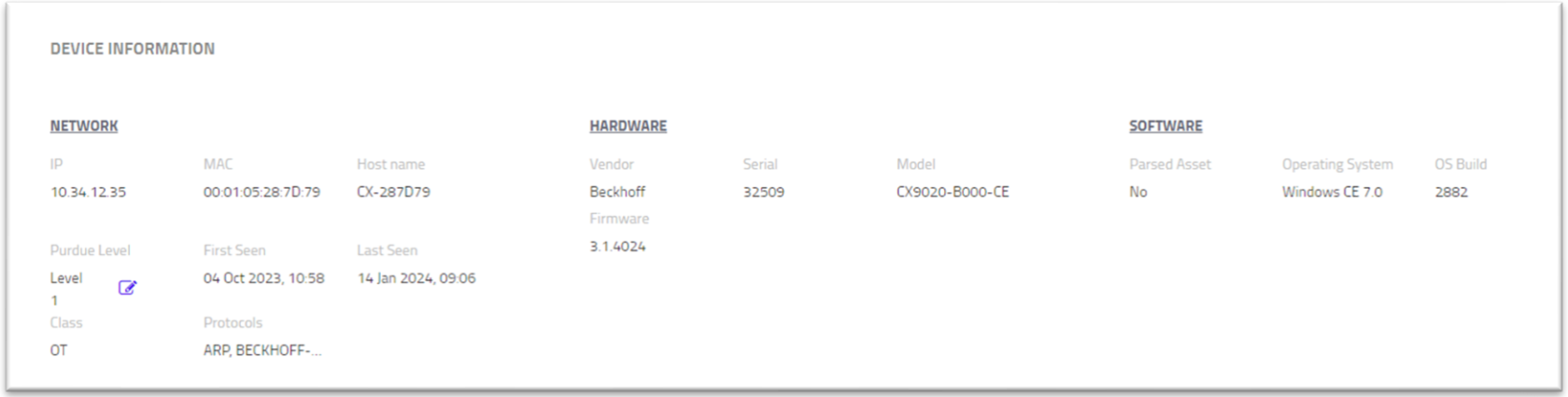
Claroty CTD demo

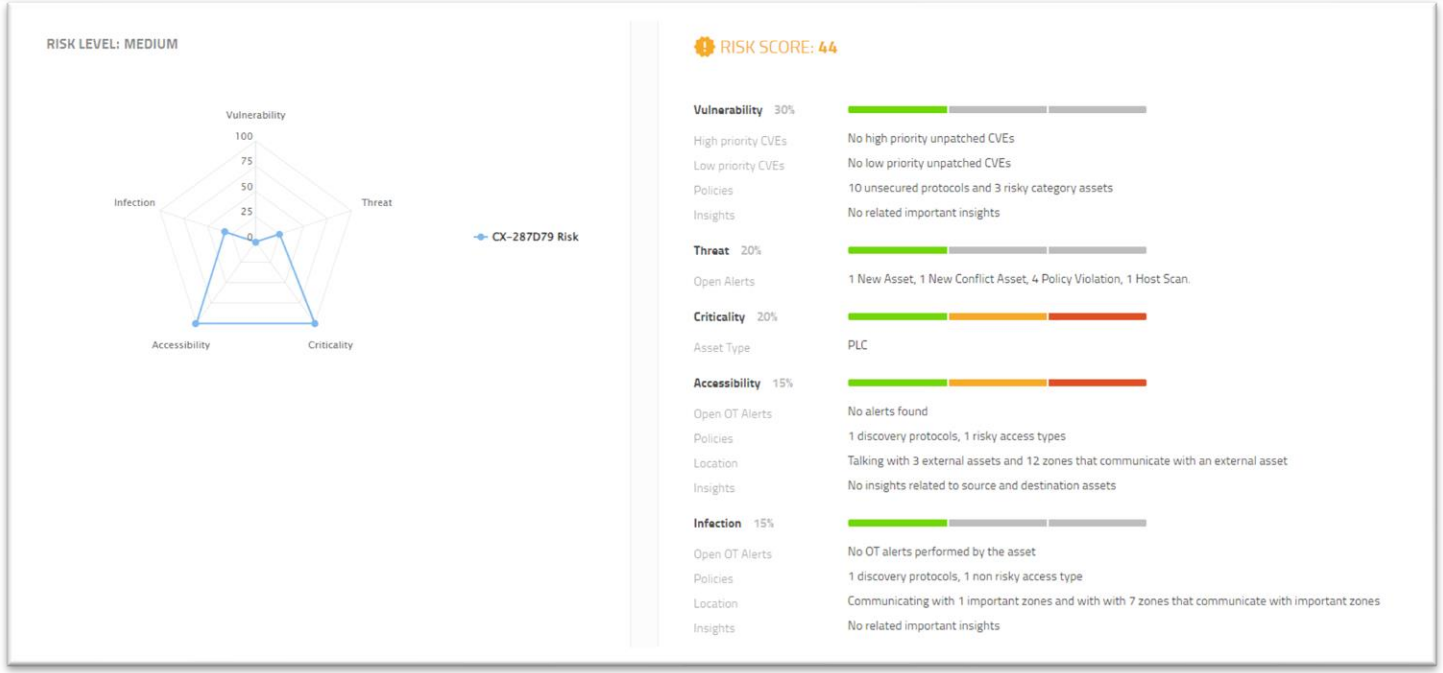


Dubex:

