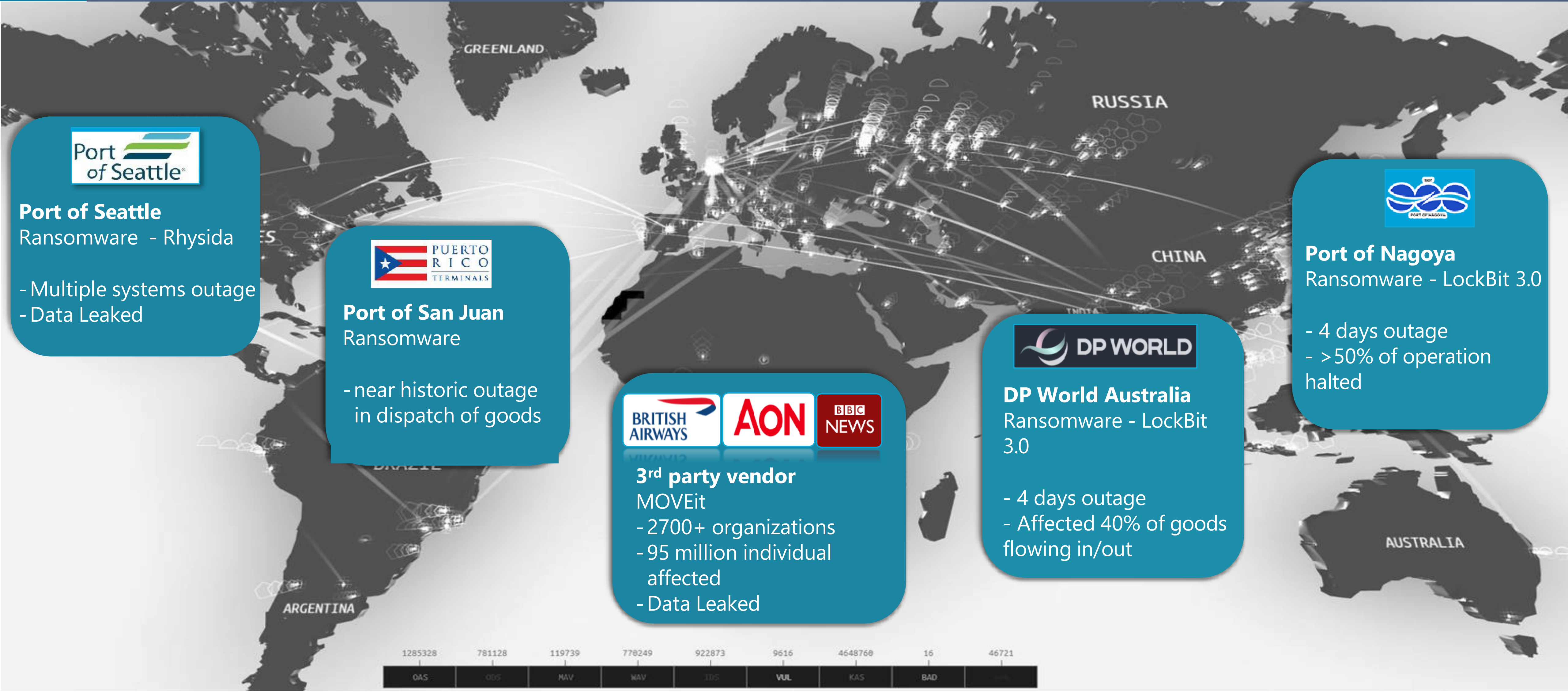
TRUST BUT VERIFY

Importance of Cybersecurity for Container Ports amid Technological Advancement

Annual Meeting
Davos 2025
WORLD ECONOMIC FORUM
Cyberattacks on shipping are on the rise

Global Cyber Attack Landscape



Port of Seattle
Ransomware - Rhysida

- Multiple systems outage
- Data Leaked

Port of San Juan
Ransomware

- near historic outage in dispatch of goods

3rd party vendor
MOVEit

- 2700+ organizations
- 95 million individual affected
- Data Leaked

DP World Australia
Ransomware - LockBit 3.0

- 4 days outage
- Affected 40% of goods flowing in/out

Port of Nagoya
Ransomware - LockBit 3.0

- 4 days outage
- >50% of operation halted

Global Cyber Attack Landscape

50%

Ransomware attack increase (>80% has data stolen)

