FHI INDUSTRIËLE AUTOMATISERING

OT cybersecurity monitoring

Praktische tips

Productie Proces Automatisering

24 januari 2023 | Hart van Holland Nijkerk

OTconnect
Securing Industrial Control Systems

FHI INDUSTRIËLE AUTOMATISERING

Agenda

01 Wat te monitoren

02 Waarom monitoren – compliancy

03 Waarom monitoren – asset inventarisatie

04 Waarom monitoren – cybersecurity

05 Hoe te monitoren

06 Waar te monitoren

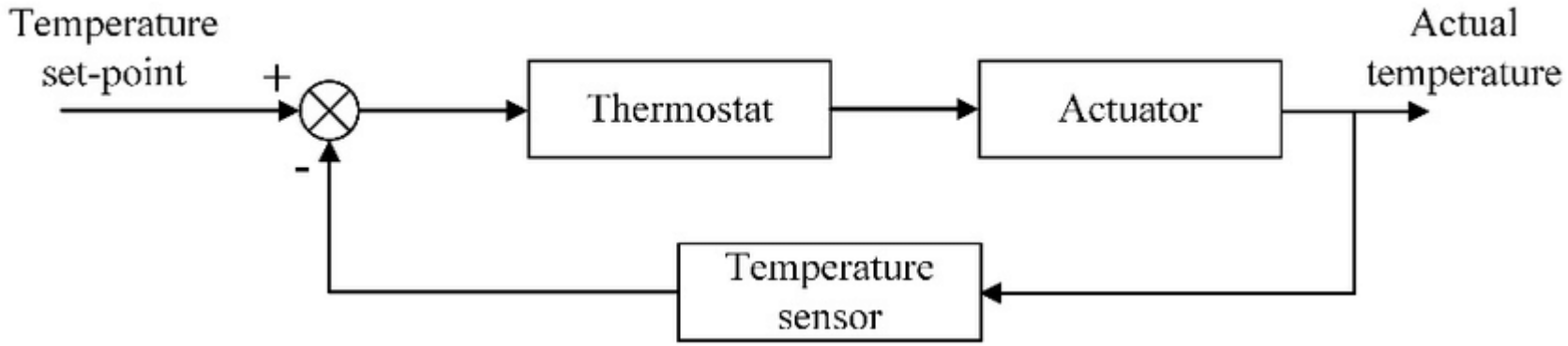
07 Hoe te beginnen met monitoren

08 Volgende stappen

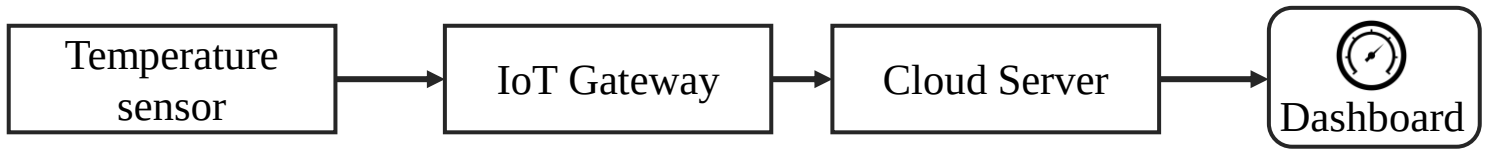
09 Afsluiting

Wat te monitoren – setting the scene

Operational Technology



Industrial Internet of Things



Waarom monitoren – compliancy

https://www.nis-2-directive.com/

NIS

- Gezondheidszorg
- Digitale infrastructuur (internetknooppunten, DNS, register TLDs
- Vervoer
- Drinkwatervoorziening en –distributie
- Digitale service providers
- Bankwezen en financiele infrastructuur
- Energie

NIS2

- Aanbieders van publieke communicatie netwerken of diensten
- Afvalwater en afvalstoffenbeheer
- Vervaardiging, productie en distributie van chemische stoffen, medische hulpmiddelen, elektronische apparatuur, etc
- Productie, verwerking en distributie van levensmiddelen
- Digitale aanbieders (sociale-netwerk diensten, etc)
- Ruimtevaart
- Post- en koeriersdiensten
- Overheidsdiensten

