Shield vzw

A Cyber oriented non-profit for Healthcare & Education

Stronger Together

Kurt Gielen
COO - Shield vzw

The challenges

We find ourselves in the eye of what could be a perfect storm

- Poorly funded sectors (at least with regards to the cyber domain)
  - Under-staffed
  - Under-skilled
  - Budgettary constraints
- Very valuable information
- Very complex organizations (we do everything –ourselves-)
- Employer attractiveness (not very competitive)
- Open organizations
  - Employees
  - Contractors
  - Doctors
  - Patients & Visitors
  - Students….
- Increasing regulatory obligations

The challenges

Yet….

- The sector is a major player in the socio-economic sphere with potential corresponding weight
- Every hospital/university lacks people and skills, but the sector as a whole has numerous specialists (although tied up in other things)
- Every hospital/university lacks resources, yet is reinventing the wheel time and time again
- Every hospital/university is tied up in long and complex purchasing processes, yet we all need the same equipement and services to solve the same problems

==> Major opportunities for deep cooperation

That is where Shield comes in

- Build an all-encompassing sectoral Cyber Resilience architecture blueprint. Focus of People, Processes and Technology. Both GRC and Tech matter
- Build a sector member initiative by and for it's members, aiming for deep, non-opportunistic cooperation. No therapy sessions, but deliverable driven
- Unlock the weight potential of the sector and it's existing specialists through active community working. Engineers in the drivers seat and reward them
- Offer a complete catalogue of products and services, delivered by both Shield and partners.
- Take away the burden of administrative and legal aspects in purchasing

"Shield vzw – STRONGER TOGETHER"

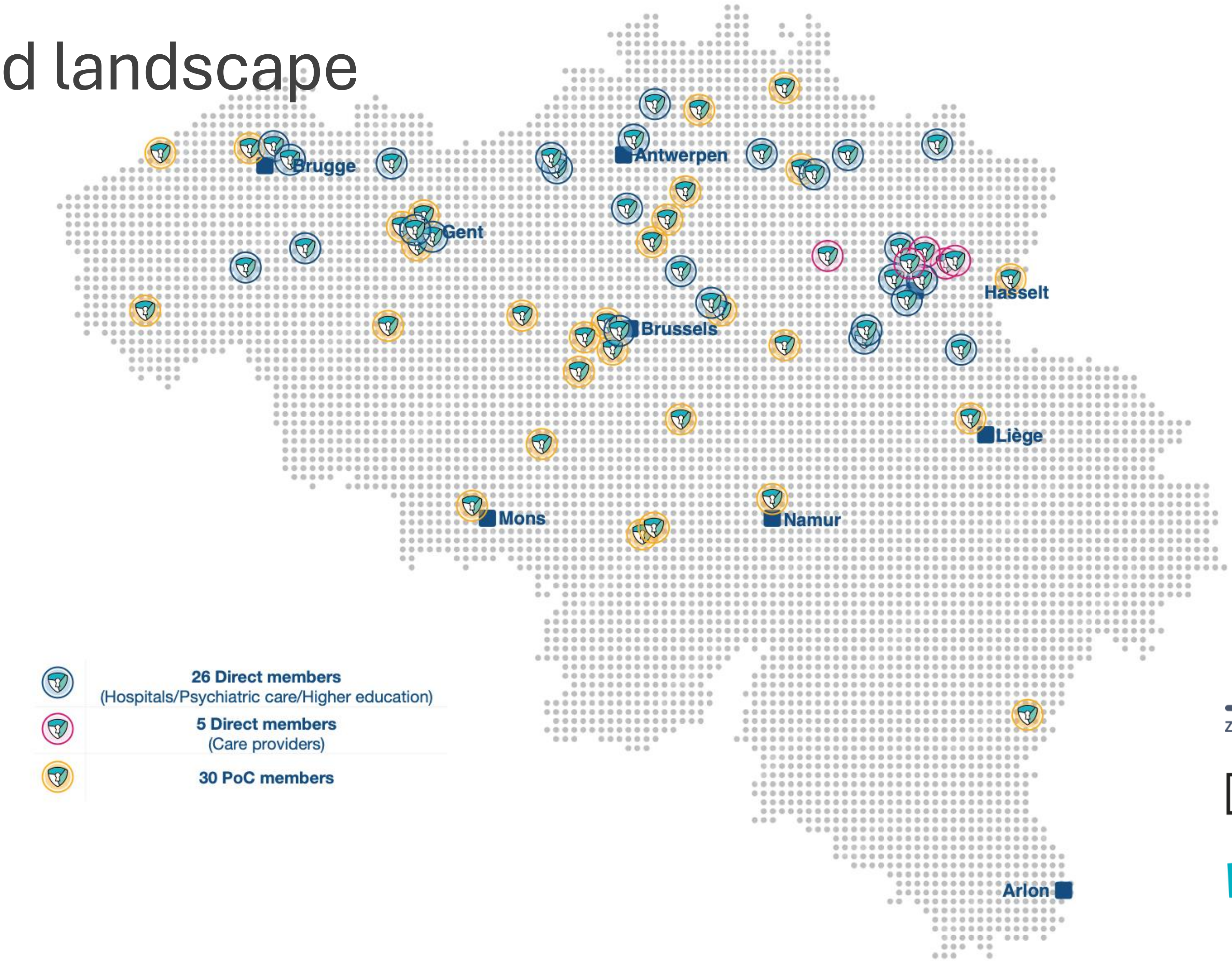
NON-PROFIT, COMMUNITY-DRIVEN SERVICE HUB FOR AND BY MEMBERS

SHIELD vzw

Founded Nov/23, Operational Jun/24

New members – Shield vzw

Shield landscape



● **26 Direct members**
(Hospitals/Psychiatric care/Higher education)

● **5 Direct members**
(Care providers)

● **30 PoC members**

Jessa ZIEKENHUIS

UHASSELT

Ziekenhuis Oost-Limburg

New members – Shield vzw

New members – Shield vzw

SHIELD vzw

Direct Members Hospitals/Higher Education (22)

- az alma – zorg met een hart
- AZ herentals
- H. Hartziekenhuis Mol
- Mijn Ziekenhuis
- az delta – Uw ziekenhuis.
- Ziekenhuis Oost-Limburg
- noorder hart
- Sint-Andries Ziekenhuis Tielt – Uw gezondheid, onze zorg.
- AZ Klina – voluit voor zorg
- az Rivierenland
- SFZ – Sint-Franciscus Ziekenhuis
- sint trudo ziekenhuis
- az Vesalius
- az sint-lucas Brugge
- UZ Leuven
- UHasselt
- Jessa Ziekenhuis
- CHirec Hospital Group
- VITAZ sterk in zorg
- ZAS
- Ziekenhuis Geel
- imelda ziekenhuis