HOLTEC.DK®

Claroty CTD demo

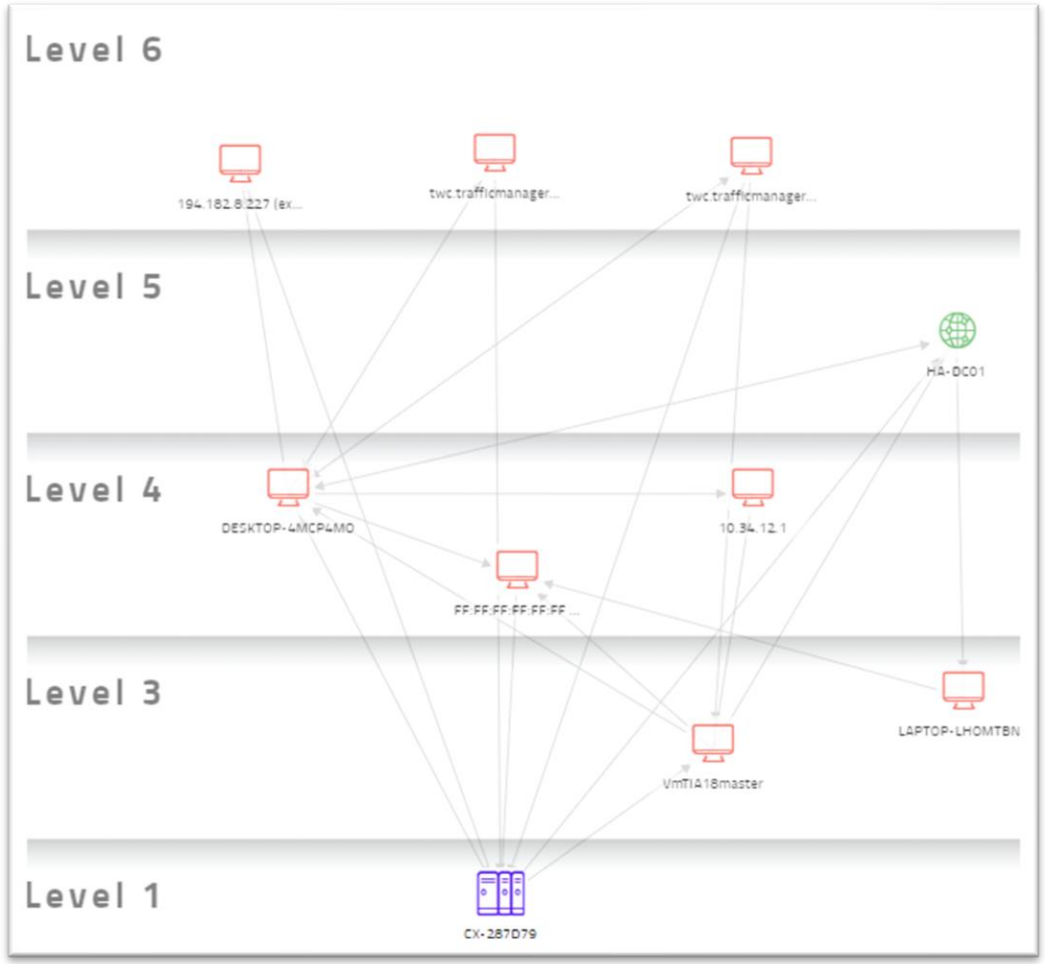


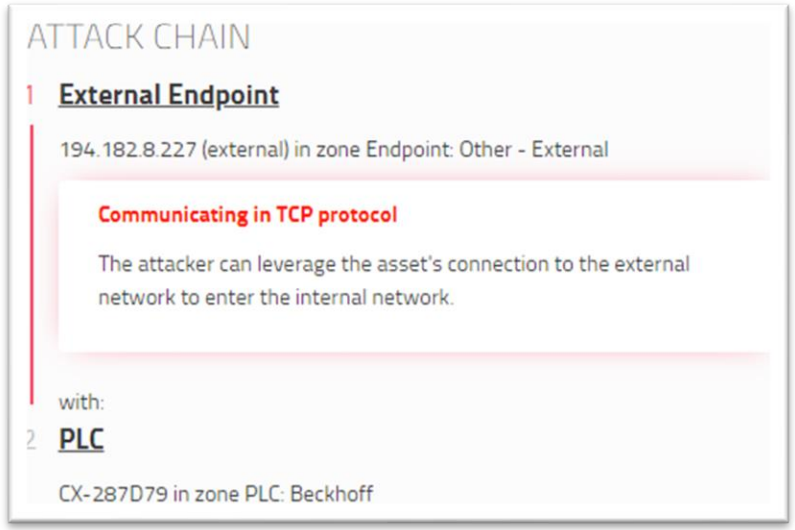


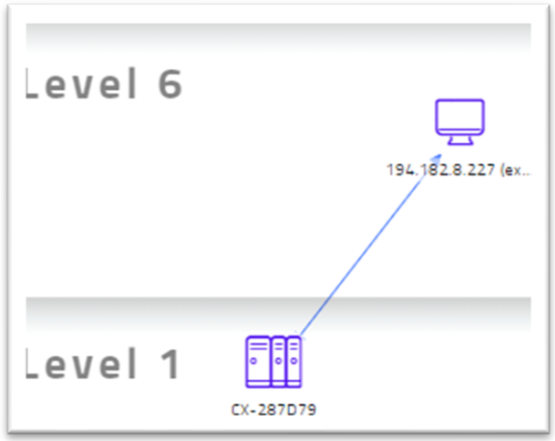
Dubex:

HOLTEC.DK®

Claroty CTD demo







Dubex:

HOLTEC.DK®

Roadmap til cybersikkerhed

- Asset inventory
- Risk assessment
- Security program
- Service provider management
- Network security
- Software updates
- Device security
- System/network access control
- Network documentation
- Physical security
- System backup/restore
- Change management
- Training
- System security verification
- Processes

Dubex:

HOLTEC.DK®

Roadmap til cybersikkerhed

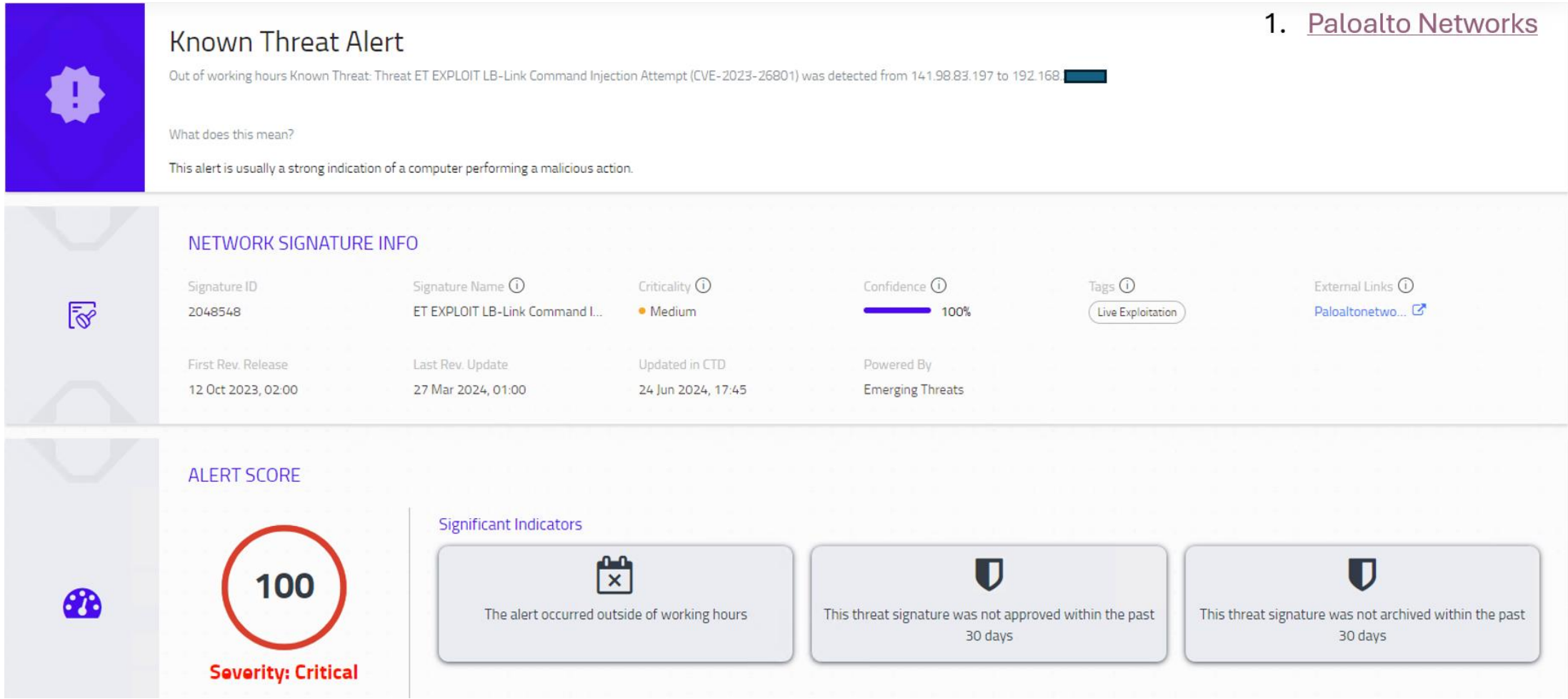
Aktivopgørelse: Opbygning af en fortegnelse over alle driftsaktiver og relaterede data såsom producent, modelnumre, softwareversioner, fysiske placeringer og netværksadresse.
Risikovurdering: Dokumentation af hvornår, hvordan og hvad der blev vurderet, og tilhørende risikovurderinger.
Sikkerhedsprogram: Oprettelse af et sikkerhedsprogram, der dækker styring, politikker og roller for både IT- og OT-personale (inklusive entreprenører).