X3

Exploitation of in-house and vendor software weaknesses

X7

OT Incidents on CI, 2022 to 2024

40%

AI-generated phishing email

60%

Recipients fall prey to AI-generated phishing email

46%

OT incidents attack path is from IT into OT environment

PSA Top Cyber Threats & Business Impact

Software Weakness Exploitation

Gain access to PSA network or system via loopholes

Third Party Vendor Compromise

Exploit PSA's trust on our vendor to attack PSA assets

Ransomware

Encrypt files, steal data. Demand for ransom Payment

Phishing Scam

Pretend to be someone trusted asking for personal info or money

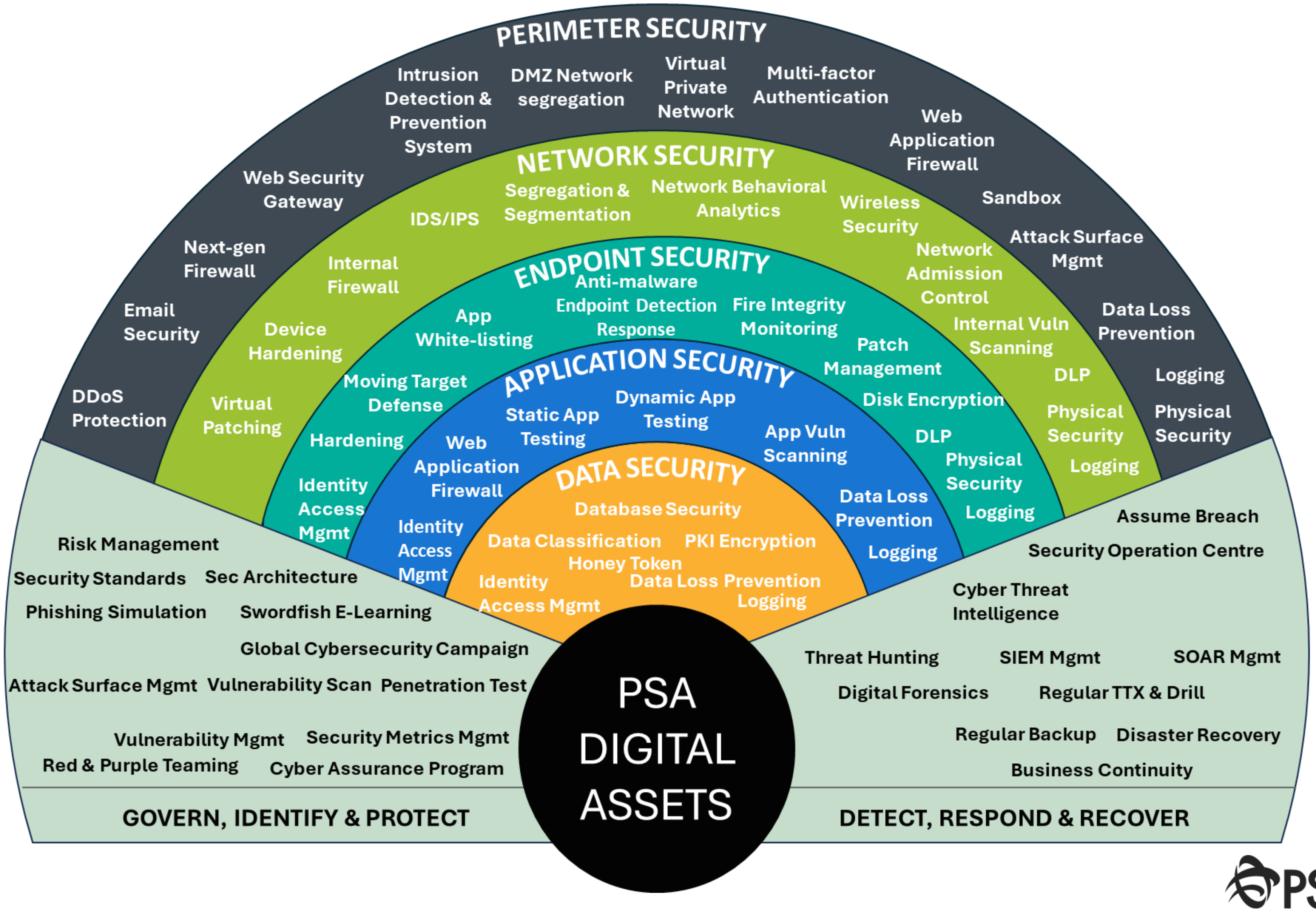
DDOS

Flood PSA Internet Service and prevent customers or users from accessing

Disrupt operations & service level to Customer | Steal PSA secrets and confidential data | Tarnish PSA reputation. Loss in stakeholders' confidence | Financial loss