Direct Members Care Providers (2)

- covida – waar je woont, werkt, geniet, leeft
- IGL

Direct Members Psychiatric Care (4)

- Bermhertigheid Jesu
- Broeders van Liefde – onderwijs en zorg
- asster
- Groep SON

PoC Members (30)

- azsintlucasgent
- AZ Sint-Jan Brugge
- YyZ – Jan Yperman Ziekenhuis
- Openbaar Psychiatrisch Zorgcentrum Rekem
- AZ Oostende
- AZ Voorkempen – algemeen ziekenhuis emmaüs
- OPZ Geel – Openbaar Psychiatrisch Zorgcentrum
- Sint-Maarten – algemeen ziekenhuis emmaüs
- AZORG
- Bethanië – geestelijke gezondheidszorg emmaüs
- Vivalia
- HUman
- CHU Saint-Pierre UMC Sint-Pieter
- CHR Haute Senne
- Hôpital Erasme ULB
- EPSYLON
- CHC Groupe Santé
- Clinique Saint-Luc Bouge
- EpiCURA – mon hôpital
- Grand Hôpital de Charleroi
- Sint-Maria Halle
- Clinique St Pierre Ottignies
- AZ Jan Palfijn Gent
- UPC Duffel – geestelijke gezondheidszorg emmaüs
- Heilig Hart
- rz tienen
- UZ Gent
- Regionaal ziekenhuis Heilig Hart Leuven
- AZ Oudenaarde vzw
- az turnhout

Jessa Ziekenhuis

UHasselt

Ziekenhuis Oost-Limburg

The 3 pillars of SHIELD

Partner management & Technology selection

- Focus group on priority themes
- Drafting of specifications and framework agreements per focus (group), depending on the sector priorities
- Framework agreement to which members can subscribe

Community

- Members participate in the focus groups that help determine the content and priorities of the service catalogue
- Contributing to the design of the reference architecture and continuous improvement of it
- Knowledge sharing through publications and lectures
- Social community work

Service Catalogue

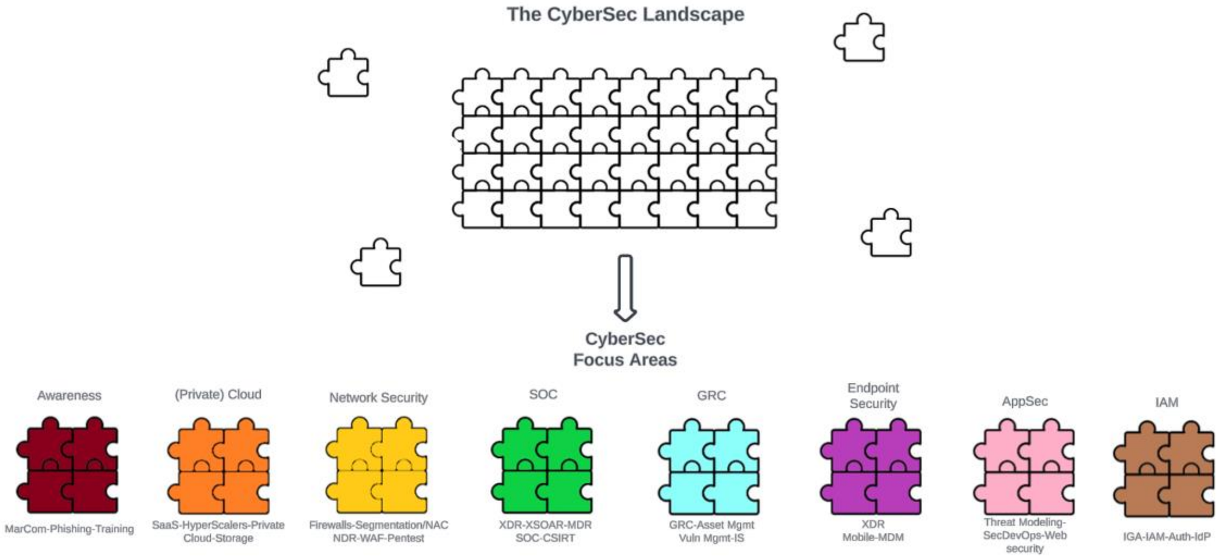
- Service catalogue of technology and services
- Implementation and support of the solutions

SHIELD vzw

New members – Shield vzw

Community operation
Reference architecture

- **MISSION: Building and maintaining a fit-for-use cyber reference architecture**
- Moving target consisting of many sub-aspects: People/Tech/Processes
- Logical grouping in Focus Areas
- Developing a Body-of-Knowledge and associated products and services, by…