Service Provider Management: Dokumentation af listen over serviceudbydere, nøglekontakter og autoriseret personale, omfanget af ansvar, systemtilladelser og andre oplysninger.
Netværkssikkerhed: Løsninger såsom firewalls hjælper med at forhindre uautoriseret adgang til et netværk og netværkssegmentering for at hjælpe med at begrænse eksponeringen, hvis der opstår et brud.
Softwareopdateringer: Regelmæssige softwareopdateringer og patches bør anvendes for at løse kendte systemsårbarheder.
Enhedssikkerhed: Enheder bør autentificeres over for hinanden ved hjælp af en nul-tillidsramme for at sikre, at enhed-til-enhed-kommunikation er tilladt, og kommunikation skal være krypteret for at beskytte data.
System-/netværksadgangskontrol: Dokumenterer, hvem der er i stand til at få adgang til netværket og enheder, hvordan de er i stand til at gøre det, og underskrevne kopier, der anerkender din fjernadgangspolitik. Der skal også inkluderes en dokumenteret proces til tilføjelse og fjernelse af brugere, tildeling af tilladelser og periodisk gennemgang.
Netværksdokumentation: Systemtegninger om, hvordan netværket og enhederne er forbundet, og relateret dokumentation for enheder, softwareversioner, netværksadresser, protokoller, VLAN'er og porte.

