Shield event · Q1-2025

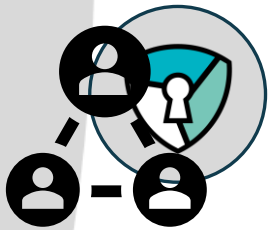
11/03/2025 – Van der Valk – Brussels Airport

Shield Update

Dr. Wim Bijnens
Shield vzw

The 3 pillars of SHIELD

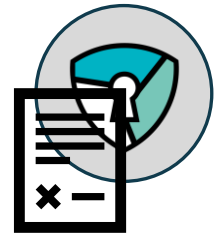
Partner management &
Technology selection



Community

Service catalogue

Partner management & Technology selection



Focus Area GRC

TOREON
Business driven cyber consulting

nviso

Focus Area Endpoint Security

Dustin

BECHTLE

Focus Area SOC

- XDR

JARVISS

CORTEX
BY PALO ALTO NETWORKS

nviso

Microsoft Defender

Focus Area Network Security

- Firewall

paloalto NETWORKS

JARVISS

NTT DATA

CISCO

NTT DATA

spotit
YOUR SECURITY & NETWORK LAYER

Partner management & Technology selection

Coming very soon…

Focus Area
SOC

CSIRT
Thales
Nviso
Spotit

Focus Area
Network Security

Pentest
Intigriti

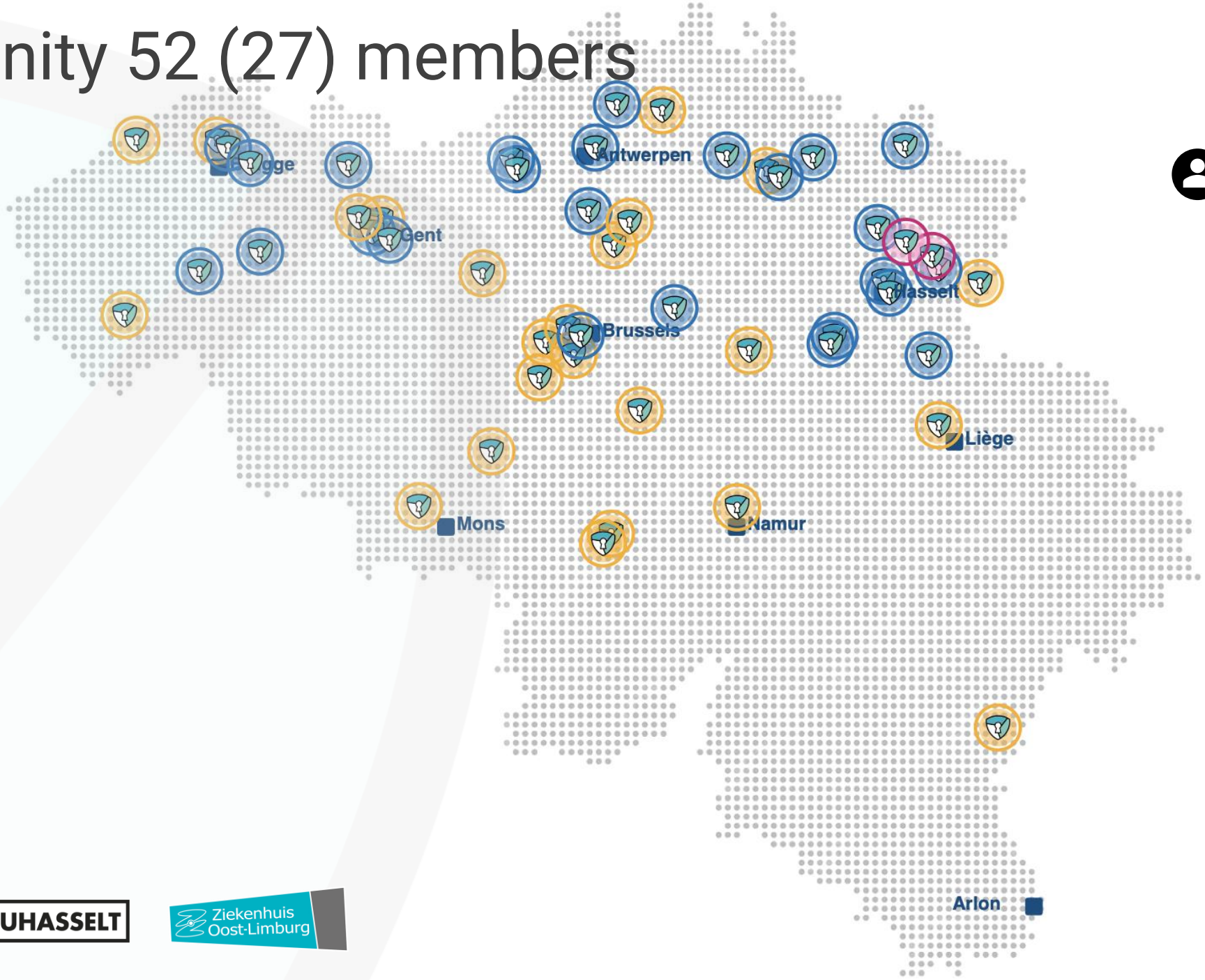
Focus Area
Awareness

Awareness
NRB
The Security Factory
Infosentry

Project proposals are being prepared

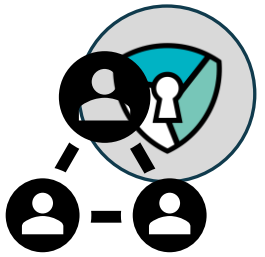
Info session - Safe the date: April, 23rd – 2025 – 16:00

