Hoe de zorgsector omgaat met de cybersecurity dreiging

Wendy Roodhooft

- Informatie beveiligingsofficier (CISO) az Vesalius Tongeren
- Focus op technische beveiliging
- Doel om de beveiliging van ziekenhuizen in België te vergroten

ANNACON

az Vesalius

- Ziekenhuis Tongeren
- 320 bedden
- Dagziekenhuis Bilzen
- 1000 werknemers
- 150-tal dokters
- 900 clients
- 250 servers

ANNACON

Le CHwapi victime d'une cyberattaque : le Centre Hospitalier dément une quelconque demande de rançon

Les équipes oeuvrent depuis ce dimanche soir afin de remettre en service le système informatique.

Le système informatique du centre hospitalier de Wallonie picarde est hors service depuis ce dimanche soir, 20h46. Le plan d'urgence hospitalier technique a directement été déclenché. "Notre première réaction a été de tout débrancher physiquement", explique Jacques Godart, le directeur informatique. "L'objectif est de ramener chacune des applications à la vie. Ce midi, le travail est toujours en cours sur 80 d'entre elles et il devrait se prolonger dans les prochains jours".

Les hackers qui ont pénétré le système n'ont, à ce jour, pas exigé de rançon. De manière imagée, le directeur Didier Delval explique que "la maison CHwapi" n'a pas été cambriolée. "On ne nous a rien volé, il n'y a rien de cassé. Les hackers ont juste changé la serrure de la maison; toute la maison. Aucune demande de rançon n'a été demandée et on ne connait toujours pas l'objectif poursuivi".

Cyberattaque sur Vivalia: le réseau fonctionne au ralenti et tout est à réinventer

La cyberattaque de ce week-end au sein de l'intercommunale hospitalière luxembourgeoise a tout chamboulé. Si de nombreux rendez-vous sont annulés, la prise en charge de toutes les urgences reste de mise.

Article réservé aux abonnés

Ransomware-aanval op Duits ziekenhuis leidde mogelijk tot dood patiënte

Een ransomware-aanval die de systemen van een ziekenhuis in Düsseldorf trof, heeft mogelijk geleid tot het overlijden van een patiënte, nadat de vrouw in kritieke toestand naar een ander ziekenhuis gebracht moest worden.

Op 10 september verklaarde het Universitair Ziekenhuis Düsseldorf dat er een omvangrijke it-storing gaande was, waardoor de kliniek slechts beperkt bereikbaar was. Het ziekenhuis schrapte alle afspraken, adviseerde patiënten niet te komen en staakte de spoedeisende zorg.

Donderdag maakt het ziekenhuis bekend dat het om een cyberaanval ging en dat it'ers de systemen langzaam maar zeker kunnen herstellen en toegang tot gegevens kunnen bieden. Volgens het universitaire ziekenhuis zouden de daders geen losgeld eisen. Volgens het ziekenhuis kon de aanval plaatsvinden via een kwetsbaarheid in wereldwijd gebruikte commerciële software. "Voordat het softwarebedrijf dit lek uiteindelijk dichtte, was er voldoende tijd om de systemen binnen te dringen."

Ziekenhuistoestellen makkelijk te hacken door verouderde besturingssystemen, blijkt uit test

Heel wat ziekenhuistoestellen kunnen gehackt worden. Dat blijkt uit een test door ethische hackers van Check Point. Check Point test regelmatig de veiligheid van toestellen die aan het internet verbonden zijn. Veel van die ziekenhuistoestellen draaien op een verouderd besturingssysteem. Het verhaal is bevestigd aan VRT NWS door verschillende ziekenhuisinformatici die anoniem willen blijven.

De inzet is hoog!

ANNACON

Belangrijkste prioriteiten in cybersecurity van de zorgsector

- De patiënt
- De administratieve lasten beperken.
- Beheren van (oudere) IoMT-apparaten en de opkomst van draagbare medische apparaten
- Beheren van nieuwe regelgevingen

ANNACON

Ziekenhuistoestellen makkelijk te hacken door verouderde besturingssystemen, blijkt uit test

Heel wat ziekenhuistoestellen kunnen gehackt worden. Dat blijkt uit een test door ethische hackers van Check Point. Check Point test regelmatig de veiligheid van toestellen die aan het internet verbonden zijn. Veel van die ziekenhuistoestellen draaien op een verouderd besturingssysteem. Het

Beheren van oudere IoMT-apparaten

- Leverancier werkt niet altijd mee als het gaat over veiligheid/updaten van apparaten
- Oudere/onveilige besturingssystemen
- Connectiviteit nodig met het netwerk voor uitslag testen/foto’s

ANNACON

Opkomst van draagbare apparaten

- Nieuwe technologie: de patiënt levert data aan
- Uitleenbare toestellen door het ziekenhuis

ANNACON

Beheren nieuwe regelgeving

- NIS2

Onze weg voorwaarts?