Roadmap til cybersikkerhed

Fysisk sikkerhed: Smart bygningsenheder skal være fysisk sikret, og adgang til dem bør kun være begrænset til autoriseret personale. Dette hjælper med at forhindre uautoriseret fysisk adgang og manipulation med enhederne, hvilket kan kompromittere deres sikkerhed eller aktivere enhedsspoofing.
System Backup/Restore: Dokumentation og proces for hvad der tages backup af, hyppighed af backup, hvordan og hvor backups gemmes, og hvem der har adgang til backups. Også dokumenteret proces for, hvordan man gendanner software og konfigurationsindstillinger.
Change Management: Dokumentation, der beskriver processen for godkendelse, planlægning og implementering af ændringer til den smarte bygnings infrastruktur.
Uddannelse: Personale og entreprenører bør have uddannelse i sikkerhedsbevidsthed for at kunne få adgang til de systemer, der driver den smarte bygningsinfrastruktur
Systemsikkerhedsverifikation: Dokumentation, der indikerer, at systemerne eller ændringerne er blevet implementeret, og cybersikkerhedsforanstaltninger er blevet implementeret og testet. Også inkluderet bør planlægges for løbende gennemgange og test for at verificere, at sikkerhedsforanstaltninger ikke er blevet elimineret eller ændret.
Processer: Sikkerhedsprocesser bør dokumenteres og revideres for at sikre, at de bliver fulgt, og hvordan man reagerer i tilfælde af en cybersikkerhedsbegivenhed. Smart bygningsenheder bør integreres i bygningens overordnede sikkerhedsarkitektur. Dette omfatter at sikre, at enhederne er en del af en omfattende sikkerhedsplan, som omfatter hændelsesprocedurer, regelmæssige sikkerhedsaudits og træning i sikkerhedsbevidsthed for medarbejdere.