PSA TRUST BUT VERIFY

PSA Multi-Layer Defences



PERIMETER SECURITY

Intrusion Detection & Prevention System

DMZ Network segregation

Virtual Private Network

Multi-factor Authentication

Web Application Firewall

Sandbox

Attack Surface Mgmt

Data Loss Prevention

Logging

Physical Security

Web Security Gateway

Next-gen Firewall

Email Security

DDoS Protection

NETWORK SECURITY

IDS/IPS

Segregation & Segmentation

Network Behavioral Analytics

Wireless Security

Network Admission Control

Internal Vuln Scanning

DLP

Physical Security

Logging

Internal Firewall

Device Hardening

Virtual Patching

ENDPOINT SECURITY

Anti-malware

Endpoint Detection Response

Fire Integrity Monitoring

Patch Management

Disk Encryption

DLP

Physical Security

Logging

App White-listing

Moving Target Defense

Hardening

Identity Access Mgmt

APPLICATION SECURITY

Static App Testing

Dynamic App Testing

App Vuln Scanning

Data Loss Prevention

Logging

Web Application Firewall

Identity Access Mgmt

DATA SECURITY

Database Security

Data Classification

PKI Encryption

Honey Token

Identity Access Mgmt

Data Loss Prevention

Logging

PSA DIGITAL ASSETS

Risk Management

Security Standards

Sec Architecture

Phishing Simulation

Swordfish E-Learning

Global Cybersecurity Campaign

Attack Surface Mgmt

Vulnerability Scan

Penetration Test

Vulnerability Mgmt

Security Metrics Mgmt

Red & Purple Teaming

Cyber Assurance Program

GOVERN, IDENTIFY & PROTECT

Assume Breach

Security Operation Centre

Cyber Threat Intelligence

Threat Hunting

SIEM Mgmt

SOAR Mgmt

Digital Forensics

Regular TTX & Drill

Regular Backup

Disaster Recovery

Business Continuity

DETECT, RESPOND & RECOVER

PSA TRUST BUT VERIFY

Uplifting BUs Cybersecurity Maturity

C2M2

Cybersecurity Capability Maturity Model (C2M2)

PSA Dashboard For IT

ASSET	🟩	🟩	🟩	🟩	🟨	🟩	🟨	🟩	🟩	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟩	🟩	🟩	🟨	🟩	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟨	🟩	🟨	🟩	🟩	🟨	🟨
THREAT	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟨	🟩	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟨	🟩
RISK	🟩	🟩	🟩	🟩	🟨	🟩	🟨	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩
ACCESS	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟩	🟨	🟩	🟩	🟩	🟩	🟩	🟨	🟩	🟨	🟩	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟨	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩
SITUATION	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟨	🟨	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩
RESPONSE	🟩	🟩	🟩	🟨	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟨	🟨	🟩	🟩	🟨	🟩
THIRD PARTY	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩
WORKFORCE	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟩	🟨	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟩	🟩	🟩
ARCHITECTURE	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟨	🟩	🟨	🟨	🟩	🟩	🟨	🟩	🟩	🟨	🟩	🟨	🟩	🟨	🟩	🟨	🟨	🟨	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟩	🟨	🟨	🟨	🟩	🟩	🟨	🟨
PROGRAM	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

🟩 Target Maturity 🟨 Areas to improve

To enhance Cybersecurity Posture, BU to achieve the target maturity. Prioritize actions and investments accordingly.

PSA

TRUST BUT VERIFY

Strengthening Group-wide Cybersecurity Resilience with 3Rs

Remediate Fast

Promptly apply software patch to address critical vulnerabilities, especially for **critical software**

[Time to Remediate]

Measure how promptly critical vulnerabilities are remediated

Target : Meet remediation timeline in Group Cybersecurity Standards

Respond Fast

Regularly update and test incident response plan with **scenario-specific playbooks**, integrated with crisis mgmt and communication plan

[Time to Respond]

Measure how quickly incident can be responded to

Target : Meet response time in service level agreement

Recover Fast

Regularly update and test recovery plan (DRP & BCP) with **table-top exercises** and **drills**

[Time to Recover]

Measure how quickly operations can resume from an incident

Target : Meet business maximum allowable outage timeline

PSA TRUST BUT VERIFY

PSA Global Cybersecurity 2025-2026 Focus Areas

OT Posture

- GOTSS
- SIEM OT Monitoring
- OT Posture Assessment

Resilience

- 3Rs Strategy
- CSMS
- Cyber Masterplan 2.0

Assurance

- Global CAP
- Red Team & TTX
- BAS - Cymulate
- C2M2 Cyber Maturity

Capability

- Global Cyber Workshop
- Employee Awareness
- Cyber Staff Development

Technology

- Cybersecurity Architecture Blueprint
- Securing Emerging Technology

PSA

TRUST BUT VERIFY

TRUST BUT VERIFY

Thank You

Building a Secure & Resilient Digital Ecosystem through Collective Defence