

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

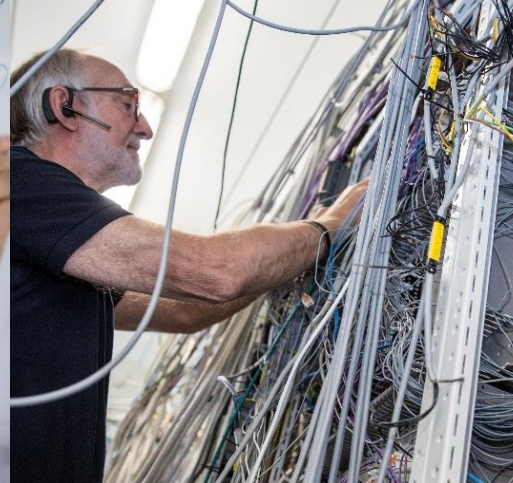
www.linkedin.com/in/jens-l-vestergaard



Afdelingsleder - Holtec

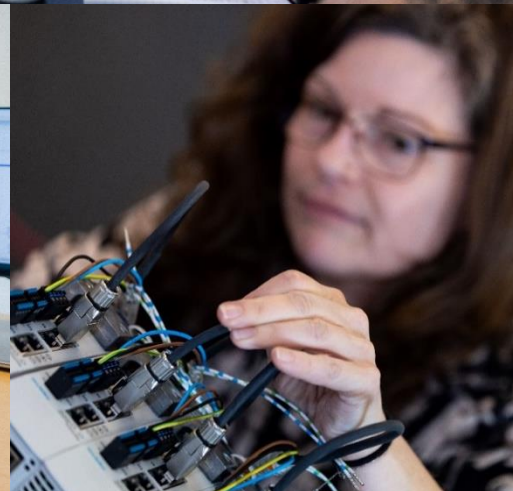
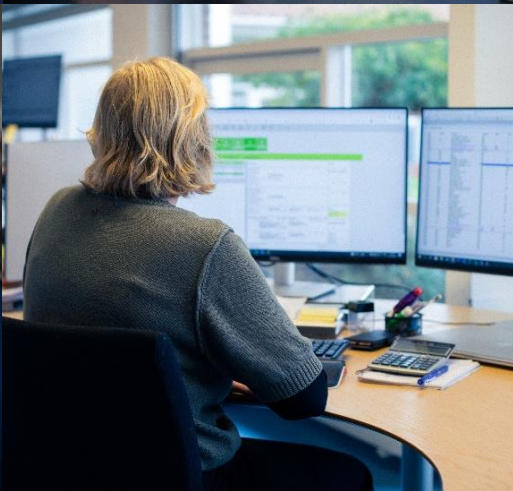
TLF. 91890572