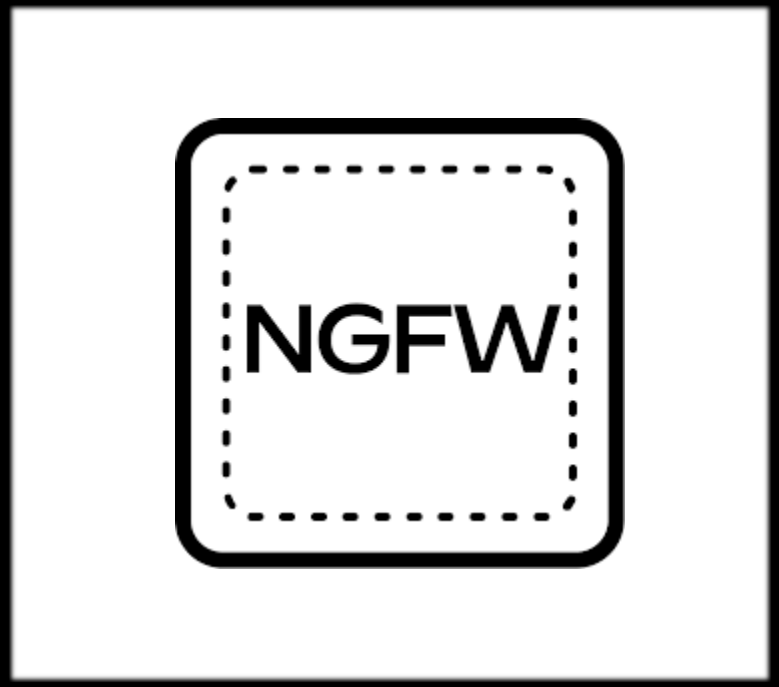
- Consolidatie
- Visie
- Kennisdeling

ANNACON

Security visie az Vesalius

- Basis van NIST & CIS-controls opgesteld
- Toekomstvisie voor 3 jaar
- Vooral ingezet op consolidatie van tools en A.I./Machine learning