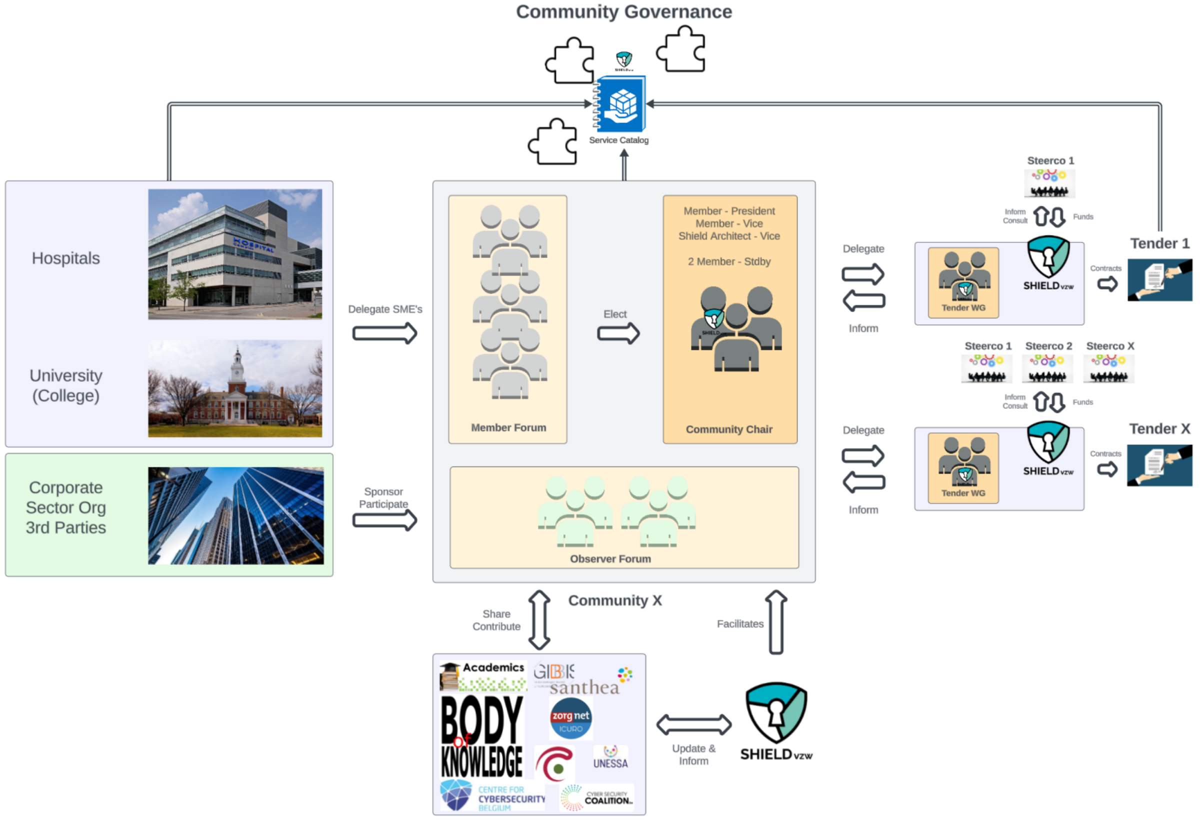


New members – Shield vzw

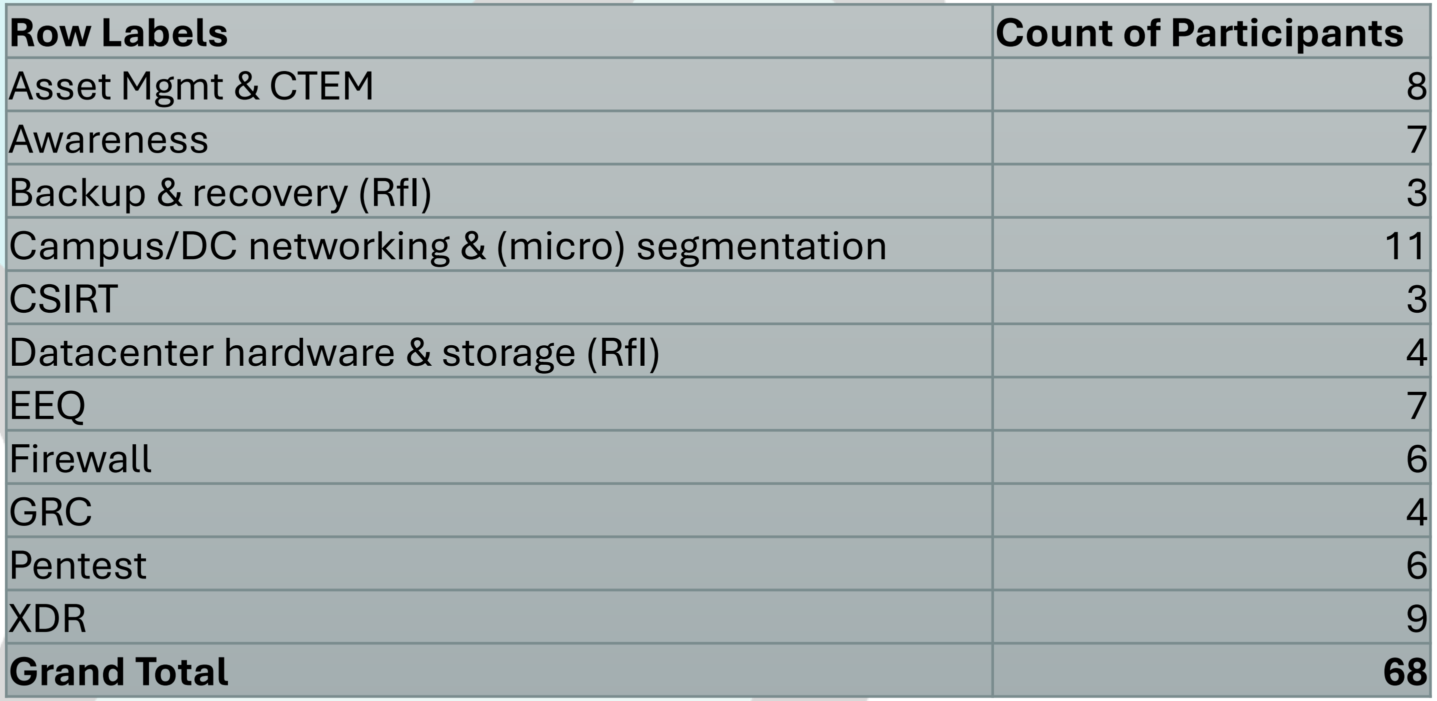
Community operation
Reference architecture

… Developing and facilitating lively community work

- The community gathers the experts from the sector around a focus area
- The community organizes forums for knowledge sharing and assurance
- The community helps build the Shield reference architecture



Community - Working Groups



Row Labels	Count of Participants
Asset Mgmt & CTEM	8
Awareness	7
Backup & recovery (Rfl)	3
Campus/DC networking & (micro) segmentation	11
CSIRT	3
Datacenter hardware & storage (Rfl)	4
EEQ	7
Firewall	6
GRC	4
Pentest	6
XDR	9
Grand Total	**68**

New members – Shield vzw

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

spotit
YOUR SECURITY & NETWORK LAYER

NTT DATA

SHIELD vzw

New members – Shield vzw

SHIELD vzw

Focus Area - Network Security

- Lot 1 – Generic — paloalto NETWORKS
- Lot 2 – Cisco — cisco
- Lot 3 – Palo Alto Networks — paloalto NETWORKS

Shield partners

JARVISS

NTT DATA   spotit YOUR SECURITY & NETWORK LAYER

JARVISS   NTT DATA

Focus Area - SOC

- Solution based on CORTEX BY PALO ALTO NETWORKS
- Solution based on Microsoft Defender

Shield partners

JARVISS

nviso

New members – Shield vzw

Focus Area - GRC

- Toreon
- Nviso

Shield partners

TOREON
Business driven cyber consulting

nviso

Focus Area - Endpoint Security

- Lot 1 - PC's, all-in-one's & workstations: Dustin/Bechtle (cascade)
- Lot 2 – Laptops: Dustin/Bechtle (cascade)
- Lot 3 - Mobile devices: Dustin/Bechtle (cascade)
- Lot 4 - Displays & projectors: Dustin/Bechtle (cascade)
- Lot 5 – Conference: Bechtle
- Lot 6 – Printing: Bechtle