Mail jlv@holtec.dk



HOLTEC.DK®

Din professionelle
partner i industriel
automation og IT



HOLTEC gruppen

- VI HAR 10 AFDELINGER I DANMARK

HOLTEC.DK®



SETEK
PROCESS & DATA

HOLTEC i tal

8

Lokationer
fordelt
i Danmark

35

Års erfaring
på
automations-
markedet

110

Medarbejdere
med erfaring,
viden og
analytiske evner

1000

Projektportefølje
årligt

3000

Tavler produceret
årligt



HOLTEC.DK®

Brancher og fokusområder

Cyber security, BI og dataopsamling



Vand

Vandværker • Industrielle
vaskeanlæg/systemer • Vandbehandling



Miljø

Affaldssortering • Renseanlæg •
Spildevandsløsninger



Energi

Vindkraft • Biogasanlæg • Power-to-X •
Forbrændingsanlæg • Varmeværker



Maskinbyggere

OEM • Maskinværksteder • Ventilation •
Udviklingsopgaver projekter



Produktion / Proces

Alle typer produktionsvirksomheder •
Optimering af processer og teknologier



Fødevarer

Producenter • Forædling/bearbejdning •
Mejerier • Slagterier • OEM

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



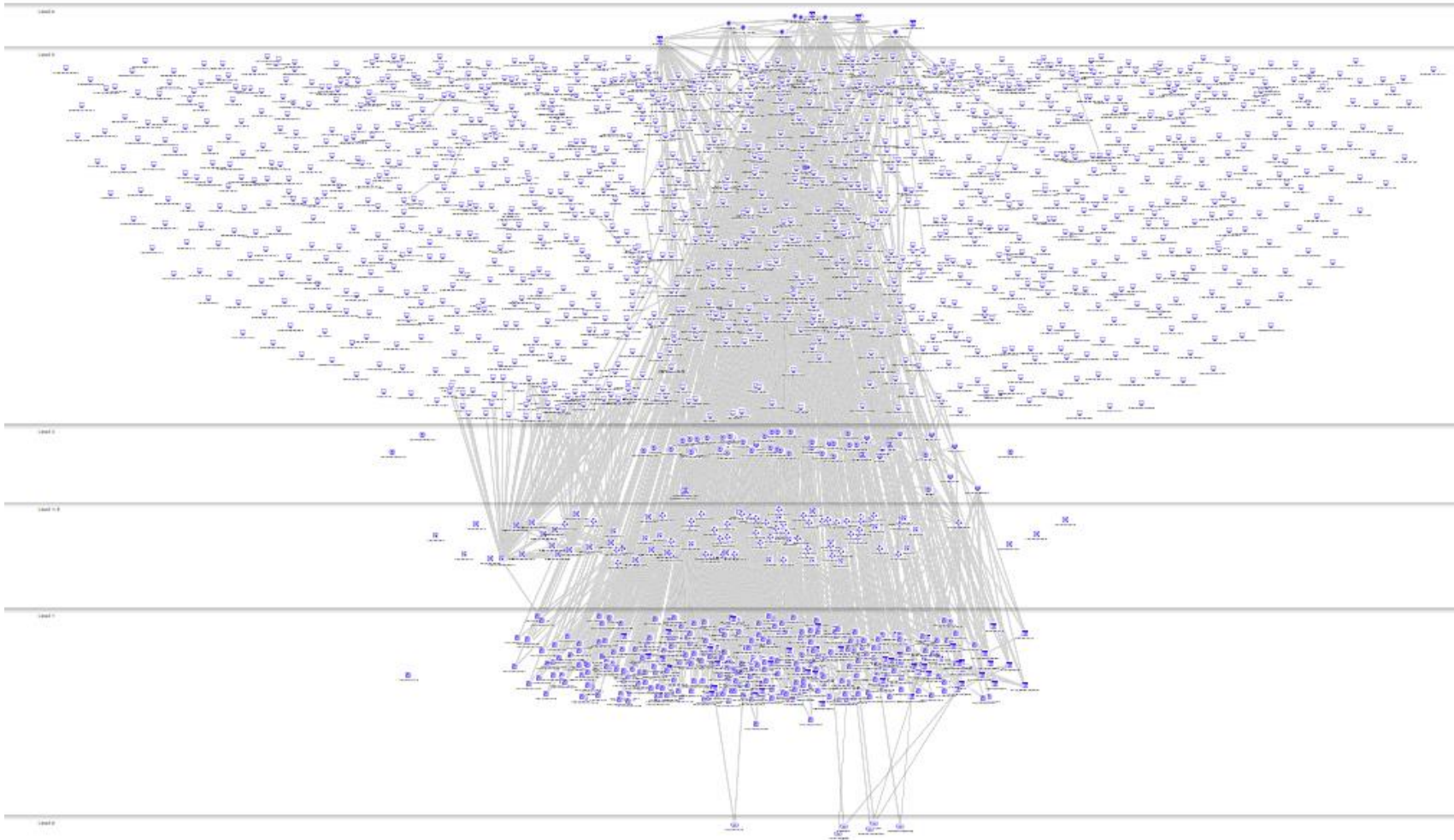
NIS2 og CTS

- Risikostyring og robusthed
- Incident management
- Forretningkontinuitet
- Ledelsesansvar