Community 52 (27) members



Shield event – 11/03/2025

Community 52 (27) members



Direct Members Hospitals/Higher Education

az alma zorg met een hart · AZ Herentals · H. Hartziekenhuis Mol · Maria Middelares · azdelta · AZ Sint-Vincentius Deinze · noorderhart · Sint-Andries Ziekenhuis Tielt · AZ Klina · az Rivierenland · SFZ · trudo · azVesalius · az sint-lucas Brugge · UZ Leuven · Uhasselt · Jessa Ziekenhuis · CHirec · Vitaz · ZAS · Ziekenhuis Geel · Ziekenhuis Oost-Limburg

Direct Members Care Providers

covida · IGL

Direct Members Psychiatric Care

Bermhertigheid Jesu · Broeders van Liefde · asster · Groep SON

PoC Members

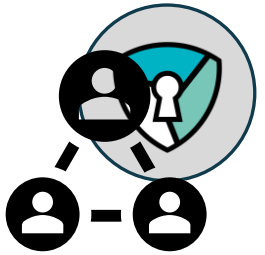
azsintlucasgent · AZ Sint-Jan Brugge · JYZ Jan Yperman Ziekenhuis · Openbaar Psychiatrisch Zorgcentrum Rekem · AZ Oostende · AZ Voorkempen · OPZ Geel · Sint-Maarten · AZORG · Bethanië · Vivalia · HUman · CHU Saint-Pierre UMC Sint-Pieter · CHR Haute Senne · Hôpital Erasme ULB · Epsylon · CHC Groupe Santé · Clinique Saint-Luc Bouge · EpiCURA · Grand Hôpital de Charleroi · Sint-Maria Halle · Clinique St Pierre Ottignies · AZ Jan Palfijn Gent · UPC Duffel · rz tienen

Jessa Ziekenhuis · Uhasselt · Ziekenhuis Oost-Limburg

SHIELD vzw

Shield event – 11/03/2025

Community call-out!

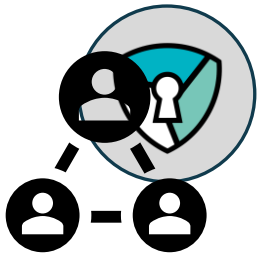


We're still looking for community contributors/technical experts to:

- Extend/join the existing workgroups:
  - GRC
  - XDR // Sectorial SOC
  - Network Security – Firewall
- Support the Shield initiatives for 2025:
  - Focus Area Network security:
    - Campus/DC networking & (micro) segmentation
  - Focus Area (Private) Cloud & datacenter:
    - Datacenter hardware & storage
    - Backup & recovery
  - Focus Area Endpoint security:
    - Asset mgmt & insights, CPS platforms & vulnerability management

Contact: wouter.demuynck@shield-vzw.be

Save the date!



Info-session on the ongoing Shield projects:

- Awareness
- CSIRT
- Bug bounty pentesting

A webinar will be hosted on April, 23rd – 2025 – 16:00

Service catalogue – reference architecture - GRC

NIS2 Management Training

NIS2 is sinds oktober 2024 van kracht. Organisaties die als essentieel aangeduid werden **moeten vanaf eind april 2025 voldoen aan vereisten rond awareness en training van leidinggevenden**, met name over NIS2 specifieke verplichtingen, risk management en incident management. Deze opleiding is belangrijk omdat **leidinggevenden persoonlijk aansprakelijk zijn voor compliance aan de wetgeving**. De omschreven training voldoet aan de eisen voor jaarlijkse awareness en training onder NIS2.

Deze training heeft als doel om een **grondig inzicht te bieden in de NIS2-richtlijn**, de **gevolgen ervan** voor uw organisatie, en de **stappen die nodig zijn om aan de vereisten te voldoen**, specifiek gericht op senior management, directie en raad van bestuur.