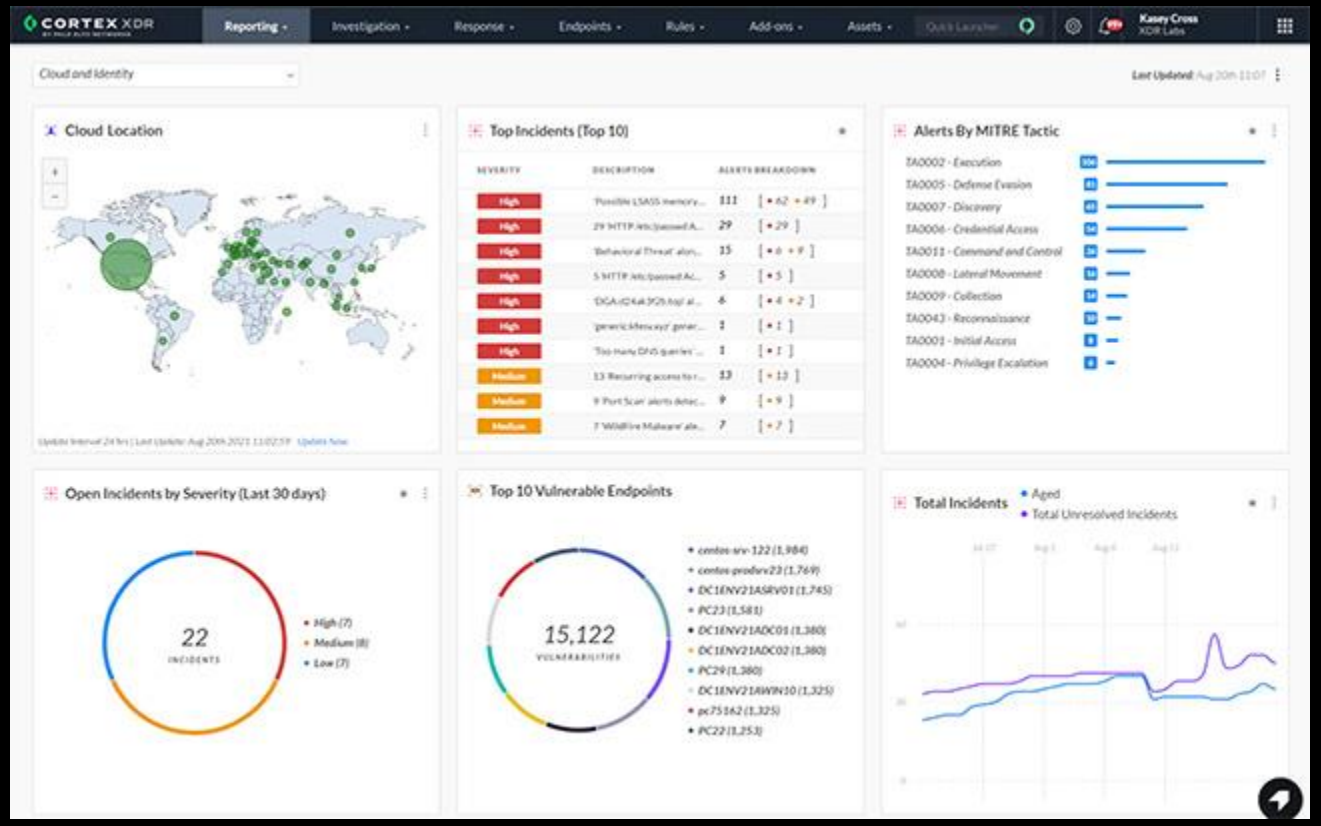
ANNACON



Vlan-segmenting en firewalling

- Aankoop nieuwe generatie firewall
- Meer dan 50 Vlans
- Continue verbetering via BPA en checkups