Shield partners

Dustin
bechtle

bechtle

Partner management & Technology selection

Focus Area
SOC
· CSIRT ·

* nviso

THALES

Focus Area
Network Security
· Bug-bounty pentest ·

* INTIGRITI

Focus Area
Awareness

OUTKEPT

* INFOSENTRY
get assured

PHISHED

TSF | THE SECURITY FACTORY

* Proposed solution PoC FPS Public Health

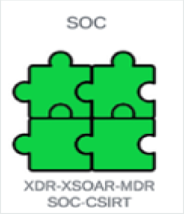
New members – Shield vzw

Service catalogue: Reference architecture

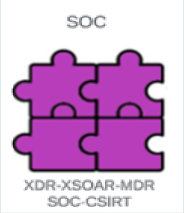
24-AWARENESS-SHIELD-01_pub01

24-FIREWALLS-SHIELD-01

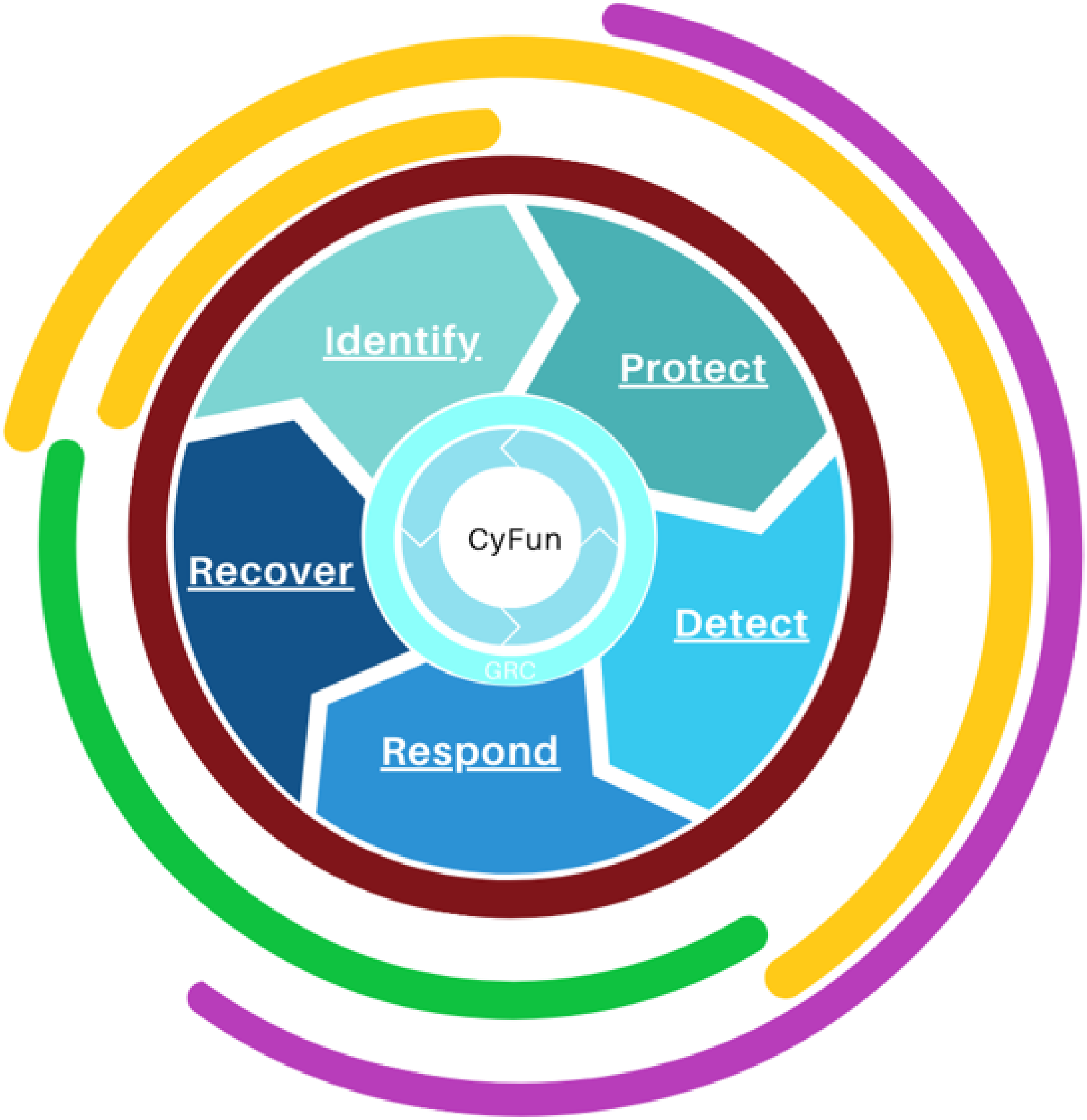
24-PENTEST-SHIELD-01_pub01



24-CSIRT-SHIELD-01_pub01



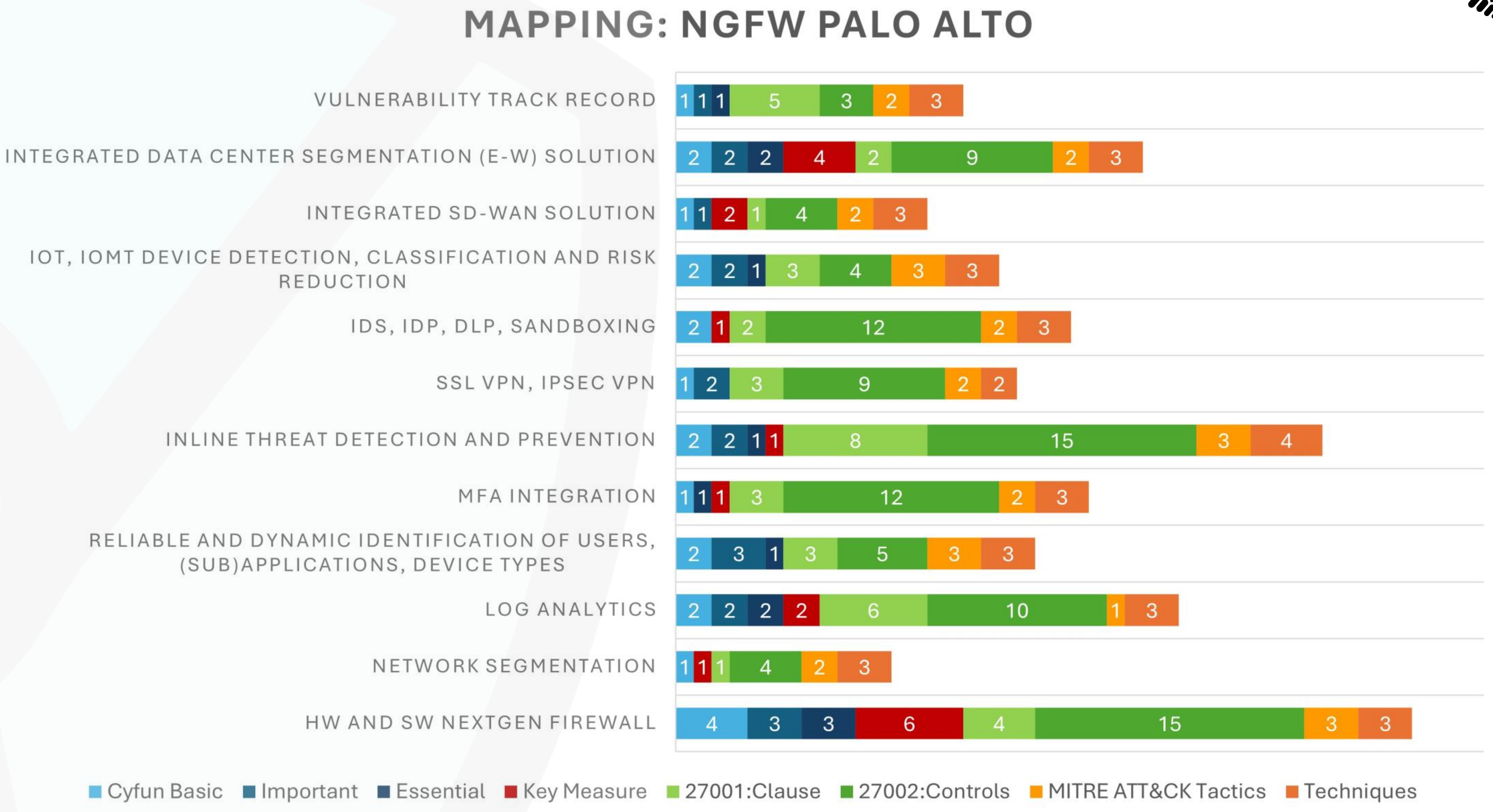
24-XDR-SHIELD-01



New members – Shield vzw

Service catalogue – Reference Architecture

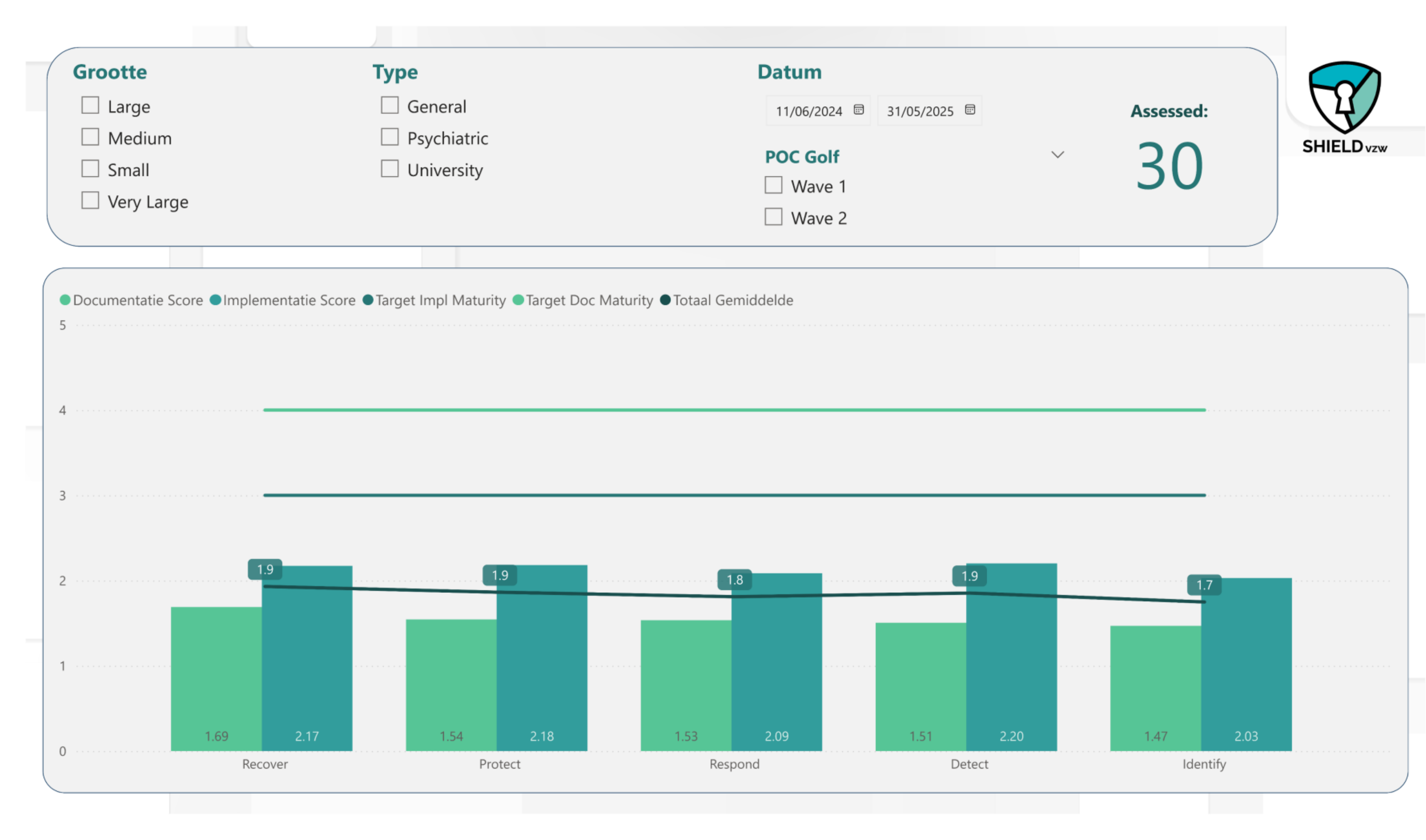
Firewall NGWF Palo Alto



New members – Shield vzw

Security Assessments

- Number of assessments performed: 30