OTconnect
Securing Industrial Control Systems

Waarom monitoren – asset inventarisatie

OT-asset management

Het proces van het beheer van de hardware- en software assets die worden gebruikt om de activiteiten en productie van een organisatie te ondersteunen

OT-assets

- PLCs
- HMIs & SCADA
- Historian
- MES

OT-asset management is belangrijk

- Betrouwbaarheid en beschikbaarheid
- Lagere downtime
- Kosten verlagen
- Beveiliging verbeteren

FHI INDUSTRIËLE AUTOMATISERING

Waarom monitoren – cybersecurity

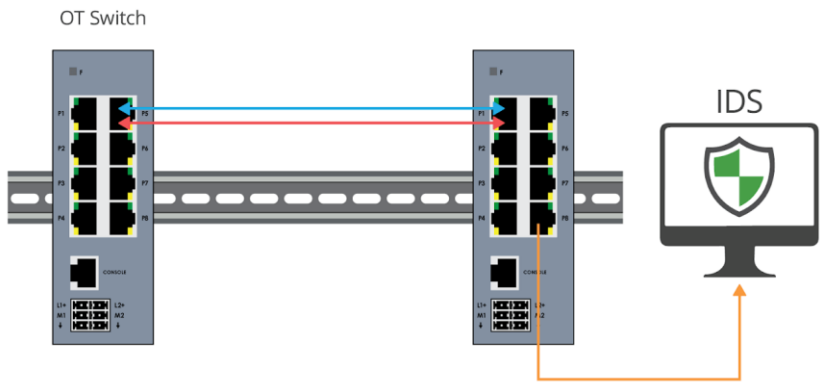
In kaart brengen van

- Software versies
- Kwetsbaarheden in de software
- Verkeersstromen (t.b.v. firewall rules)

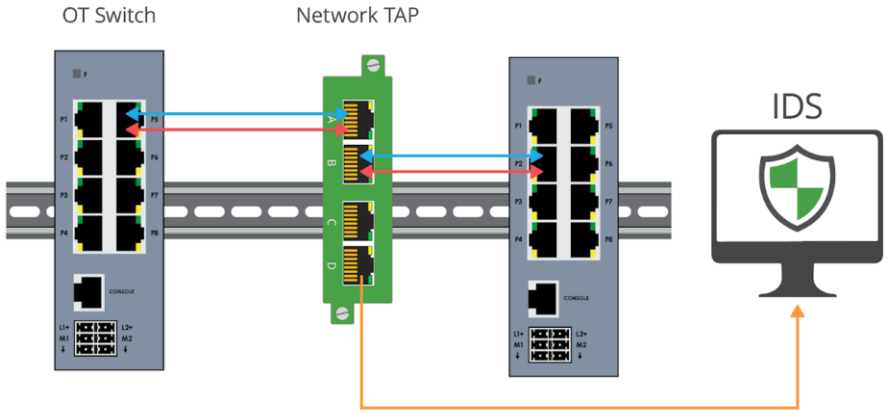
OTconnect
Securing Industrial Control Systems