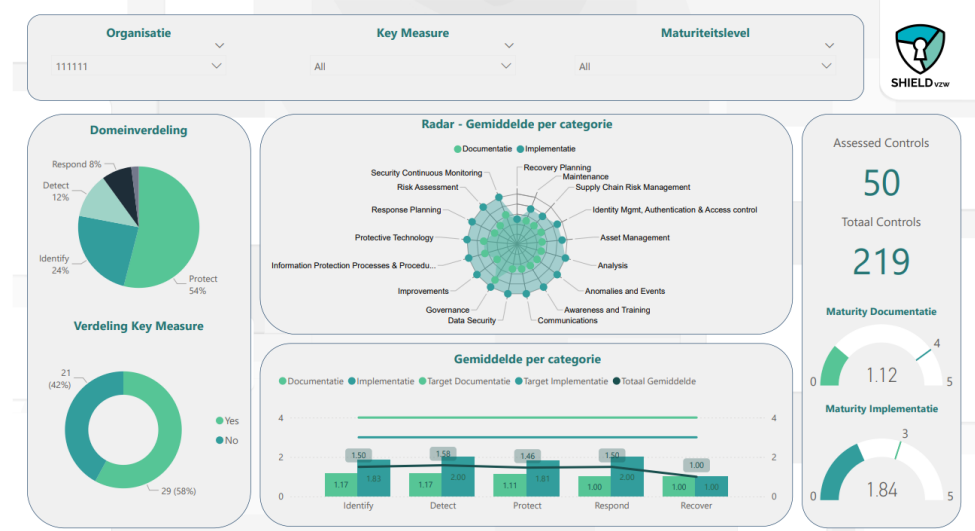
Roadmap

1. **Inleiding tot NIS2**
   - **Wat betekent NIS2 voor de zorgsector.**
   - **Wat is de implementatietimeline volgens de wetgeving**
   - **Welke stappen kan U zetten om compliant te worden**
2. **Governance en Verantwoordelijkheid**
   - **Uw verantwoordelijkheden als bestuurder onder NIS2**
   - **Hoe u aansprakelijkheid en persoonlijke sancties voorkomt**
   - **Welke concequenties zijn er bij niet-compliance**
3. **Risicogebaseerde Aanpak**
   - **Cybersecurity is niet alleen een IT-aangelegenheid;** cybersecurity verankeren in de zorginstelling
   - **Risicobeoordeling en risicomanagement**
4. **Beveiligingsmaatregelen (minimale vereisten NIS2)**

   Een robuuste cybersecuritystrategie gaat verder dan compliance. Zorg ervoor dat uw organisatie bestand is tegen cyberdreigingen met de juiste maatregelen:
   - **Bedrijfscontinuïteit:** back-ups, disaster recovery & crisismanagement
   - **Beveiliging bij ontwerp:** veilige configuraties en best practices
   - **Cryptografie & versleuteling:** bescherming van gevoelige data
   - **Patch management:** kwetsbaarheden snel en effectief verhelpen
5. **Incidentbeheer en Kwetsbaarheidscoördinatie**

   Een cyberincident kan grote gevolgen hebben. Wat te doen bij een 'significant incident'?
   - Procedures voor incidentafhandeling & kwetsbaarheidsmeldingen
   - Passende technische en organisatorische maatregelen
   - Wat zijn 'significante incidenten' en de hoe zit het met de meldingsplicht
6. **Leveranciersbeheer – Cyberveiligheid in de supplychain**
   - **Het belang van cybersecurity binnen de supply chain**
   - **Afspraken maken met leveranciers over cyberveiligheid**
   - **Beoordelen van third-party risico's en continu monitoren**
7. **Implementatie binnen de zorgorganisatie**
   - **Governance: rol van de CISO, Security Board, rapportagelijnen**
   - **Effectieve samenwerking tussen Security, IT, DPO, Legal en Management**
   - **Cultuurverandering: van 'checklist-compliance' naar 'cyber resilience'**

Shield vzw
Kempische Steenweg, 303/200
3500 Hasselt
www.shield-vzw.be



	Complete Service	Costs	Internal effort***	Domains
Governance	Template documentation*	**	1 MD	Document management accountable, CISO, DPO
	Alignment of (templated) documentation by expert	24 MD	40 MD	Engineer (Infra / application/ Workplace/ Security) CISO, CIO, CEO, DPO, CHRM, Purchasing admin HR admin
	Implementation of (templated) documentation by expert	10 MD	2 MD	Quality accountable, Document management accountable, CEO
Risk	15 example risks	2 MD	1 MD	CISO
	Evaluation of the risk assessment (review and applicability of 15 example risks) by expert	10 MD	2 MD	CEO, CIO, DPO
	Review and registration of risk register by expert	2 MD	1 MD	CISO, DPO
Compliance	Execution of internal audit by expert	10 MD	5 MD	Engineer (Infra / application/ Workplace/ Security) CISO, CIO, CEO, DPO, CHRM, Purchasing admin HR admin
	Implementation and/or configuration of compliance measuring tool by expert	2 MD	1 MD	Quality accountable, DPO, CISO
	Total costs	60 MD	53 MD	

Medical Device

This Medical Device Policy exists to help hospitals systematically identify, evaluate, and mitigate information security risks inherent to medical devices, which ultimately compromise patient safety and data integrity. By adopting a risk-based approach grounded in established frameworks such as ISO27001:2022, ENISA and CyFun organizations can handle security challenges through structured steps like inventory management, robust access control, ongoing vulnerability assessment, and incident response.