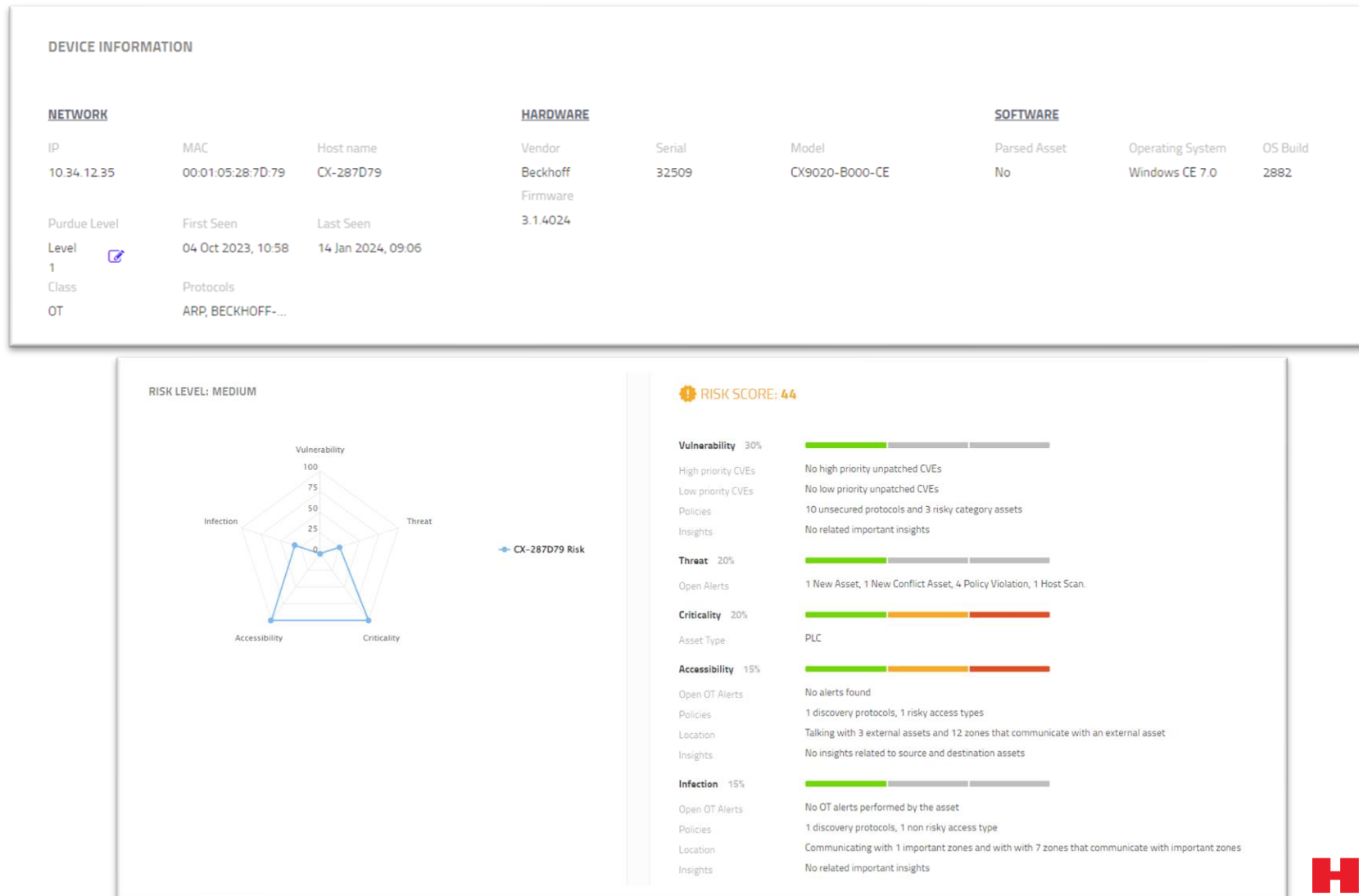
Roadmap til cybersikkerhed

- 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

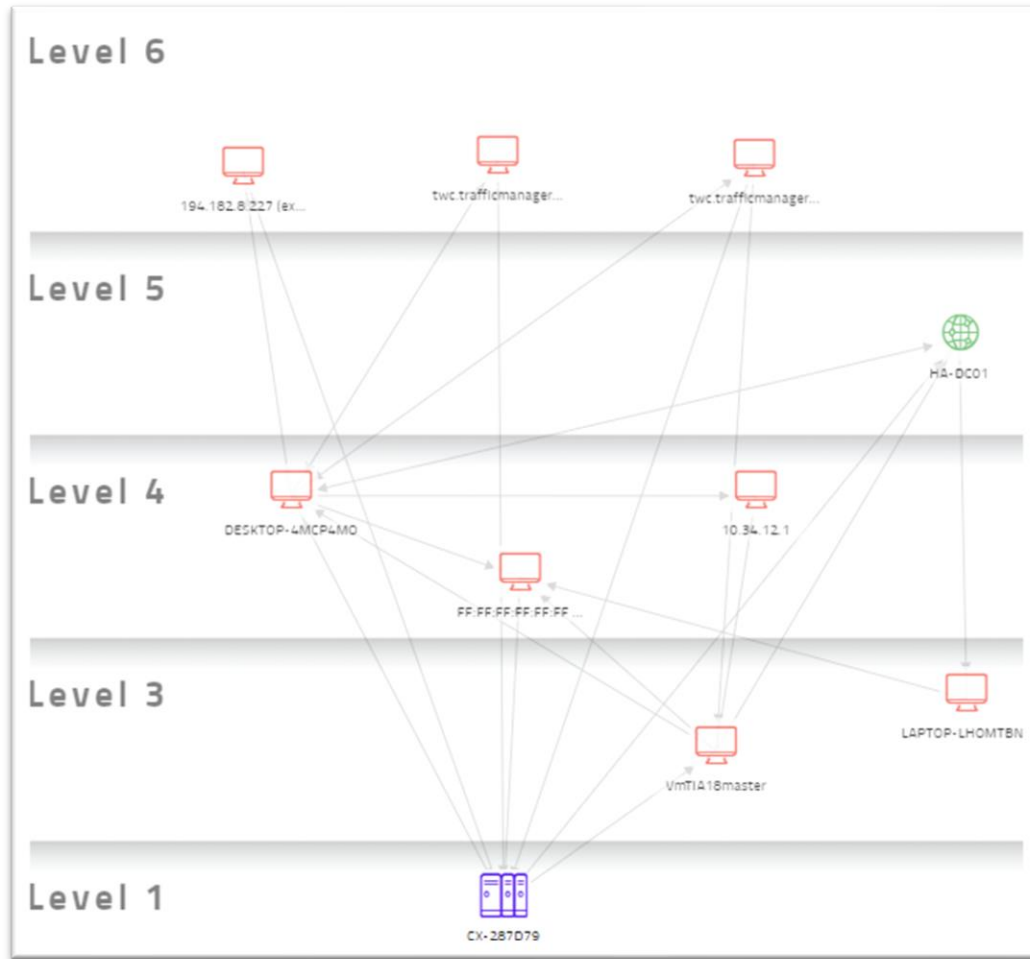
Claroty CTD demo



Claroty CTD demo



Claroty CTD demo



ATTACK CHAIN

1 External Endpoint

194.182.8.227 (external) in zone Endpoint: Other - External

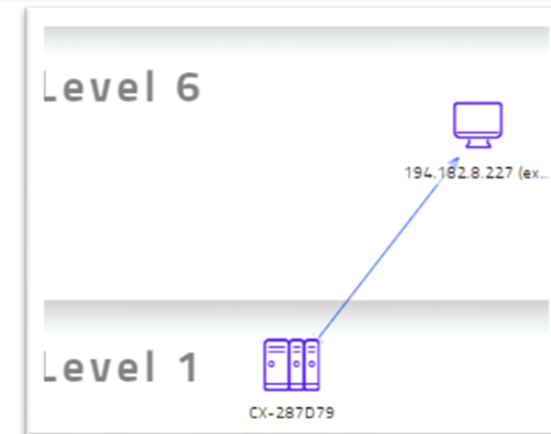
Communicating in TCP protocol

The attacker can leverage the asset's connection to the external network to enter the internal network.

with:

2 PLC

CX-287D79 in zone PLC: Beckhoff



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

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-enheds-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 bygningsinfrastruktur.

