New Era...
New Cybersecurity Habits

paloalto®
NETWORKS

pylones*

New Era... New Cybersecurity Habits

George Fares

Sales Executive – Enterprise & Industry Business

Pylones Hellas

September 2021

Cyber OnBoarding

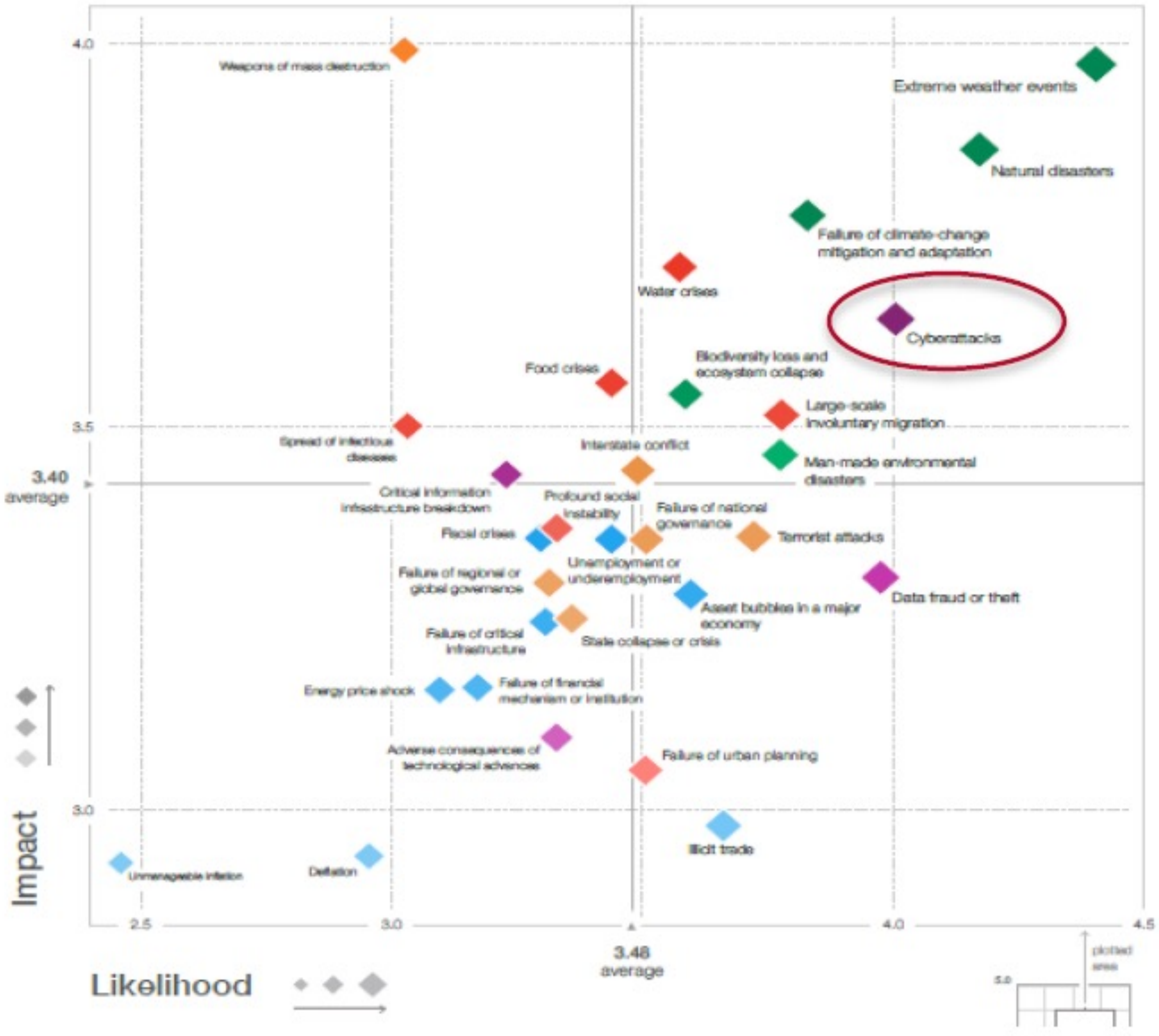
MARITIME CYBER SECURITY CHALLENGES

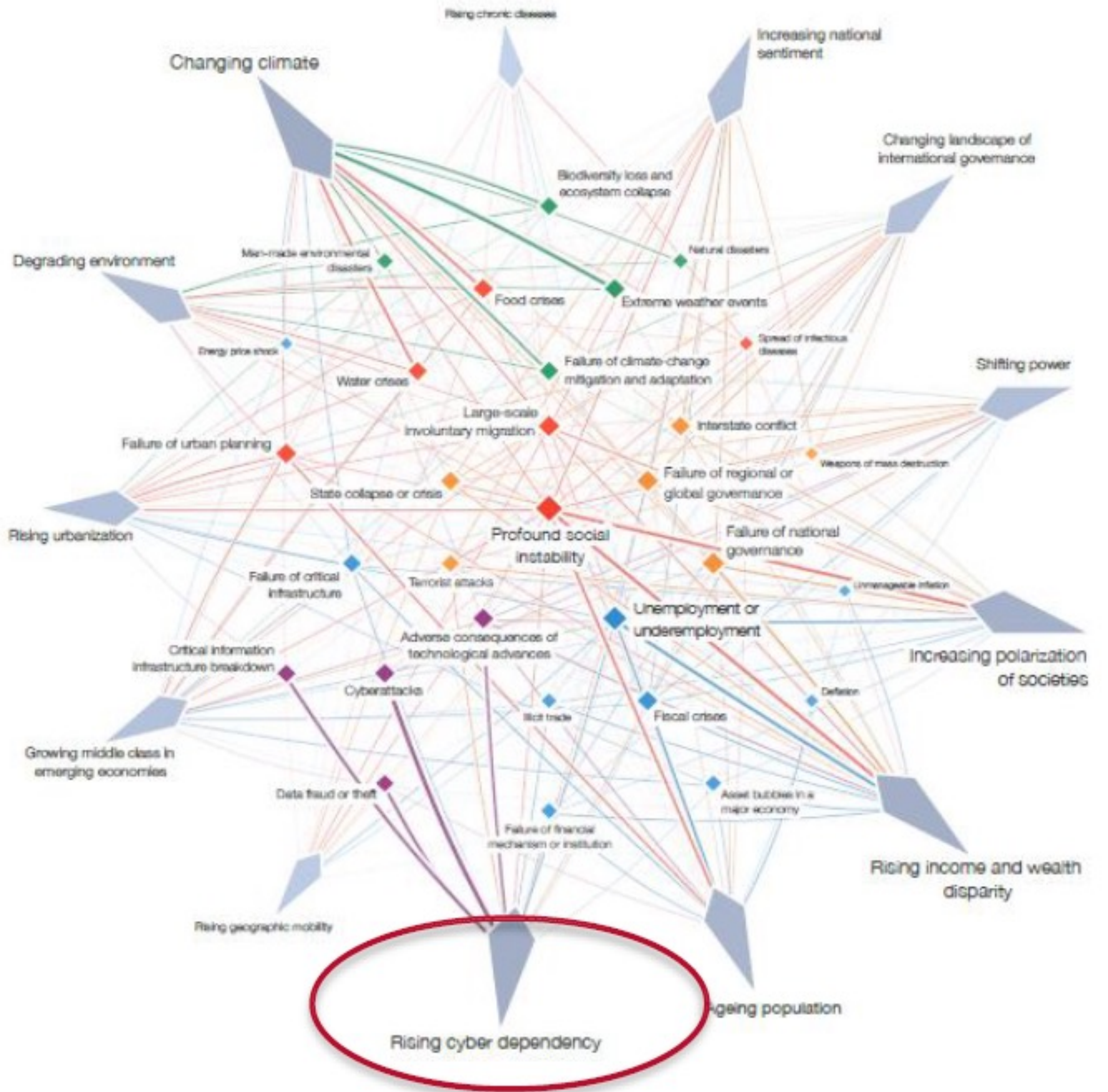
- Shore based attacks
- Vessel attacks
  - IT Systems
  - OT Systems

Maritime Cyber Attacks Increase by **900%** in Three Years

Cyber-Attacks: The new type of piracy in the Maritime World

World Economic Forum Report – last 3Y Top concern +COVIDx





Rising chronic diseases
Changing climate
Increasing national sentiment
Changing landscape of international governance
Biodiversity loss and ecosystem collapse
Degrading environment
Man-made environmental disasters
Natural disasters
Food crises
Extreme weather events
Energy price shock
Spread of infectious diseases
Water crises
Failure of climate-change mitigation and adaptation
Shifting power
Large-scale involuntary migration
Interstate conflict
Failure of urban planning
Weapons of mass destruction
State collapse or crisis
Failure of regional or global governance
Rising urbanization
Profound social instability
Failure of national governance
Failure of critical infrastructure
Terrorist attacks
Unmanageable inflation
Unemployment or underemployment
Adverse consequences of technological advances
Increasing polarization of societies
Critical information infrastructure breakdown
Cyberattacks
Deflation
Illicit trade
Fiscal crises
Growing middle class in emerging economies
Data fraud or theft
Asset bubbles in a major economy
Failure of financial mechanism or institution
Rising income and wealth disparity
Rising geographic mobility
Ageing population
Rising cyber dependency