The policy is particularly designed for hospitals with no existing implementation of measures or even if some measures may already exist to address risks related to the processing, storage, or transmission of information, providing them with key foundational guidelines.

Definition:

A medical device is an instrument, apparatus, software, implant, or other article intended by the manufacturer for medical purposes such as diagnosis, treatment, monitoring, or compensation for conditions or disabilities. It does not primarily function through pharmacological, immunological, or metabolic means.

This policy applies exclusively to medical devices that:

- Process sensitive (personal) data to support the healthcare process, or
- Influence or automate decision-making within the healthcare process.

Risk Classification:

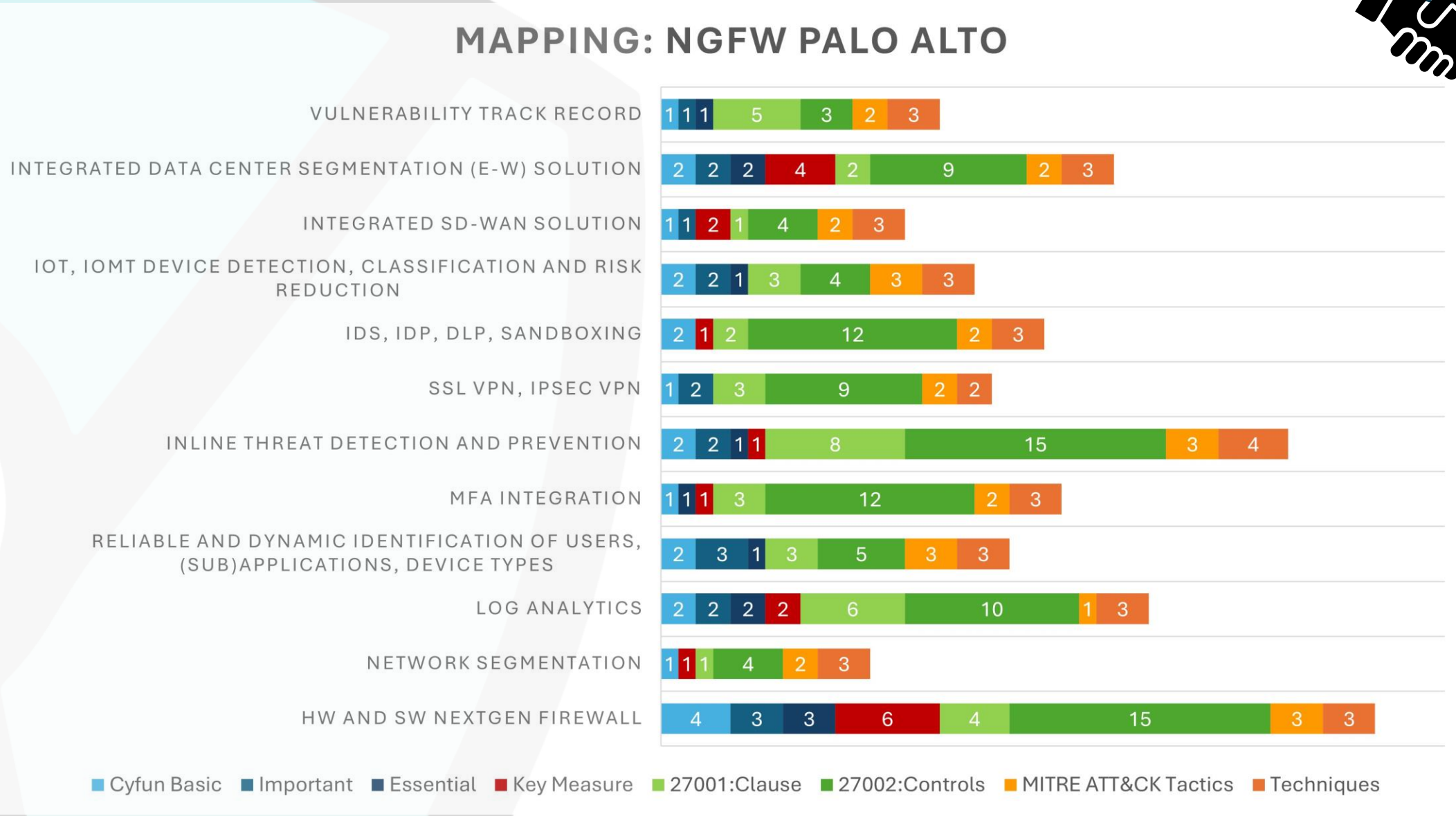
Category of information	MDR Medical Device Class			
	Class I	Class IIa	Class IIb	Class III
Special Personal Data	5	5	5	5
Information Decision for the Care Process	3	3	4	5
Ordinary Personal Data	2	2	3	5
Information Supporting the Care Process	1	2	3	5