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



Known Threat Alert

Out of working hours Known Threat: Threat ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801) was detected from 141.98.83.197 to 192.168. 

What does this mean?

This alert is usually a strong indication of a computer performing a malicious action.

1. [Paloalto Networks](#)



NETWORK SIGNATURE INFO

Signature ID 2048548	Signature Name ⓘ ET EXPLOIT LB-Link Command I...	Criticality ⓘ ● Medium	Confidence ⓘ 100%	Tags ⓘ Live Exploitation	External Links ⓘ Paloaltonetwo...
First Rev. Release 12 Oct 2023, 02:00	Last Rev. Update 27 Mar 2024, 01:00	Updated in CTD 24 Jun 2024, 17:45	Powered By Emerging Threats		



ALERT SCORE

100

Severity: Critical

Significant Indicators



The alert occurred outside of working hours



This threat signature was not approved within the past 30 days



This threat signature was not archived within the past 30 days

Angreb på CTS i Industribygning

ALERT

27.43.206.160 (external)

IP

27.43.206.160

Criticality

Low

Network

Default

Virtual Zone

Endpoint: Other - External

Risk Level

Low

Site

Purdue Level

Level 6.00

Asset Type

Endpoint

IP

192.168.220.22

MAC

AO-BD-1D

Network

Default

Risk Level

Medium

Asset Type

Video Recorder

Site

Criticality

Low

Vendor

Zhejiang Dahua Technology

EVENT DETAILS

RESULTS (1/1)

Search by Description

ID	Description	Type	Timestamp
6966	ET EXPLOIT MvPower DVR Shell UCE (27.43.206.160:20051 -> 192.168.220.22:80). Signature: content:"/shell?"; http_uri: depth:7; fast_pattern: content:!"Referer"; http_header;	Known Threat Event	Last Monday, 02:35

<<

<

Page 1 of 1

>

>>

Dubex:

HOLTEC.DK®

Angreb på CTS i Industribygning

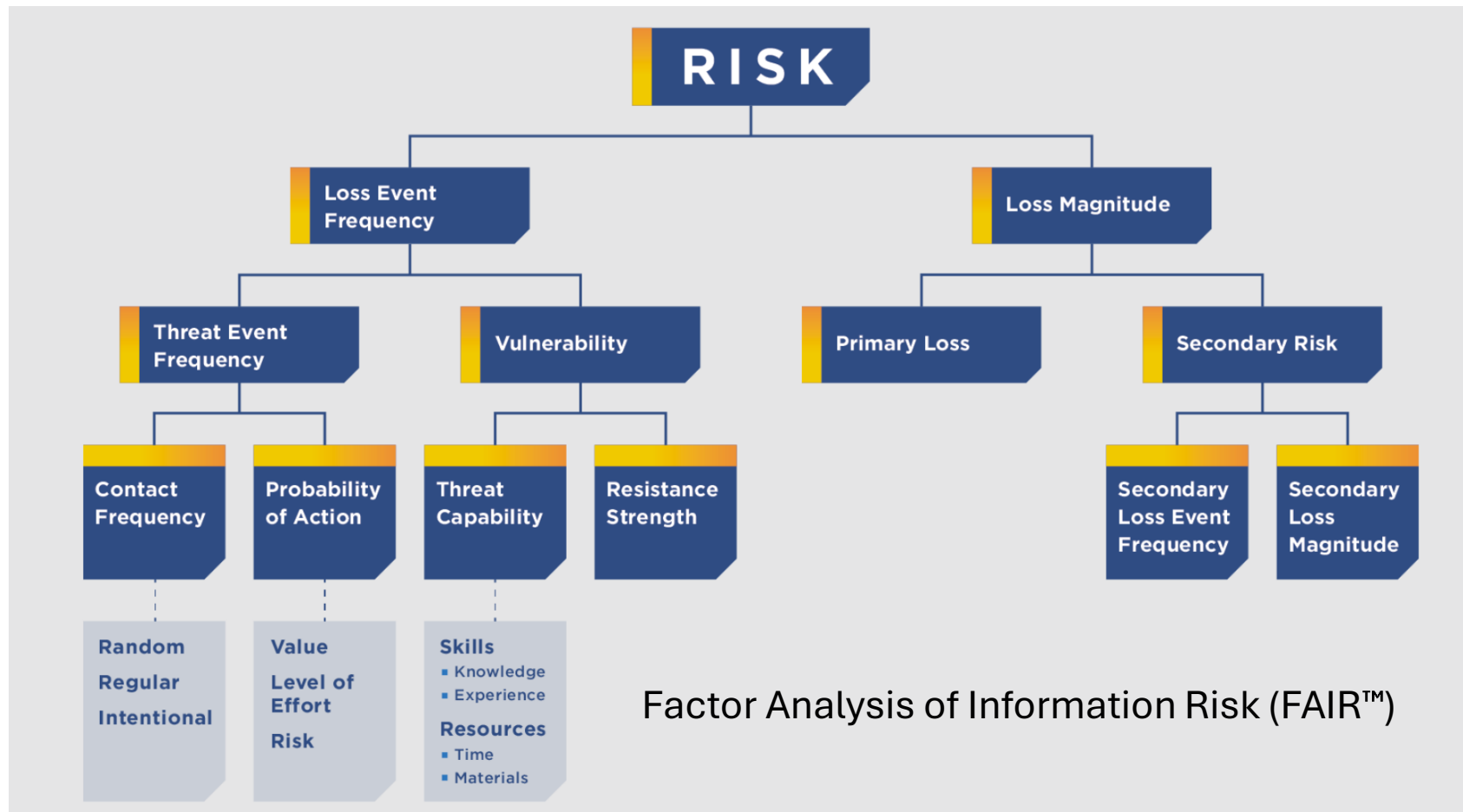
The screenshot displays the Dubex security dashboard interface, which is divided into several sections:

- ROOT CAUSE ANALYSIS:** This section contains a vertical timeline of four alerts, each marked with a red gear icon. The top alert is highlighted in green and labeled "Current".
 - known threat Alert:** Out of working hours Known Threat: Threat ET EXPLOIT PaperCut MF/NG SetupCompleted Authentication Bypass (CVE-2023-27350) was detected from 107.175.242.95 to 192.168. [redacted].
 - Known Threat Alert:** Out of working hours Known Threat: Threat ET WEB_SPECIFIC_APPS Apache Struts java.lang inbound OGNL injection remote code execution attempt was detected from 107.175.242.95 to 192.168. [redacted].
 - Known Threat Alert:** Out of working hours Known Threat: Threat SERVER-WEBAPP Atlassian Confluence OGNL expression injection attempt was detected from 107.175.242.95 to 192.168. [redacted].
 - Known Threat Alert:** Out of working hours Known Threat: Threat ET EXPLOIT F5 BIG-IP iControl REST Authentication Bypass Attempt (CVE-2022-1388) M2 was detected from 107.175.242.95 to 192.168. [redacted].
- ASSET RESULTS (2):** This section shows a network diagram with a red line connecting an asset icon (labeled "107.175.242.95 (e...") to a server icon (labeled "Level 3").
- MITIGATION STEPS:** This section contains a single step: "1. Attack alarm! Report this activity to your Security Risk Officer as soon as possible."