Angreb på CTS i Industribygning

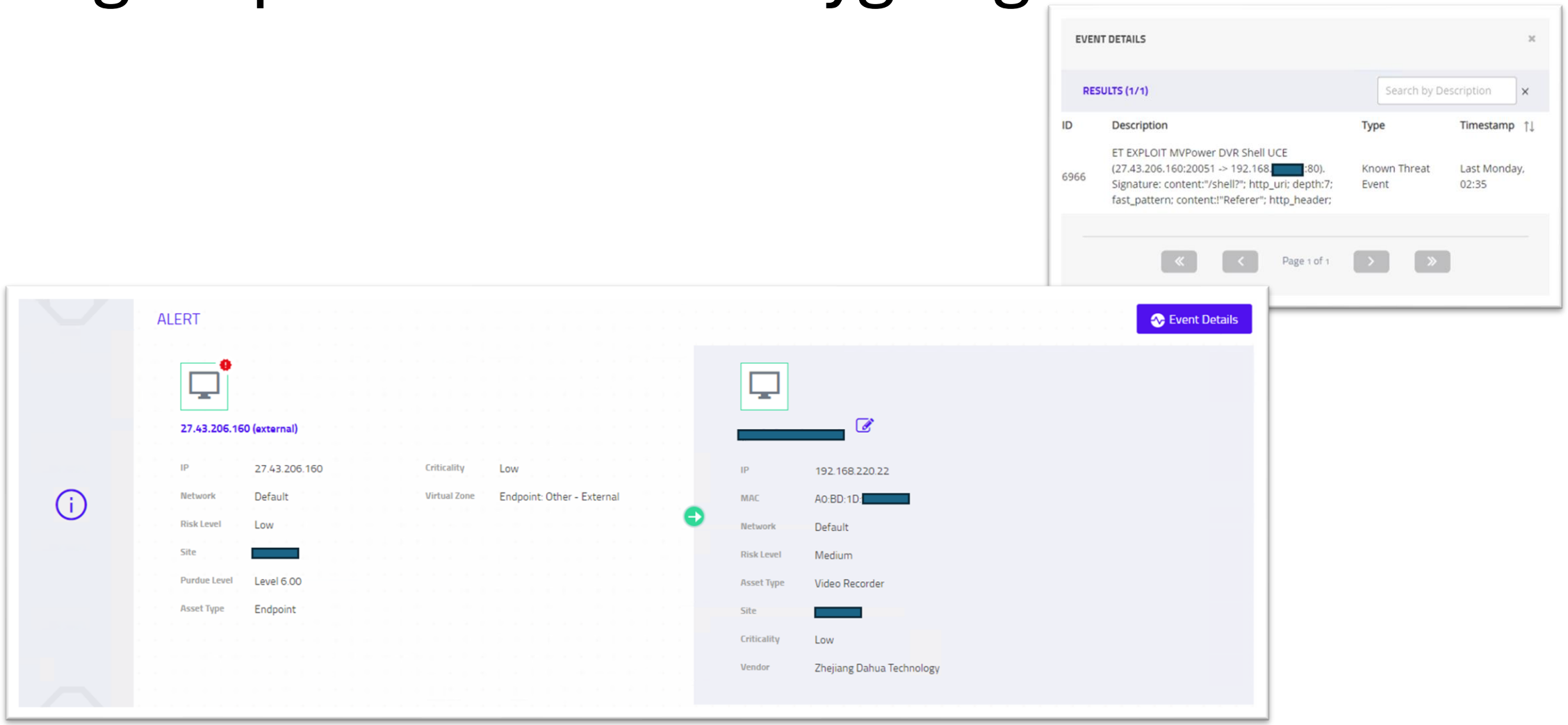
1. Paloalto Networks



Dubex:

HOLTEC.DK®

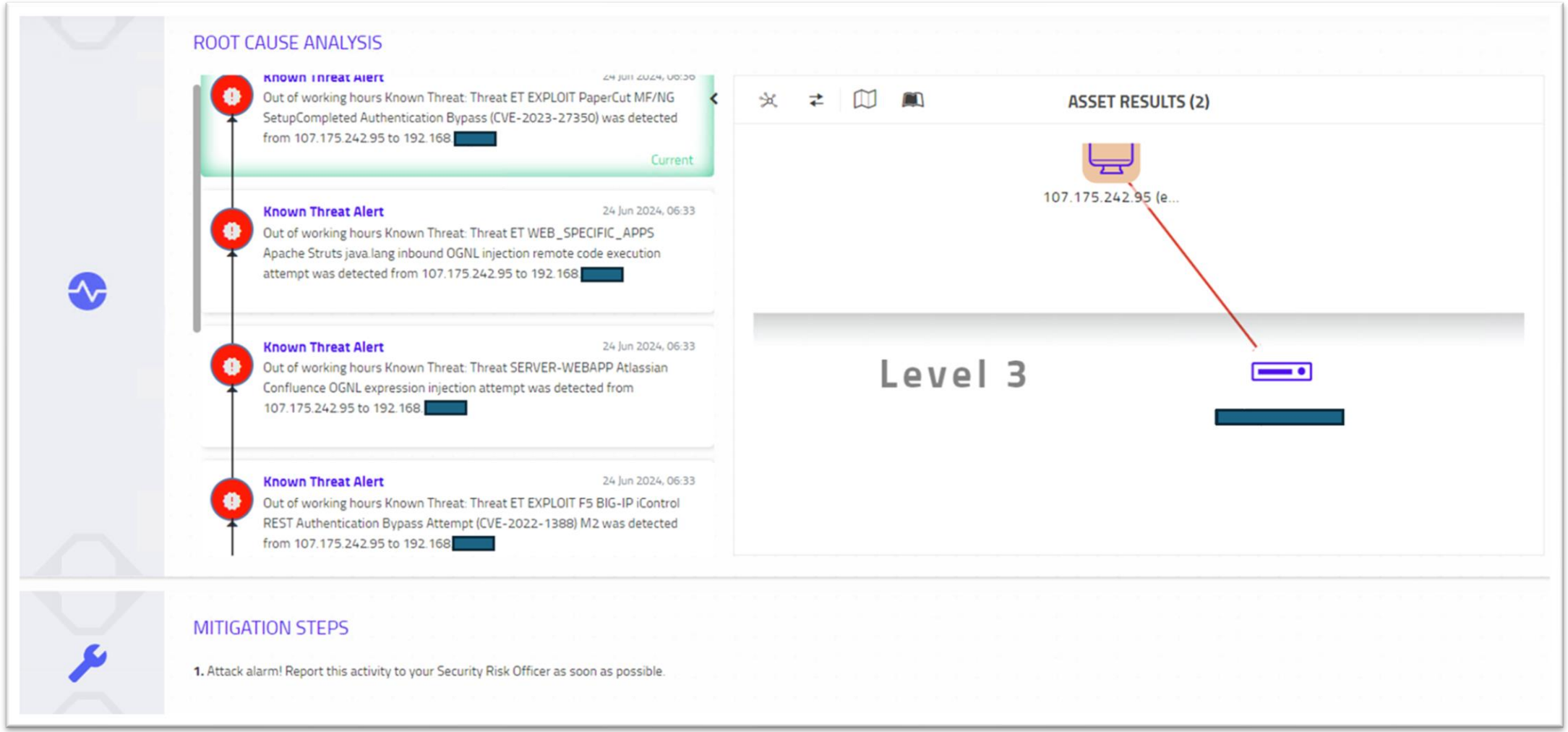
Angreb på CTS i Industribygning



Dubex:

HOLTEC.DK®

Angreb på CTS i Industribygning



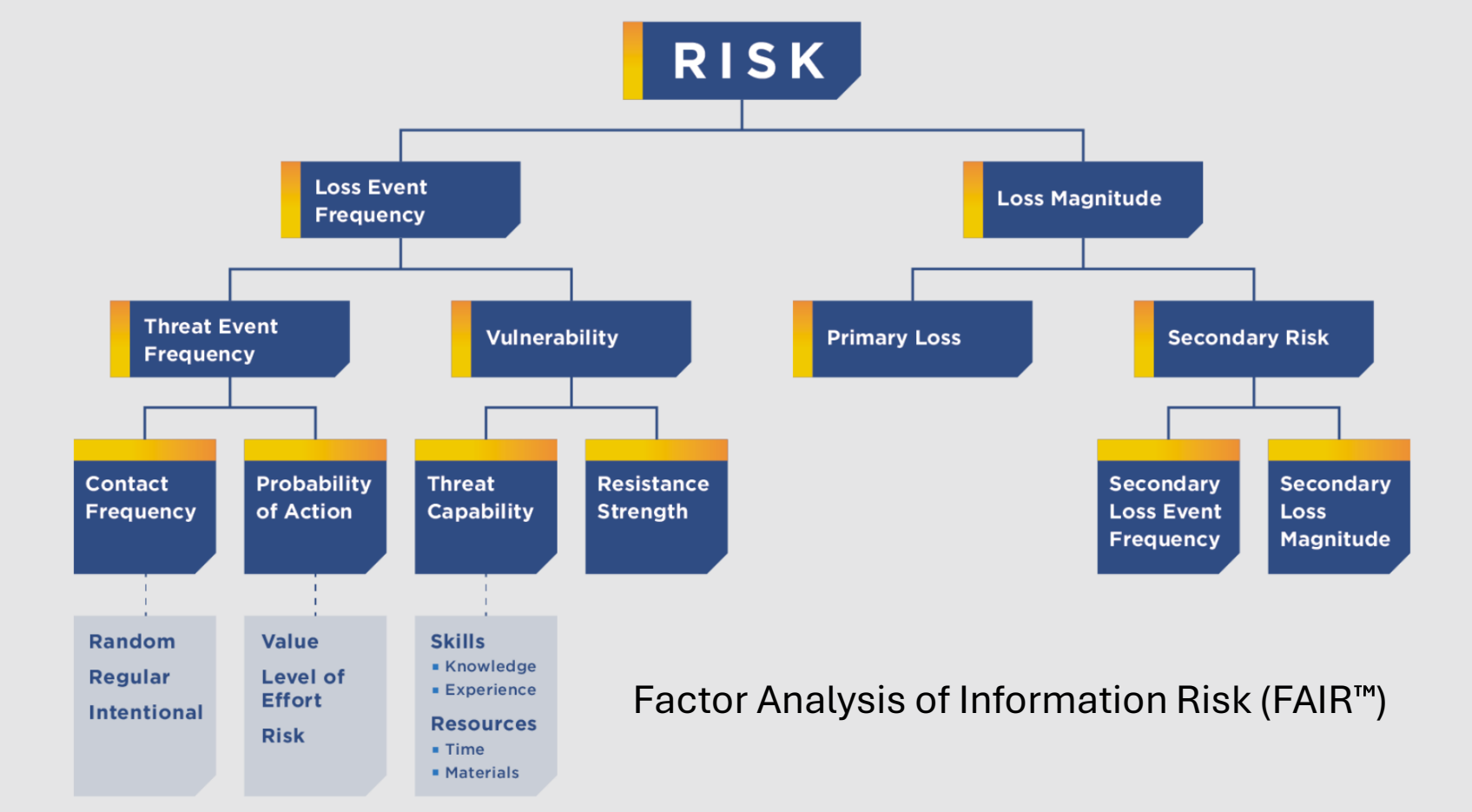
Dubex:

HOLTEC.DK®

NIS2-relevante sårbarheder og udfordringer, som vi ser i vores arbejde er:

1. **Manglende overblik:** Ingen samlet asset management-system for OT/CTS-enheder og deres cybersikkerhedsstatus.
2. **Fragmenteret governance:** Uklar ansvarsfordeling mellem IT, Teknik og eksterne leverandører.
3. **Utilstrækkelig segmentering:** Mange systemer har for tæt integration med administrative netværk.
4. **Svage autentificeringskrav:** Manglende implementering af stærk autentificering og privilegiestyring.
5. **Forældede protokoller:** Udbredt brug af usikre og ukrypterede protokoller som Modbus, BACnet uden sikkerhedsudvidelser.
6. **Manglende hændelsesdetektering:** Begrænset overvågning og logning af sikkerhedshændelser.
7. **Leverandørstyring:** Utilstrækkelig kontrol med tredjepartsleverandørers adgang og aktiviteter.
8. **Manglende beredskab:** Ingen formaliserede incident response-procedurer specifikt for OT/CTS-hændelser.
9. **Kompetencegab:** Meget begrænset teknisk kompetence i krydsfeltet mellem bygningsautomation og cybersikkerhed.
10. **Manglende patch management:** Ingen struktureret proces for sikkerhedsopdatering af CTS og IoT-enheder.

FAIR Cyber Risk Management Framework



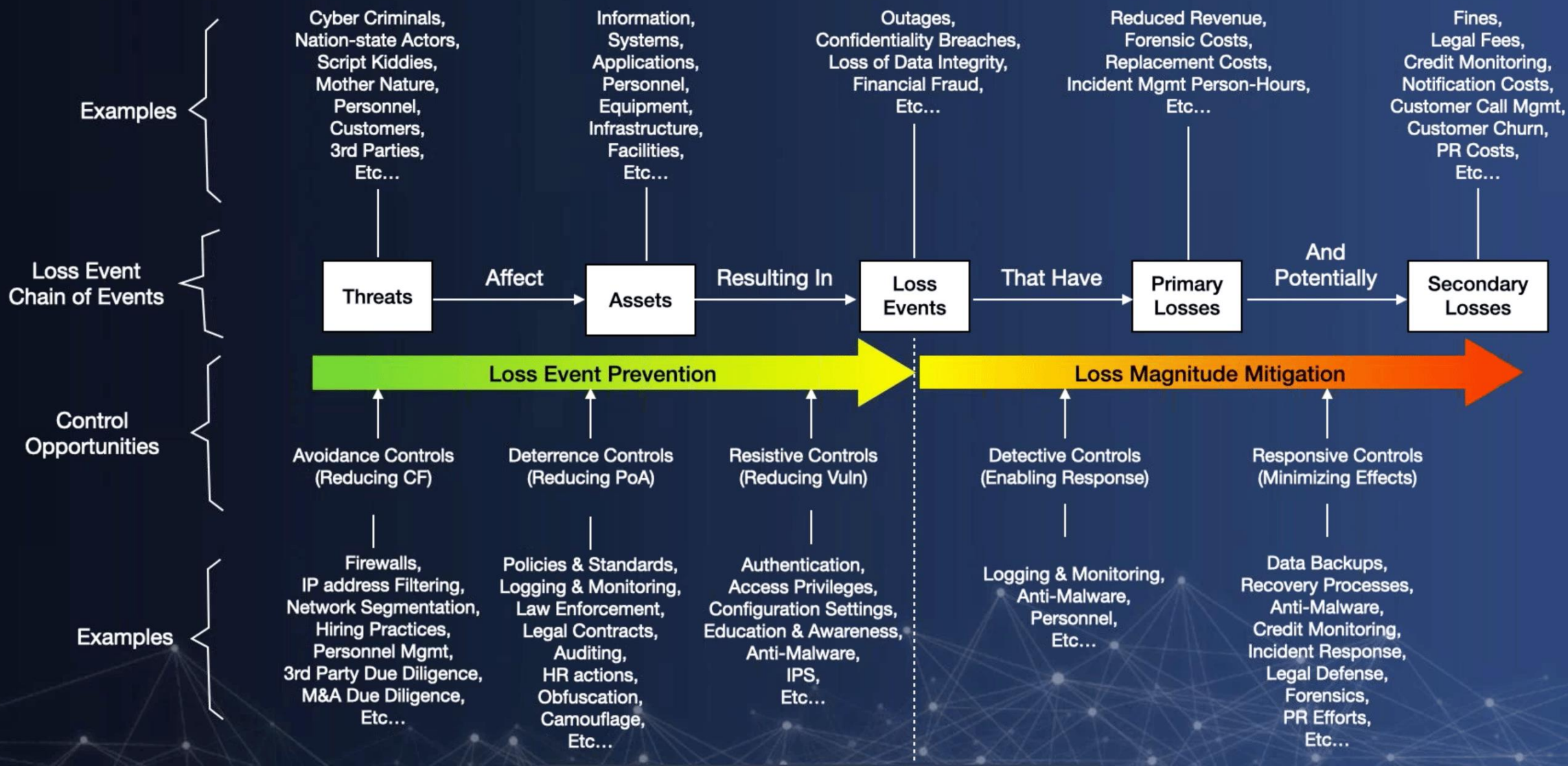
Factor Analysis of Information Risk (FAIR™)