Summary table of the 5 risk class scale of medical devices

Shield vzw
Kempische Steenweg 303/200
3500 Hasselt
www.shield-vzw.be

Service catalogue – reference architecture

Firewall NGWF Palo Alto



Service catalogue – reference architecture

Firewall NGWF Palo Alto

	HW and SW NextGen Firewall	Log analytics	Network Segmentation & MFA Integration	Inline Threat Detection and Prevention
	Cyfun Control PR.AC-5 (Identity Management, Authentication and Access Control) DE.AE-3.1 (Anomalies and Events) DE.CM-1 (Security Continuous Monitoring) **Cyfun Level** Basic : 4 (PR.AC-5.1, PR.AC-5.2, DE.AE-3.1, DE.CM-1.1) Important : 3 (PR.AC-5.3, PR.AC-5.4, DE.CM-1.2) Essential : 3 (PR.AC-5.5, PR.AC-5.6, DE.CM-1.3) Key Measures : 6 (PR.AC-5.1, PR.AC-5.2, PR.AC-5.3, PR.AC-5.4, DE.AE-3.1, DE.CM-1.2)	**Cyfun Control** PR.PT-1.1, PR.PT-1.2 (Protective Technology) DE.AE-2.2, DE.AE-3 (Anomalies and Events) **Cyfun Level** Basic : 2 (PR.PT-1.1, DE.AE-3.1) Important : 2 (PR.PT-1.2, DE.AE-3.2) Essential : 2 (DE.AE-2.2, DE.AE-3.3) Key Measure : 2 (PR.PT-1.1, DE.AE-3.1)	**Cyfun Control** PR.AC-5.2 (Identity Management, Authentication and Access Control), MFA: PR.AC-1.4, PR.AC-3.2 (Identity Management, Authentication and Access Control) **Cyfun Level** Basic : 2 (PR.AC-5.2, PR.AC-3.2) Important : / Essential : 1 (PR.AC-1.4) Key Measure : 2 (PR.AC-5.2, PR.AC-3.2)	**Cyfun Control** ID.RA-1.1 (Risk Assessment) DE.CM-1, DE.CM-3.2 (Security Continuous Monitoring **Cyfun Level** Basic : 2 (ID.RA-1.1, DE.CM-1.1) Important : 2 (DE.CM-1.2, DE.CM-3.2) Essential : 1 (DE.CM-1.3) Key Measure : 1 (DE.CM-1.2)
ISO	**ISO 27001:2022** PR.AC-5 : Clause 8.1, Annex A DE.AE-3.1 : Clause 8.1, Clause 9.1, Clause 10.2, Annex A DE.CM-1: Clause 8.1, Clause 9.1, Clause 9.2 Annex A **ISO 27002:2022** PR.AC-5 : Controls 5.14, 8.20, 8.22, 8.26 DE.AE-3.1 : Controls 5.7, 5.24, 5.25, 5.28, 8.12, 8.15, 8.16, 8.17 DE.CM-1: Controls 5.7, 5.22, 8.8, 8.12, 8.15, 8.16, 8.17, 8.21	**ISO 27001:2022** PR.PT-1.1: Clause 7.5.2, Clause 7.5.3, Clause 9.1, Clause 9.2, Annex A PR.PT-1.2: Clause 7.5.2, Clause 7.5.3, Clause 9.1, Clause 9.2, Annex A DE.AE-2.2: Clause 8.1, Clause 9.1, Clause 10.2, Annex A DE.AE-3 : Clause 8.1, Clause 9.1, Clause 10.2, Annex A **ISO 27002:2022** PR.PT-1.1: Controls 5.37, 8.15, 8.17, 8.34 PR.PT-1.2: Controls 5.37, 8.15, 8.17, 8.34 DE.AE-2.2 : Controls 5.7, 5.24, 5.25, 8.15 DE.AE-3: Controls 5.7, 5.24, 5.25, 5.28, 8.12, 8.15, 8.16, 8.17	**ISO 27001:2022** PR.AC-5.2 : Clause 8.1, Annex A MFA: PR.AC-1.4 : Clause 6.1.1, Clause 8.1, Annex A, PR.AC-3.2 : Clause 7.5.2, Clause 8.1, Annex A **ISO 27002:2022** PR.AC-5.2 : Controls 5.14, 8.20, 8.22, 8.26 MFA: PR.AC-1.4 : Controls 5.16, 5.17, 5.18, 8.2, 8.3, 8.5, PR.AC-3.2 : Controls 5.14, 6.7, 7.9, 8.1, 8.5, 8.11, 8.20	**ISO 27001:2022** ID.RA-1.1 : Clause 6.1.2,Clause 6.1.3, Clause 7.5.2, Clause 8.2, Clause 8.3, Annex A, DE.CM-1 : Clause 8.1, Clause 9.1, Clause 9.2 Annex A, DE.CM-3.2 : Clause 8.1, Clause 9.1, Annex A **ISO 27002:2022** ID.RA-1.1 : Controls 5.36, 8.8, 8.33 DE.CM-1 : Controls 5.7, 5.22, 8.8, 8.12, 8.15, 8.16, 8.17, 8.21 DE.CM-3.2 : Control 5.7, 8.1, 8.7, 8.12, 8.15, 8.16, 8.19, 8.20, 8.23
MITRE ATT&CK	**MITRE ATT&CK Tactics & Techniques** Initial Access: T1133 (External Remote Services) Command and Control: T1071 (Application Layer Protocol) Defense Evasion: T1562 (Impair Defenses)	**MITRE ATT&CK Tactics & Techniques** Discovery / Detection: Many techniques become visible through logs (e.g., T1016 System Network Config Discovery, T1049 System Network Connections Discovery), Detection of T1059 (Command & Scripting Interpreter)	**MITRE ATT&CK Tactics & Techniques** Lateral Movement: T1021 (Remote Services), T1570 (Lateral Tool Transfer), Defense Evasion / Privilege Escalation (restricting adversary's ability to move laterally or pivot) MFA: Credential Access: T1110 (Brute Force), T1078 (Valid Accounts), Defense Evasion / Privilege Escalation: Harder for attackers to escalate if MFA is enforced	**MITRE ATT&CK Tactics & Techniques** Initial Access: T1566 (Phishing), T1190 (Exploit PublicFacing App) Command and Control: T1071 (Application Layer Protocol) Malware Delivery: T1204 (User Execution)