Hoe te monitoren

Passief



Mirror (SPAN) poort op een switch*



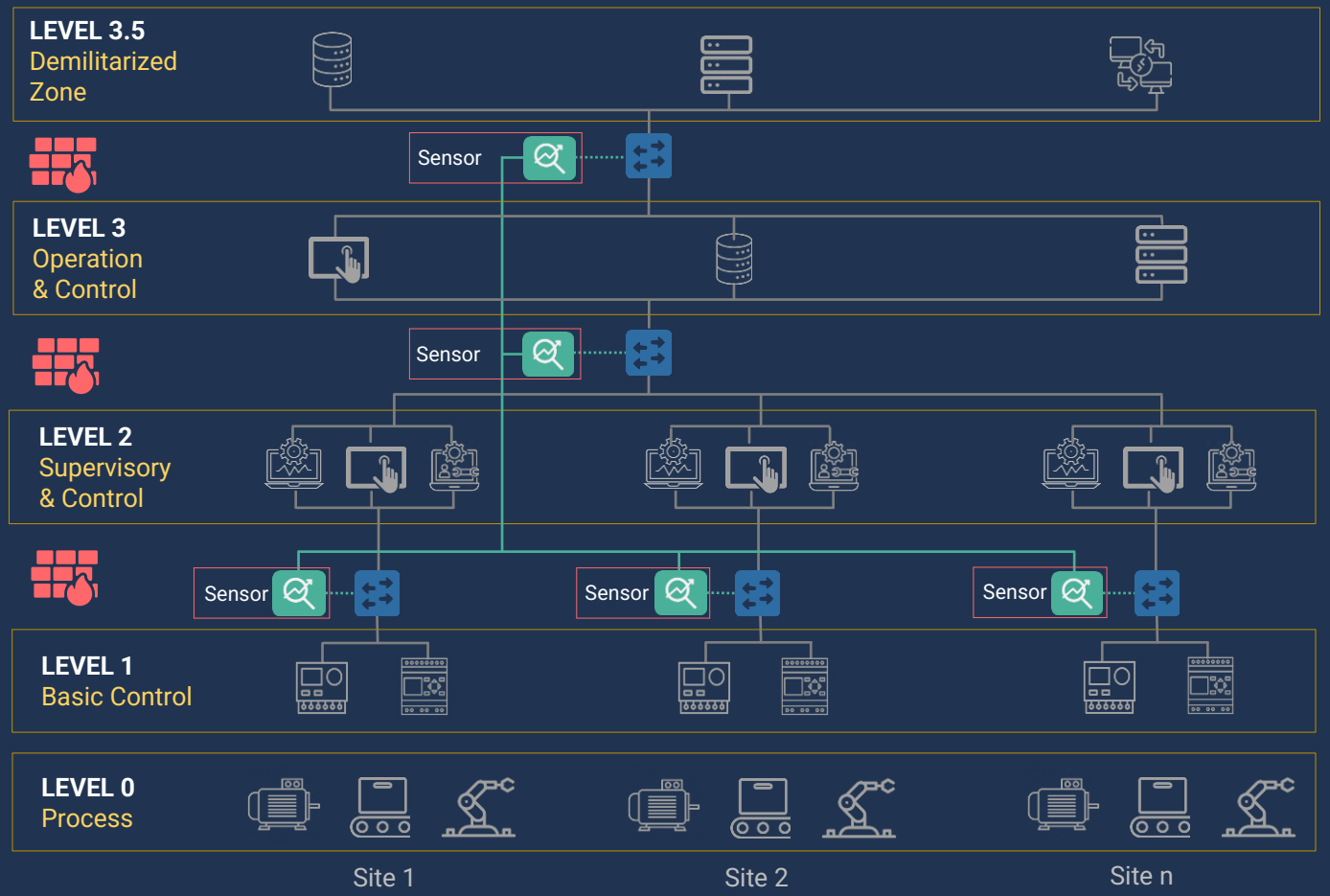
Netwerk tap*

Andere opties

- Actief – hierbij wordt het netwerk gescand
- Semi-actief – hierbij wordt ingelogd op assets die passief zijn ontdekt

* https://iebmedia.com/technology/cybersecurity/tap-vs-span-overcoming-packet-visibility-challenges-in-ot-environments/