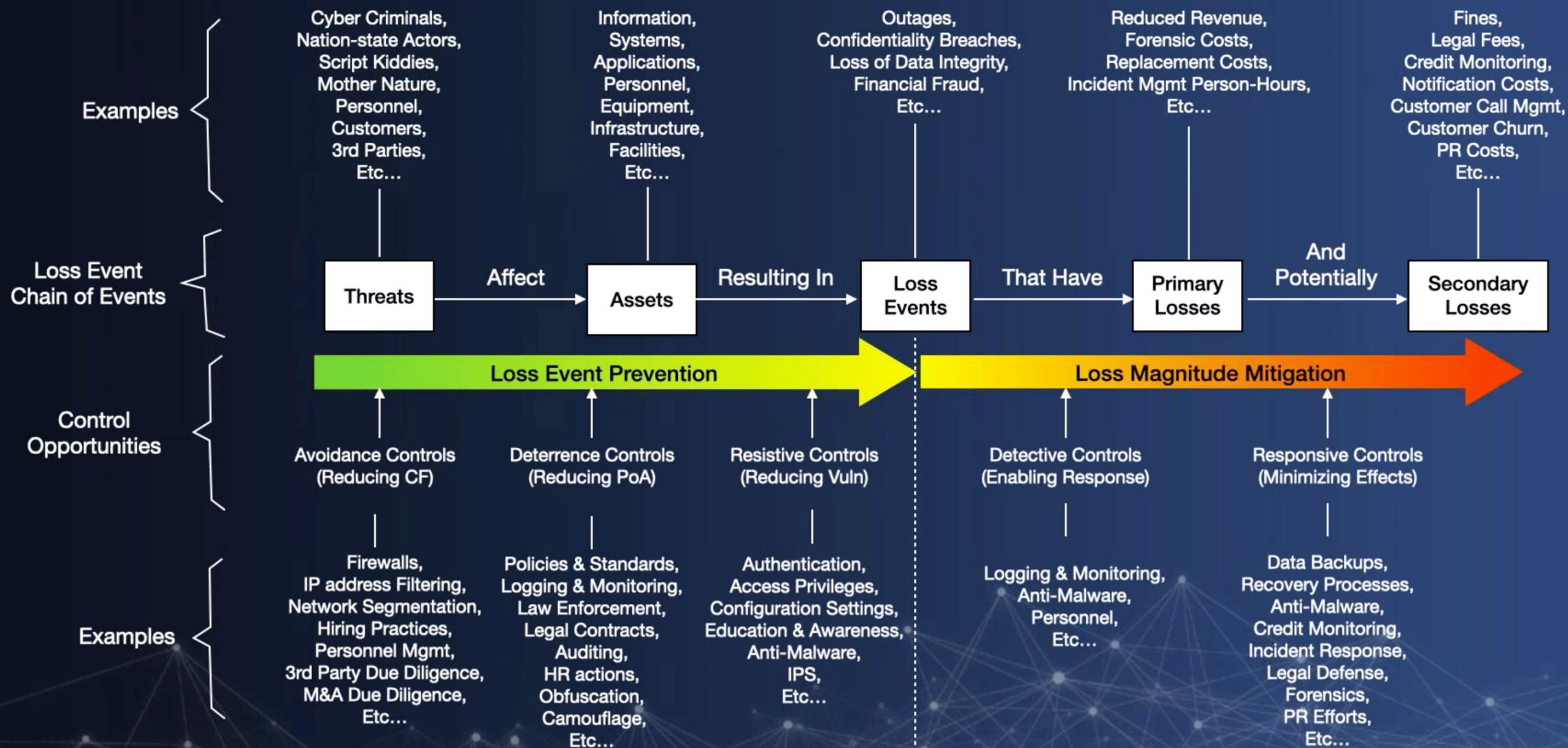
NIS2-relevante sårbarheder og udfordringer, som vi ser i vores arbejde er:

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 logging 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



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%

Business Case: Fynsborg Kommune

Business Case: Netværkssegmentering af CTS-systemer i Fynsborg Kommune



HOLTEC.DK
Dubex:

Dubex:

- 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

HOLTEC.DK