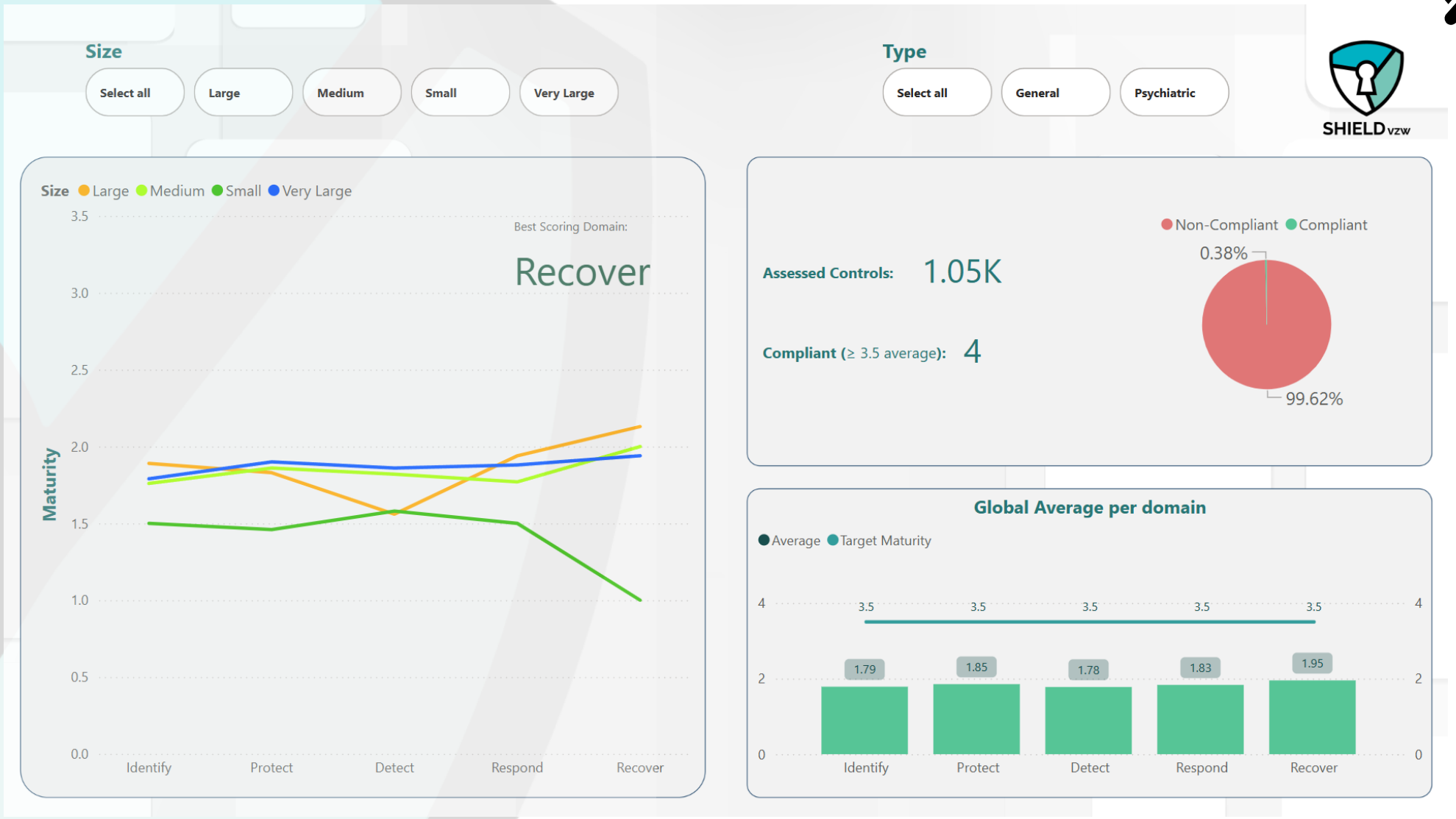
Service catalogue – reference architecture