DIGITAL ERA

Daily Workload

Limited Headcount & Budget

Digitalization & Compliance

Data analytics & Fleet Performance

Cybersecurity

Cyber OnBoarding

Crisis onboard

- Crew rotation affects operation
- Cyber awareness close to zero!
- Bandwidth (business critical)
- Inadequate measures and procedures

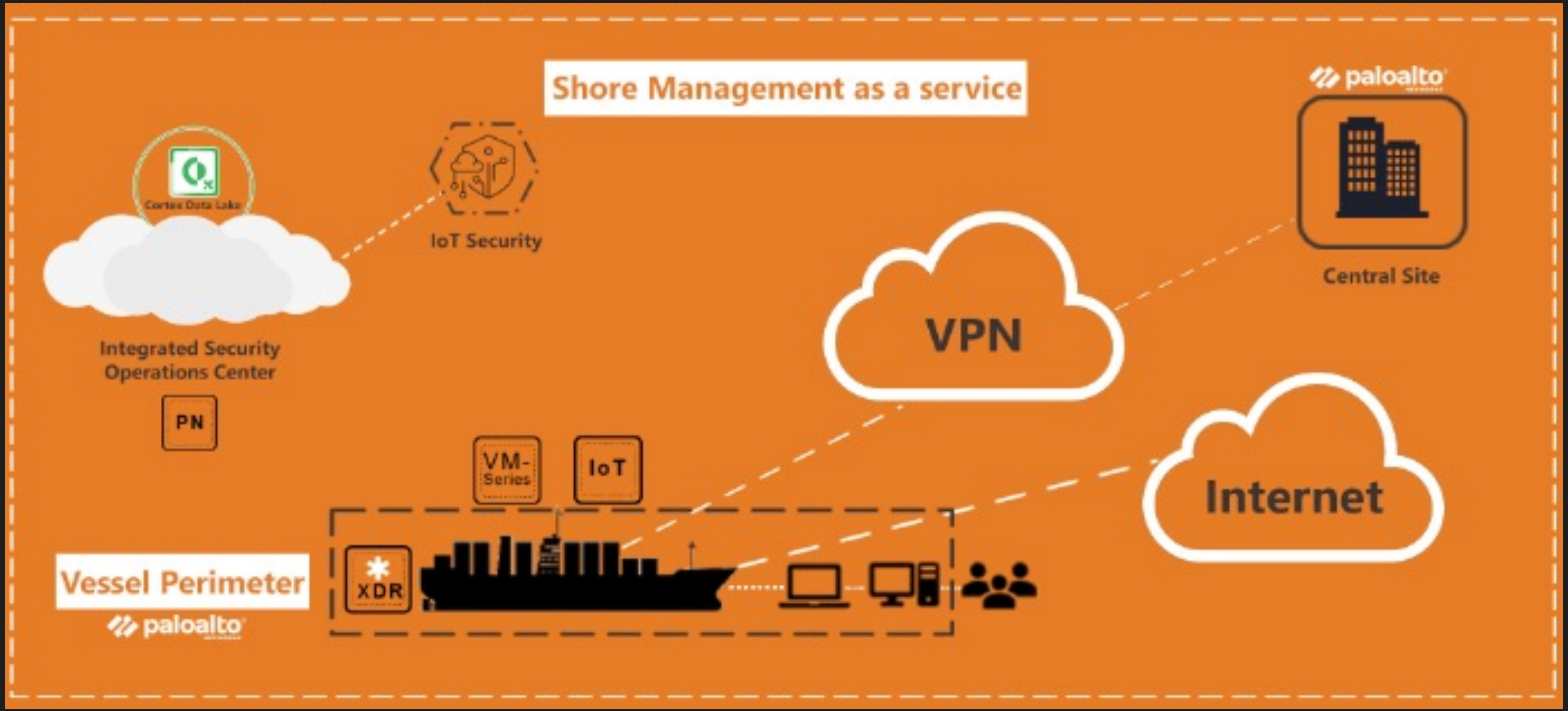
*Cyber OnBoarding

powered by Palo Alto

Cyber OnBoarding

SHORE to VESSEL

SAFEGUARD as a SERVICE | GLOBAL PROVISIONING



✱ MULTI-VECTOR PROTECTION [IT, TERMINAL, MOBILE, OT, IoT, ICS] ✱ COMPLETE RISK VISIBILITY

✱ NATIVE OPERATION ✱ OFFLINE OPERATION & BREAKPOINT ✱ NATIVE OPERATION

✱ CYBER FLEET TIMELINE ✱ AIR TIME AWARENESS ✱ COMPLIANCE VISIBILITY

Cyber OnBoarding

New Habits

Achieve efficiency with less workload

- Unified management console including 3rd party vendors
- Integration with SIEM

Daily Workload

Cyber OnBoarding

New Habits

Low TCO, no need for extra headcount

Limited Headcount & Budget

- Low TCO
- High ROI
- Enterprise solution & functionality
- Within budget limits