Grootte

- □ Large
- □ Medium
- □ Small
- □ Very Large

Type

- □ General
- □ Psychiatric
- □ University

Datum

11/06/2024 31/05/2025

POC Golf

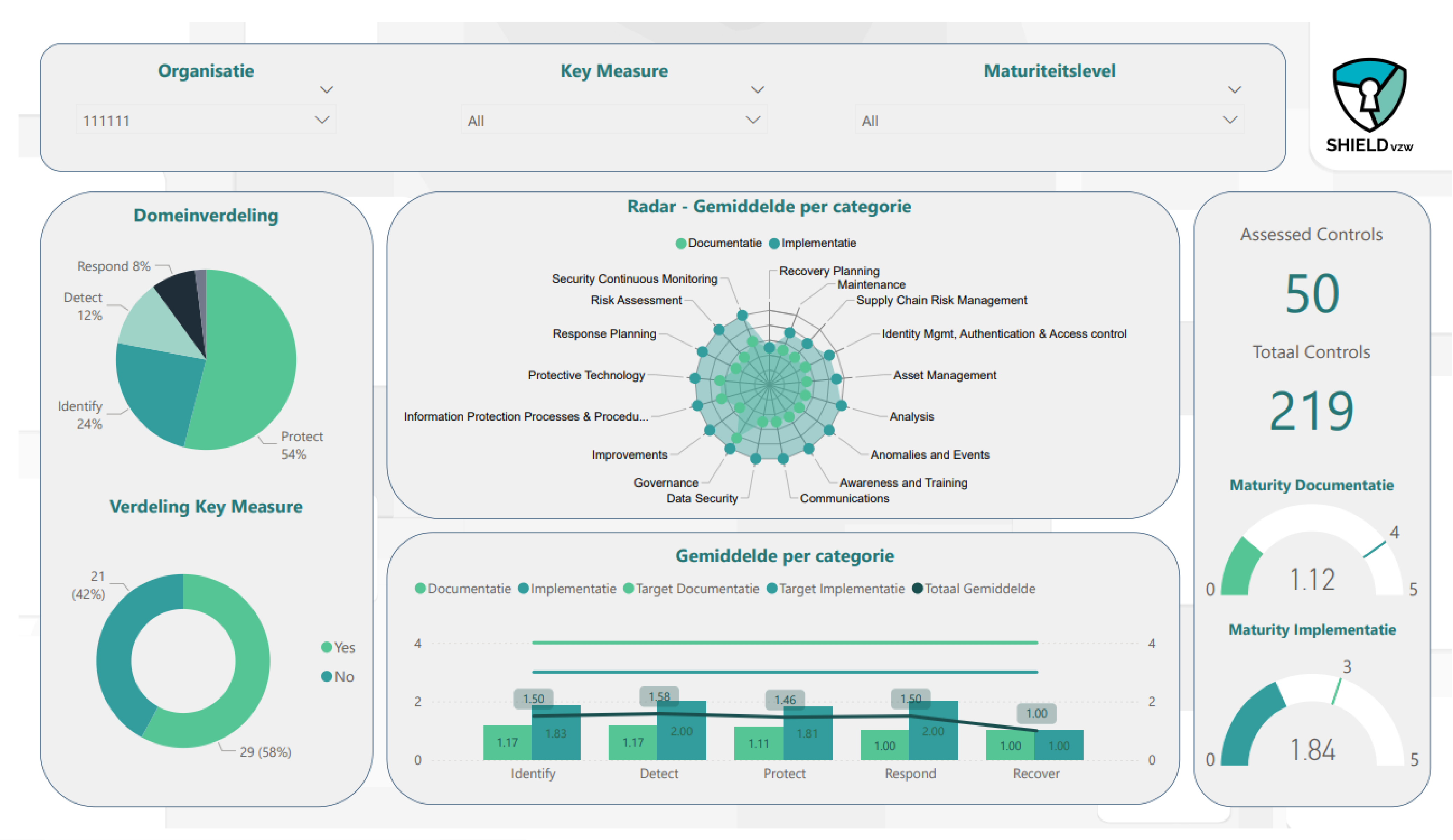
- □ Wave 1
- □ Wave 2

Assessed: 30

SHIELD vzw
● Documentatie Score ● Implementatie Score ● Target Impl Maturity ● Target Doc Maturity ● Totaal Gemiddelde
5
4
3
2
1
0
1.9
1.9
1.8
1.9
1.7
1.69
2.17
1.54
2.18
1.53
2.09
1.51
2.20
1.47
2.03
Recover
Protect
Respond
Detect
Identify