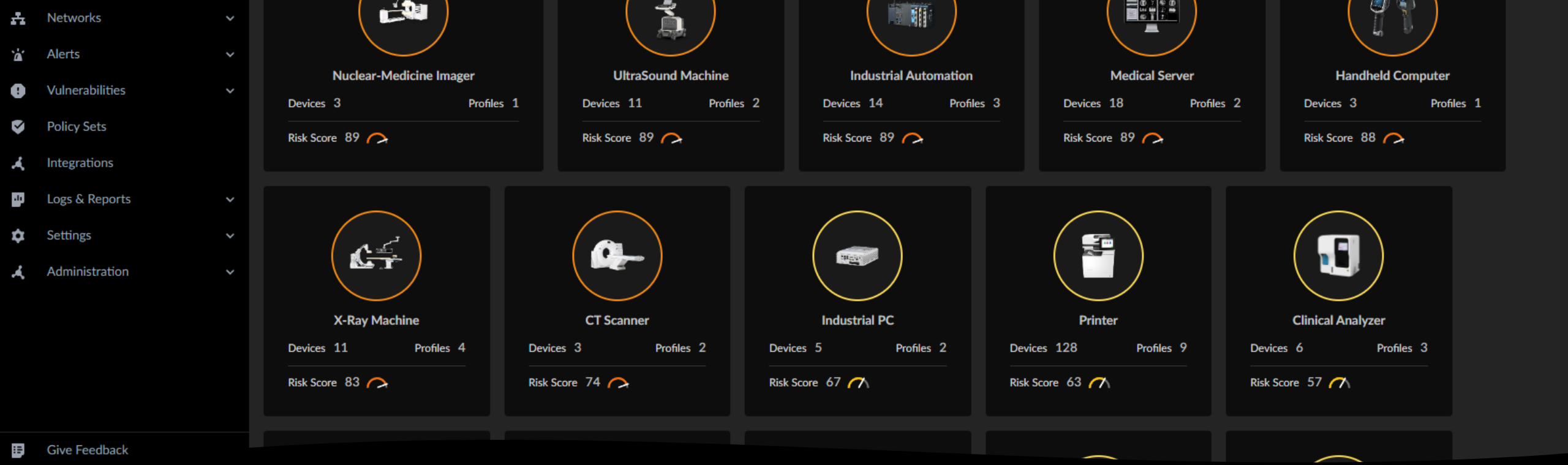
ANNACON



XDR & Data Lake

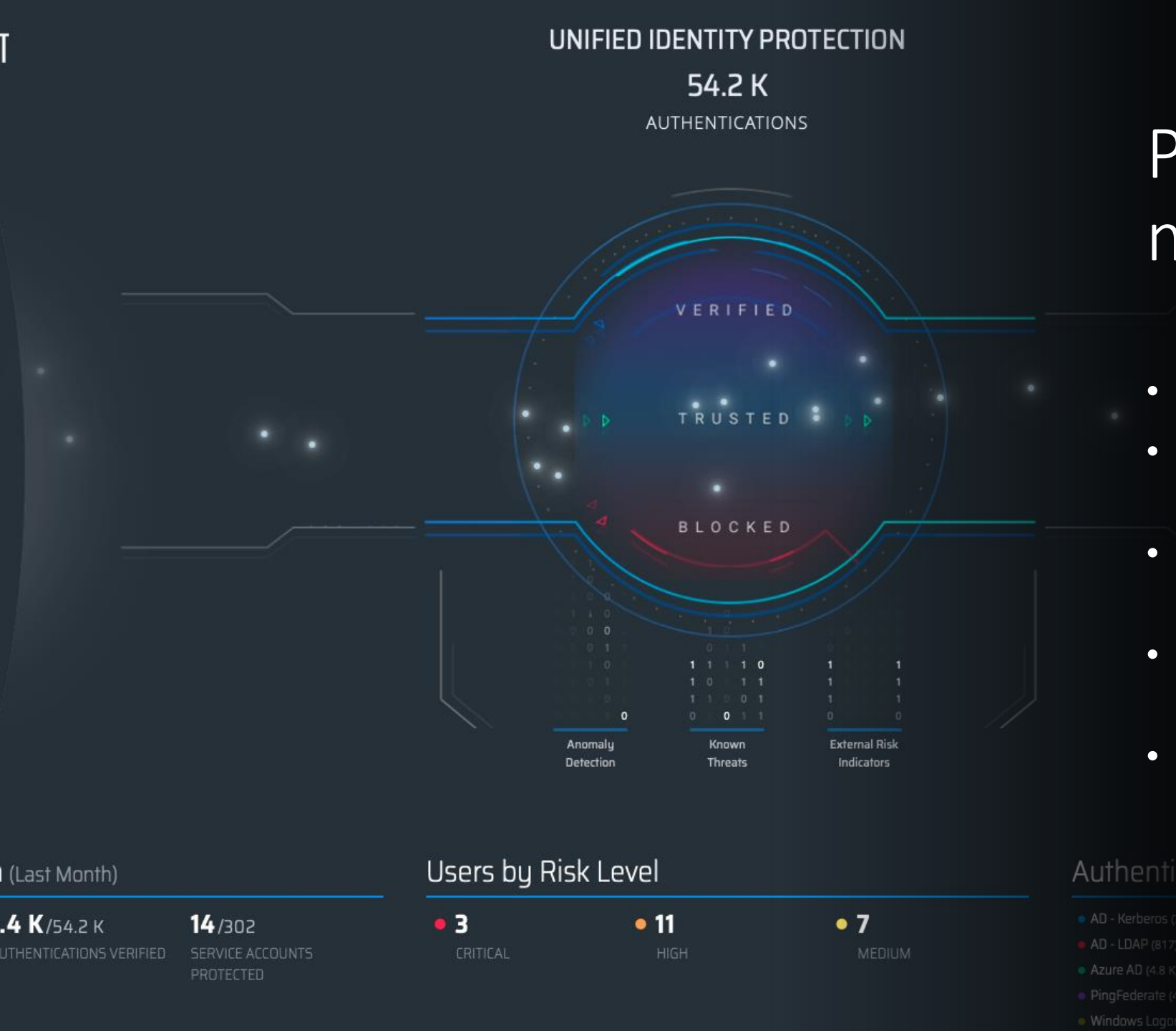
- XDR op alle eindstations en servers
- Alle logs worden naar het data lake verstuurd (inclusief firewall, DC, DNS, O365, event-logs, IIS-logs, Silverfortlogs, …)
- A.I. en machine learning geven abnormaal gedrag weer
- 3 maanden doorlooptijd alvorens de basis en allowlisting in orde was.

ANNACON



IoMT-security

- Iot uitbreiding op firewall
- Scant netwerken op IOT en IoMT apparaten
- A.I. en machine learning geven abnormaal gedrag weer
- Geeft kwetsbaarheden weer van de apparaten en foute/standaard instellingen en paswoorden.



Privileged access management

- PAM op all service accounts
- Gevoelige accounts extra beveiligt met MFA
- A.I. en machine learning geven abnormaal gedrag weer
- Extra beveiligingen op creatie nieuwe administrator accounts
- Zelfs op IoMT apparaten zit er beveiliging en MFA tussen.

ANNACON

Toekomst?

- ISO-27001 certificatie (NIS2)
- POC van automated SOC (XSOAR)
- Opnemen van laatste logs in Cortex Data Lake (F5)
- Noodplan/IRP oefeningen
- Samenwerken met andere ziekenhuizen!

ANNACON

Wat kunnen we doen in de zorgsector?

- Cyber security coalition: werkgroepen om de diverse problemen aan te pakken en kennisdeling beschikbaar te maken
- Meer samenwerking en kennisdeling
- Meer inzetten op gezamenlijke initiatieven (Netwerkziekenhuizen)
- Nieuw initiatief: Shield vzw
- Zorgen voor een visie/plan!

ANNACON

Shield vzw

- Nieuw initiatief: Shield vzw
- Samenwerking door Ziekenhuis Oost-Limburg, Jessa ziekenhuis, Universiteit Hasselt

SHIELD vzw

Ziekenhuis Oost-Limburg

jessa ZIEKENHUIS

UHASSELT

Bedankt!