MDP – Risk scoring

Medical Device		Device Application		MDR	Data Categories				Environment Risk			Risk Classification		
Types	Types Notes	Sub-types	Sub-type Notes	MDR Cl	Supporting Care Informat…	Ordinary Personal	Special Personal Data	Decisive care Informat…	Clinical Environeme	Invasivenes	Fallback / Redundanc	Risk Sum	Risk Score	Risk Interpretatio
Angiography	Imaging of blood vessels using contrast dye and X-rays.	Diagnostic Angiography	Typically lower risk, as it involves imaging without extensive intervention.	Class IIb	Yes	Yes	Yes	Yes	Ancillary / Diagnostic	Invasive / Surgical	No Redundancy	17	5	Severe (Highest) Risk
Angiography	Imaging of blood vessels using contrast dye and X-rays.	Interventional Angiography	Medium to high risk due to invasive procedures (e.g., stent placement, embolization).	Class IIb	Yes	Yes	Yes	Yes	Medium-Acuity Inpatient	Invasive / Surgical	No Redundancy	14	4	High Risk
Angiography	Imaging of blood vessels using contrast dye and X-rays.	Emergency / Trauma Angiography	Often critical risk because of urgent, life-saving interventions in unstable patients.	Class IIb	Yes	Yes	Yes	Yes	High-Acuity / Critical Care	Invasive / Surgical	No Redundancy	16	5	Severe (Highest) Risk
Central Stations	Centralized hubs aggregating patient data from multiple monitors.	ICU / High-Acuity Monitoring	Used in critical care settings (ICUs, CCUs) to aggregate and display multiple vital signs from highly acute patients (e.g. invasive blood pressure, advanced respiratory parameters).	Class IIb	Yes	Yes	Yes	Yes	High-Acuity / Critical Care	Non-Invasive	Partial Redundancy	15	4	High Risk
Central Stations	Centralized hubs aggregating patient data from multiple monitors.	Telemetry / Cardiac Monitoring	Primarily focused on continuous cardiac telemetry (ECG) for patients needing real-time rhythm surveillance.	Class IIb	Yes	Yes	Yes	Yes	Medium-Acuity Inpatient	Non-Invasive	Partial Redundancy	14	4	High Risk
Central Stations	Centralized hubs aggregating patient data from multiple monitors.	General Ward / Multi-Parameter Monitoring	Central station used in lower-acuity or general ward environments for basic vital signs (e.g., heart rate, SpO_2, blood pressure) from multiple bedside monitors.	Class IIa	Yes	Yes	Yes	Yes	Medium-Acuity Inpatient	Non-Invasive	Partial Redundancy	12	4	Moderate Risk
CR Systems	Computed radiography using digital imaging plates for X-ray capture.	General Radiography CR	CR systems Used for chest, skeletal, abdominal imaging.	Class IIb	Yes	Yes	Yes	Yes	Ambulatory / Outpatient	Non-Invasive	Partial Redundancy			
CR Systems	Computed radiography using digital imaging plates for X-ray capture.	Mobile / Emergency CR	Dedicated portable CR systems (used in wards, ICUs, operating rooms).	Class IIb	Yes	Yes	Yes	Yes	High-Acuity / Critical Care	Non-Invasive	Partial Redundancy			
CTs	Computed tomography scanners for cross-sectional body imaging.	General Diagnostic CT	Used for routine scanning (e.g., head, abdomen, chest) in outpatient or inpatient settings	Class IIb	Yes	Yes	Yes	Yes	Medium-Acuity Inpatient	Non-Invasive	Partial Redundancy			
CTs	Computed tomography scanners for cross-sectional body imaging.	Emergency / Trauma CT	Positioned for rapid, high-priority scans in emergency departments and trauma centers	Class IIb	Yes	Yes	Yes	Yes	High-Acuity / Critical Care	Non-Invasive	No Redundancy			
ECGs	Devices recording the electrical activity of the heart.	Resting ECG	Standard, brief ECG recording, often used for routine check-ups, pre-operative screenings, or diagnosing basic arrhythmias.	Class IIa	Yes	Yes	Yes	Yes	Ambulatory / Outpatient	Non-Invasive	Full Redundancy			
ECGs	Devices recording the electrical activity of the	Stress / Exercise ECG	Used to evaluate cardiac function under stress	Class IIb	Yes	Yes	Yes	Yes	Medium-Acuity Inpatient	Non-Invasive	Full Redundancy			