New members – Shield vzw

Dashboard



Organisatie: 111111

Key Measure: All

Maturiteitslevel: All

Assessed Controls: 50

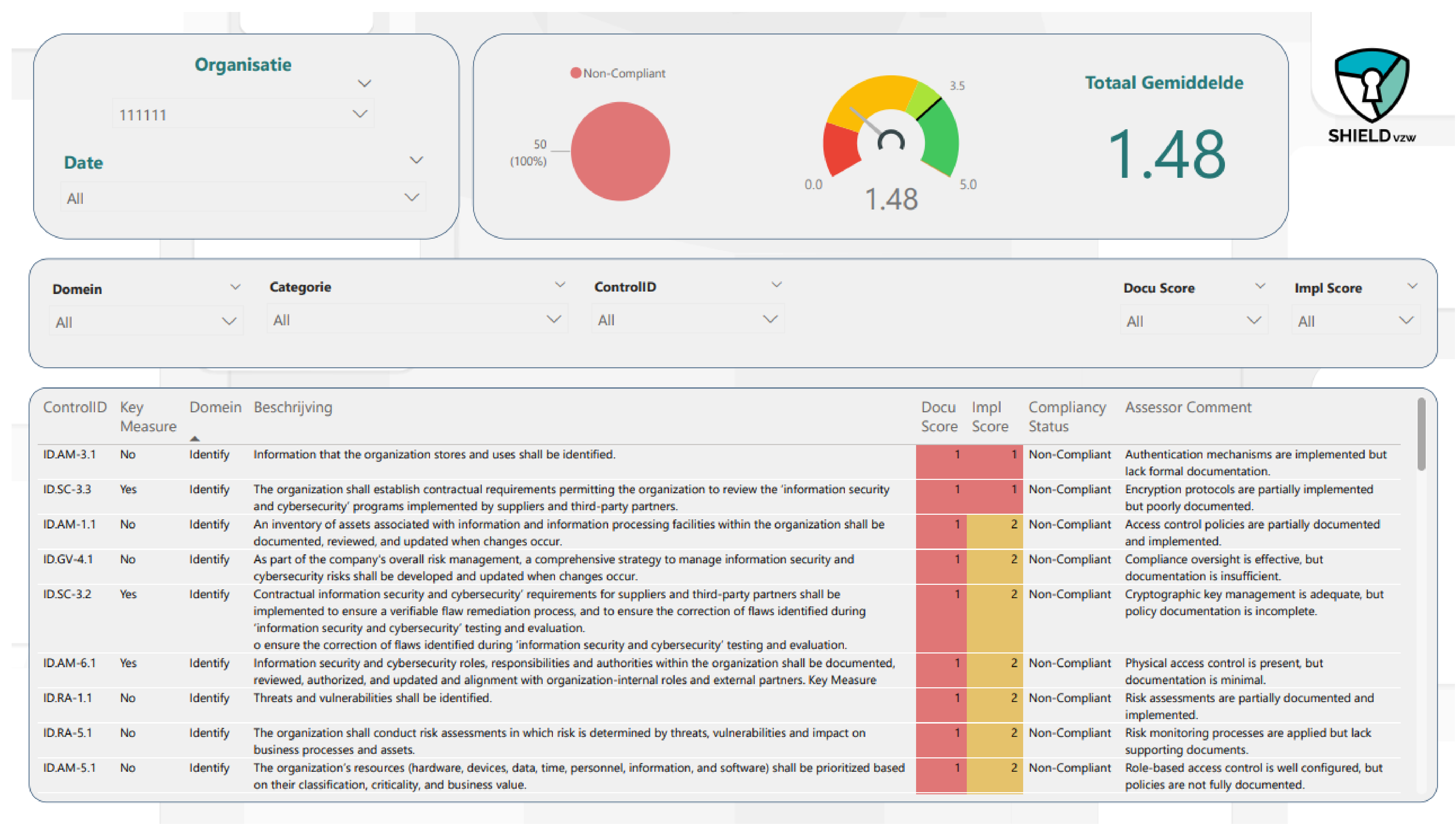
Totaal Controls: 219

Maturity Documentatie: 1.12

Maturity Implementatie: 1.84

New members – Shield vzw

Dashboard



Organisatie: 111111

Date: All

Totaal Gemiddelde

1.48

Domein: All

Categorie: All

ControlID: All

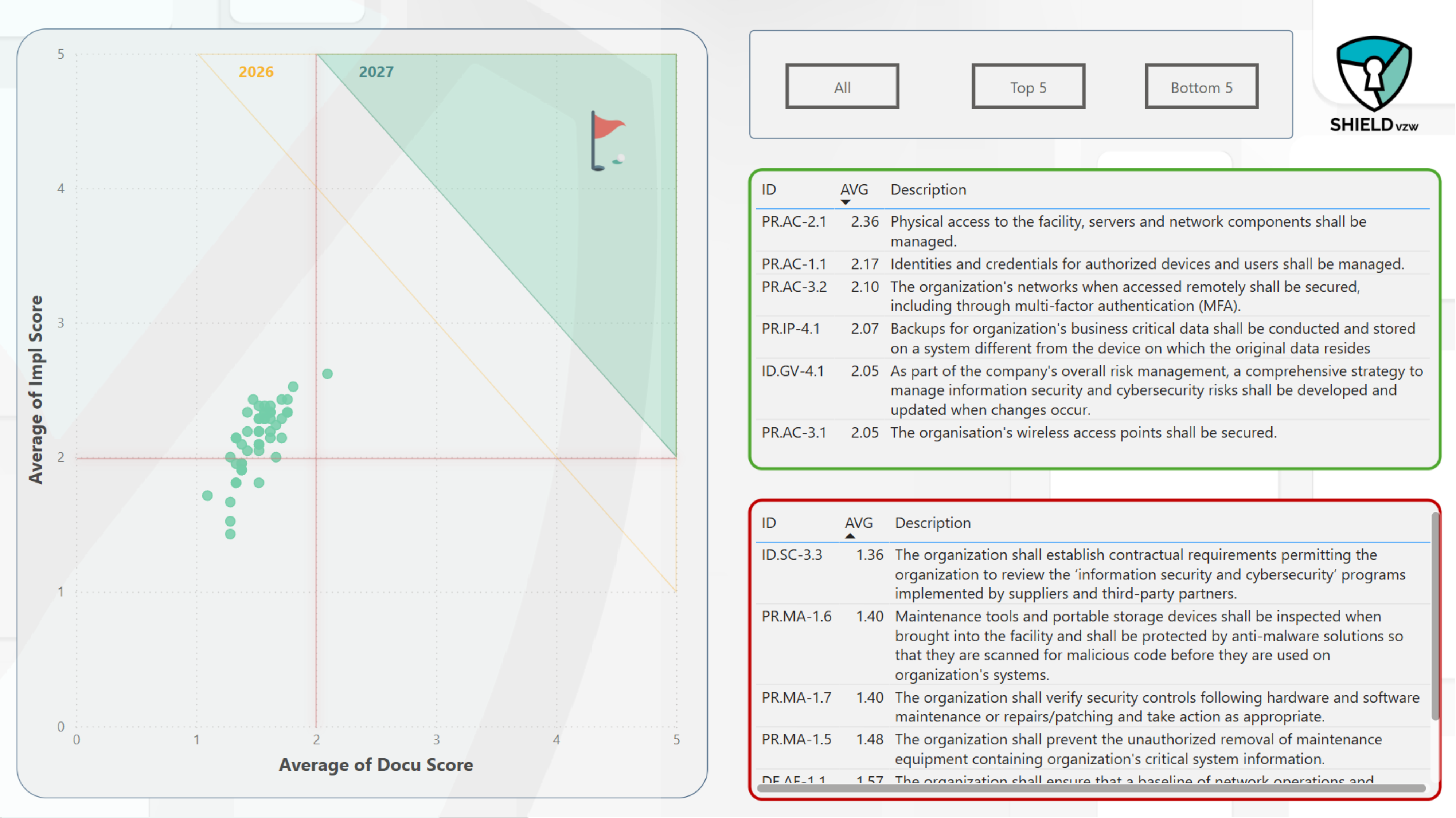
Docu Score: All

Impl Score: All

ControlID	Key Measure	Domein	Beschrijving	Docu Score	Impl Score	Compliancy Status	Assessor Comment
ID.AM-3.1	No	Identify	Information that the organization stores and uses shall be identified.	1	1	Non-Compliant	Authentication mechanisms are implemented but lack formal documentation.
ID.SC-3.3	Yes	Identify	The organization shall establish contractual requirements permitting the organization to review the 'information security and cybersecurity' programs implemented by suppliers and third-party partners.	1	1	Non-Compliant	Encryption protocols are partially implemented but poorly documented.
ID.AM-1.1	No	Identify	An inventory of assets associated with information and information processing facilities within the organization shall be documented, reviewed, and updated when changes occur.	1	2	Non-Compliant	Access control policies are partially documented and implemented.
ID.GV-4.1	No	Identify	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.	1	2	Non-Compliant	Compliance oversight is effective, but documentation is insufficient.
ID.SC-3.2	Yes	Identify	Contractual information security and cybersecurity' requirements for suppliers and third-party partners shall be implemented to ensure a verifiable flaw remediation process, and to ensure the correction of flaws identified during 'information security and cybersecurity' testing and evaluation. o ensure the correction of flaws identified during 'information security and cybersecurity' testing and evaluation.	1	2	Non-Compliant	Cryptographic key management is adequate, but policy documentation is incomplete.
ID.AM-6.1	Yes	Identify	Information security and cybersecurity roles, responsibilities and authorities within the organization shall be documented, reviewed, authorized, and updated and alignment with organization-internal roles and external partners. Key Measure	1	2	Non-Compliant	Physical access control is present, but documentation is minimal.
ID.RA-1.1	No	Identify	Threats and vulnerabilities shall be identified.	1	2	Non-Compliant	Risk assessments are partially documented and implemented.
ID.RA-5.1	No	Identify	The organization shall conduct risk assessments in which risk is determined by threats, vulnerabilities and impact on business processes and assets.	1	2	Non-Compliant	Risk monitoring processes are applied but lack supporting documents.
ID.AM-5.1	No	Identify	The organization's resources (hardware, devices, data, time, personnel, information, and software) shall be prioritized based on their classification, criticality, and business value.	1	2	Non-Compliant	Role-based access control is well configured, but policies are not fully documented.