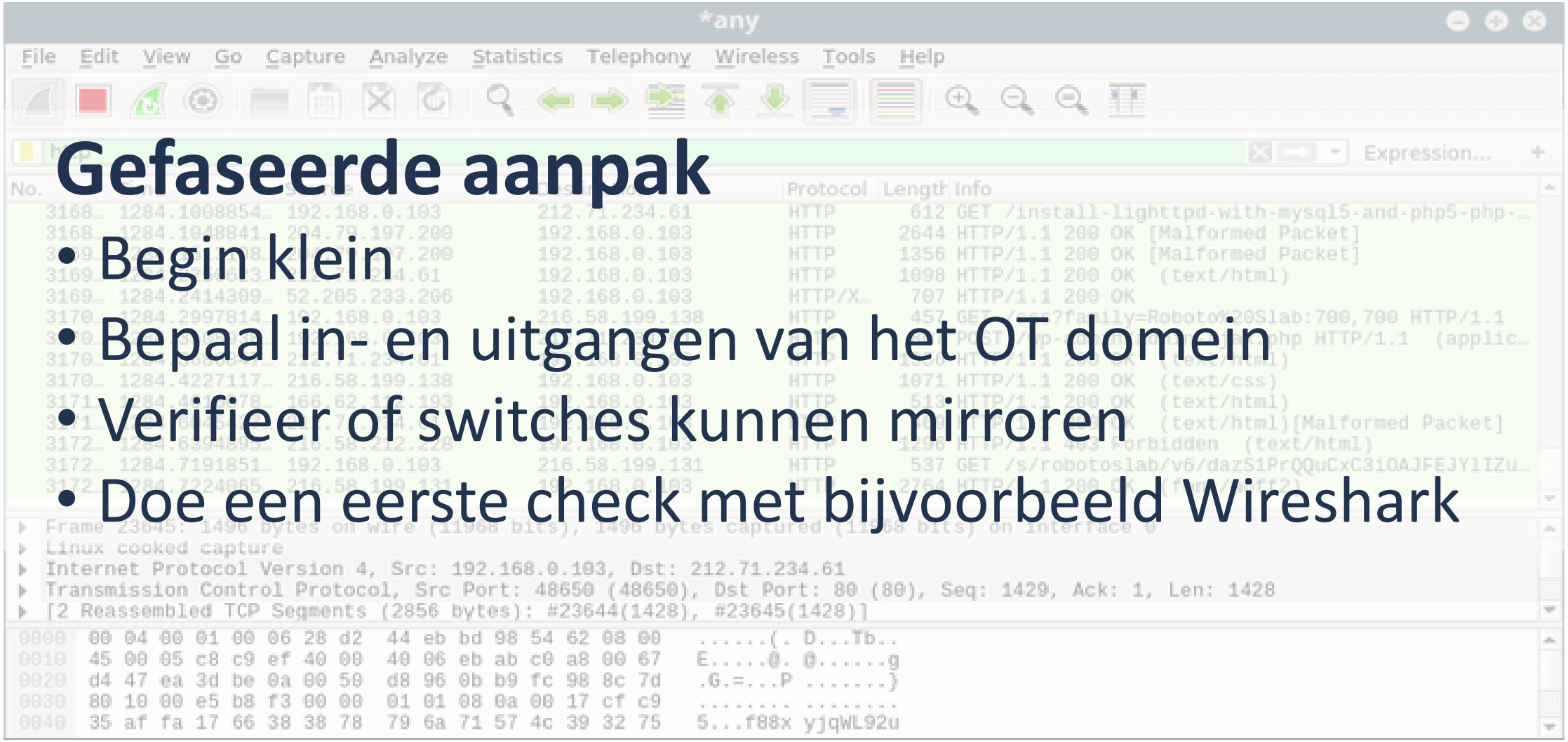
Waar te monitoren



Purdue Model for ICS Security

Structural Model for Industrial Control Systems

Hoe te beginnen met monitoren



Gefaseerde aanpak

- Begin klein
- Bepaal in- en uitgangen van het OT domein
- Verifieer of switches kunnen mirroren
- Doe een eerste check met bijvoorbeeld Wireshark

Volgende stappen

Monitoren is slechts het begin

- Verdiep je in de bedreigingen
- Bepaal je ‘risk appetite’
- Start een awareness programma
- Stel beleid op
- Bepaal wat belangrijk is – stel prioriteiten
- Implementeer basis maatregelen
- Definieer en implementeer response processen

FHI INDUSTRIËLE AUTOMATISERING

OTconnect

Securing Industrial Control Systems

Peter van der Voort

peter.vandervoort@otconnect.nl

06 – 3654 6397

contact@otconnect.nl | www.otconnect.nl | 085 – 743 0263