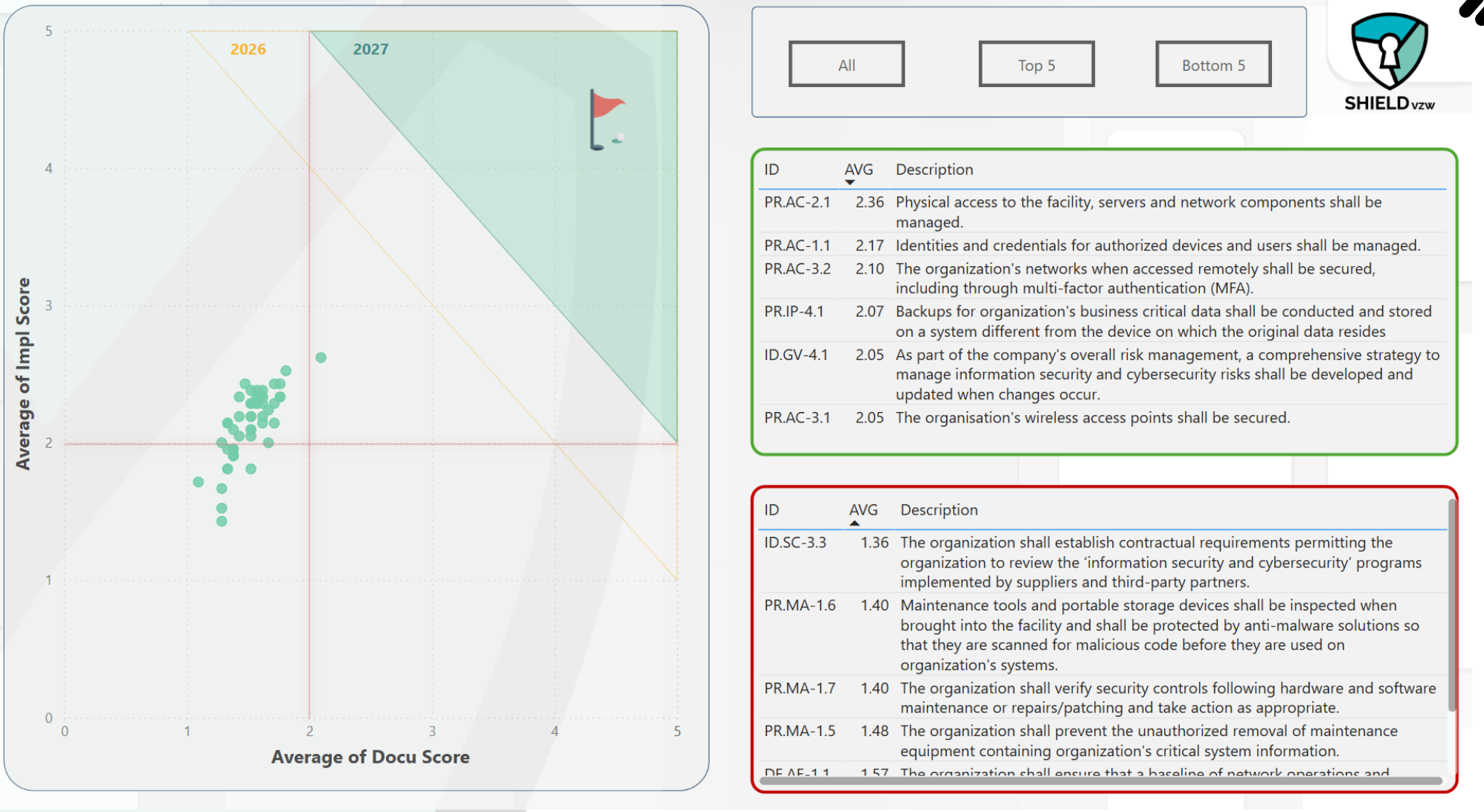
Service catalogue – reference architecture

Assessments and GRC service



Service catalogue – reference architecture

Assessments and GRC service



All | Top 5 | Bottom 5

SHIELD vzw

ID	AVG	Description
PR.AC-2.1	2.36	Physical access to the facility, servers and network components shall be managed.
PR.AC-1.1	2.17	Identities and credentials for authorized devices and users shall be managed.
PR.AC-3.2	2.10	The organization's networks when accessed remotely shall be secured, including through multi-factor authentication (MFA).
PR.IP-4.1	2.07	Backups for organization's business critical data shall be conducted and stored on a system different from the device on which the original data resides
ID.GV-4.1	2.05	As part of the company's overall risk management, a comprehensive strategy to manage information security and cybersecurity risks shall be developed and updated when changes occur.
PR.AC-3.1	2.05	The organisation's wireless access points shall be secured.

ID	AVG	Description
ID.SC-3.3	1.36	The organization shall establish contractual requirements permitting the organization to review the 'information security and cybersecurity' programs implemented by suppliers and third-party partners.
PR.MA-1.6	1.40	Maintenance tools and portable storage devices shall be inspected when brought into the facility and shall be protected by anti-malware solutions so that they are scanned for malicious code before they are used on organization's systems.
PR.MA-1.7	1.40	The organization shall verify security controls following hardware and software maintenance or repairs/patching and take action as appropriate.
PR.MA-1.5	1.48	The organization shall prevent the unauthorized removal of maintenance equipment containing organization's critical system information.
DE.AE-1.1	1.57	The organization shall ensure that a baseline of network operations and


Q
A

THANK YOU!

Dr. Wim Bijnens
wim.bijnens@shield-vzw.be
+32 495 59 02 35