Service catalogue – reference architecture

Assessments and GRC service

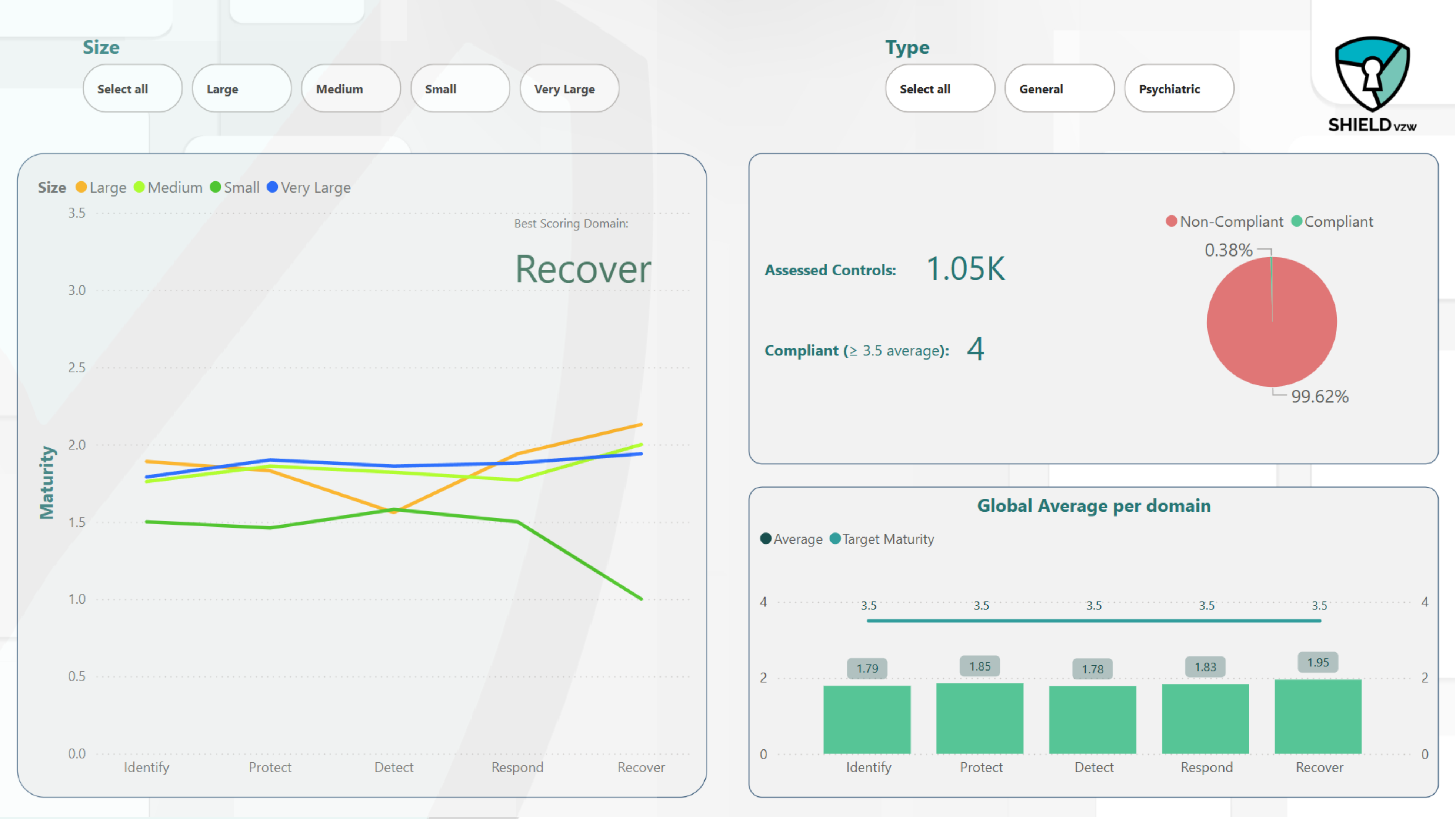


ID	AVG	Description
PR.AC-2.1	2.36	Physical access to the facility, servers and network components shall be managed.
PR.AC-1.1	2.17	Identities and credentials for authorized devices and users shall be managed.
PR.AC-3.2	2.10	The organization's networks when accessed remotely shall be secured, including 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

New members – Shield vzw

Service catalogue – reference architecture
Assessments and GRC service



Size

Select all | Large | Medium | Small | Very Large

Type

Select all | General | Psychiatric

SHIELD vzw

Best Scoring Domain: Recover

Assessed Controls: 1.05K

Compliant (≥ 3.5 average): 4

Global Average per domain

New members – Shield vzw

PoC FPS Public Health - Background

- In recent years, the FPS Public Health has launched a "Cybersecurity Programme" and made resources available to hospitals to increase their security level.
- In 2023, together with the FRZV, a partial joint approach was chosen in the pursuit of better price and quality for cybersecurity services.
- The goal is to help hospitals with (1) implementing security solutions, (2) sourcing cyber contracts, and (3) managing supplier quality.
- The POC consists of 4 phases, with specific objectives that must be achieved in order to proceed to the next phase.
- There are 28 places per phase, i.e. 1 hospital per hospital network and 3 psychiatric hospitals (3 waves in total up to 84 places).

PoC FPS Public Health - Projects

- ***Baseline measurements***: Maturity assessments

→ the start for all participating hospitals

- ***Project 1***: Common policy on medical devices

→ for the entire sector

- Implementation

→ based on individual priorities

- ***Project 2***: Platform for Pentests and Bug Bounty
- ***Project 3***: CSIRT subscription
- ***Project 4***: Cybersecurity Awareness Programs

New members – Shield vzw

Q
A

THANK YOU!

Kurt Gielen
kurt.gielen@shield-vzw.be

New members – Shield vzw