Dubex:

FAIR INSTITUTE https://www.fairinstitute.org/

HOLTEC.DK®

Loss Event Controls…



Business Case: Fynsborg Kommune

- Fynsborg Kommune forvalter 187 bygninger
- 7 forskellige CTS-systemer fra multiple leverandører
- Heterogen implementering over 20+ år
- Varierende sikkerhedsniveauer og netværkskonfigurationer
- Ransomware-angreb i 2021, der påvirkede 3 CTS-servere

- 35% af CTS-installationerne har utilstrækkelig netværkssegmentering fra administrative netværk
- 12 systemer har direkte internetforbindelse med minimal sikkerhed
- 43 installationer har særlige konti til leverandører med varierende sikkerhedsniveau
- Mindst 15-20% af ældre installationer kører med standard / default adgangskoder

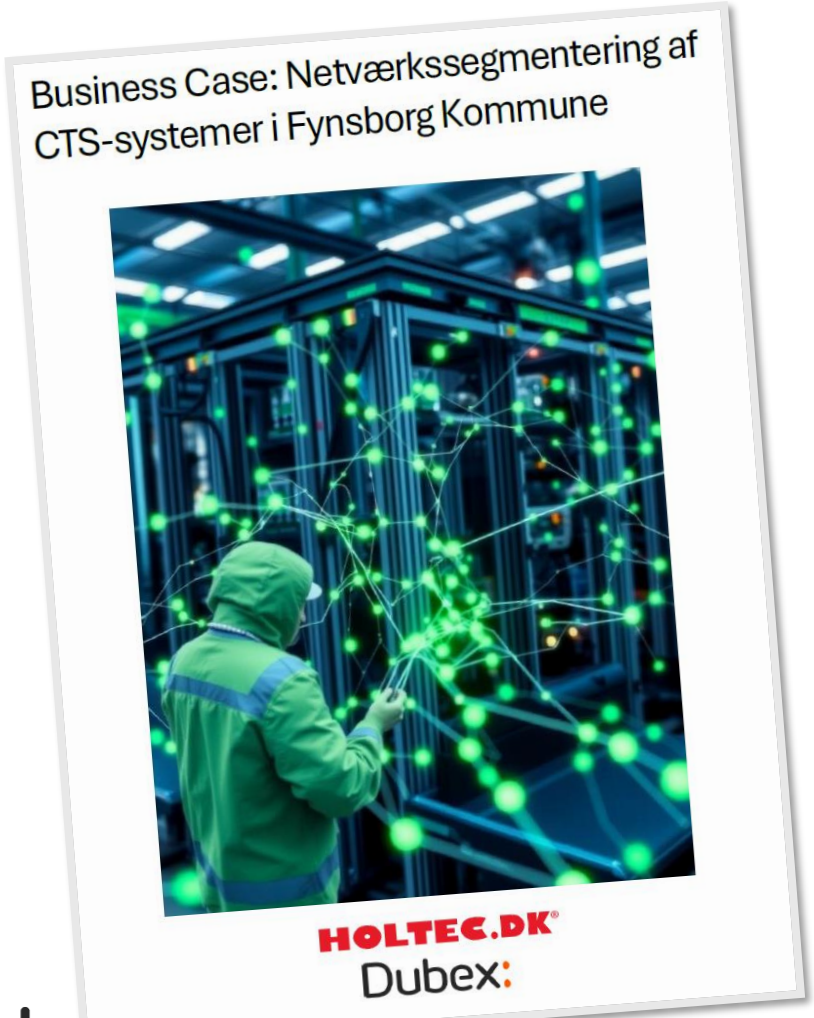
- Ransomware-angreb gav midlertidigt tab af styringskapacitet på 28 bygninger
- Manuel drift i 72 timer, herunder nattevagtsdækning
- Ekstra udgifter til IT-forensic, genopretning og sikringsforanstaltninger
- Estimeret total omkostning: ca. 850.000 kr.

- NIS2-compliance: Segmentering af netværk vil væsentligt forbedre kommunens opfyldelse af NIS2-direktivets krav.
- Betydelig risikoreduktion i den årlige risikoeksponering med 78%, fra 1.564.000 kr. pr. år til 344.000 kr. pr. år
- Positiv business case med en tilbagebetalingstid på 2,2 år og en 5-årig ROI på 128%

Dubex:

HOLTEC.DK®

Business Case: Fynsborg Kommune



- Denne business case præsenterer et projekt til netværkssegmentering af Fynsborg Kommunes CTS-systemer (Central Tilstands- og Styringssystemer) for at sikre compliance med NIS2-direktivet samt generelt reducere kommunens cybersikkerhedsrisici.
- Projektet adresserer en kritisk sårbarhed, hvor 35% af kommunens CTS-installationer har utilstrækkelig adskillelse fra det administrative netværk.
- De der måtte ønske den fulde case beskrivelse tilsendt kan skrive til: jbe@dubex.dk eller jlv@holtec.dk

Dubex:

HOLTEC.DK®