Cyber OnBoarding

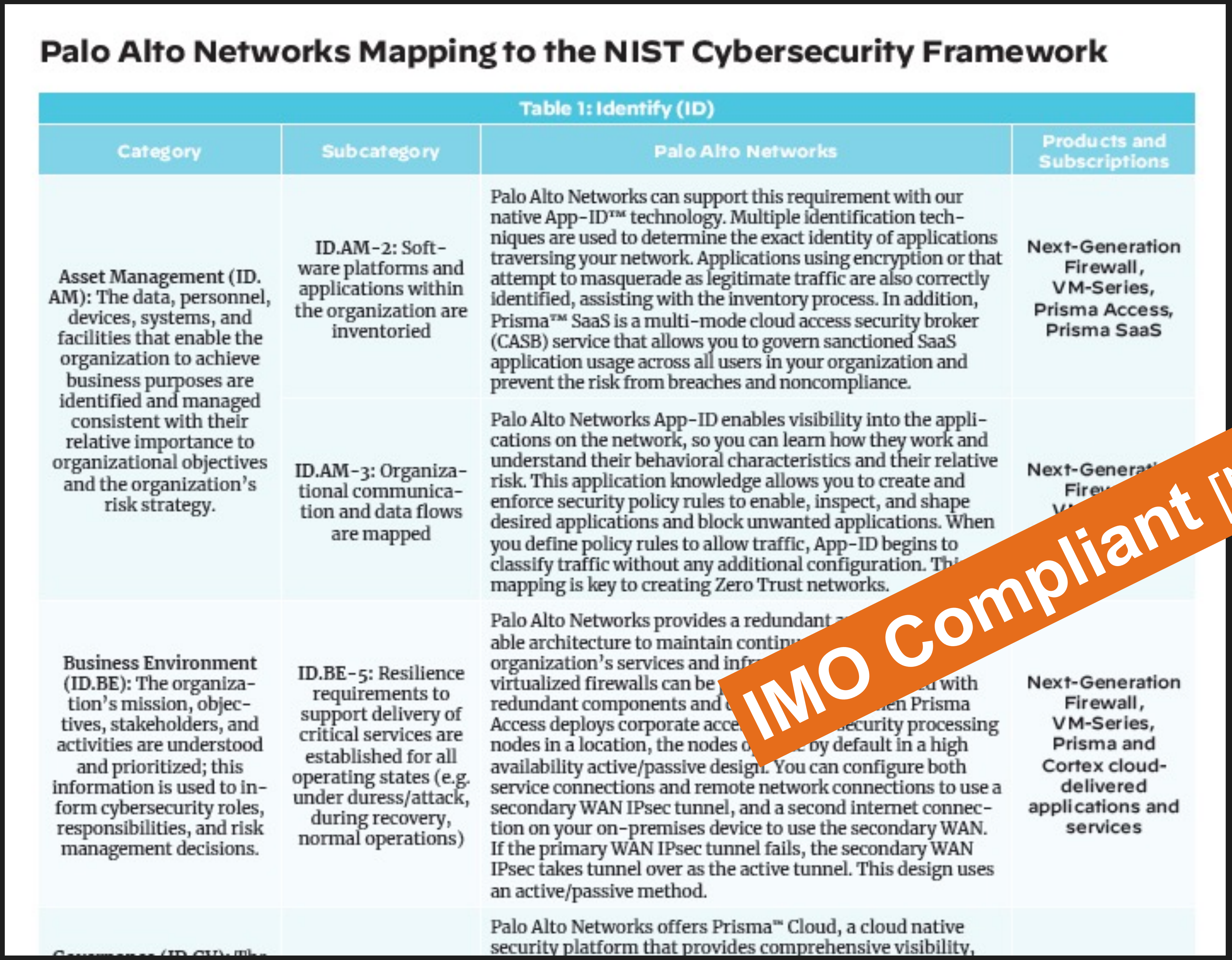
New Habits

pylones* we got IT | paloalto NETWORKS

Compliance has never been easier

✱ One click compliance report per fleet (or per vessel, you choose!)

Digitalization & Compliance

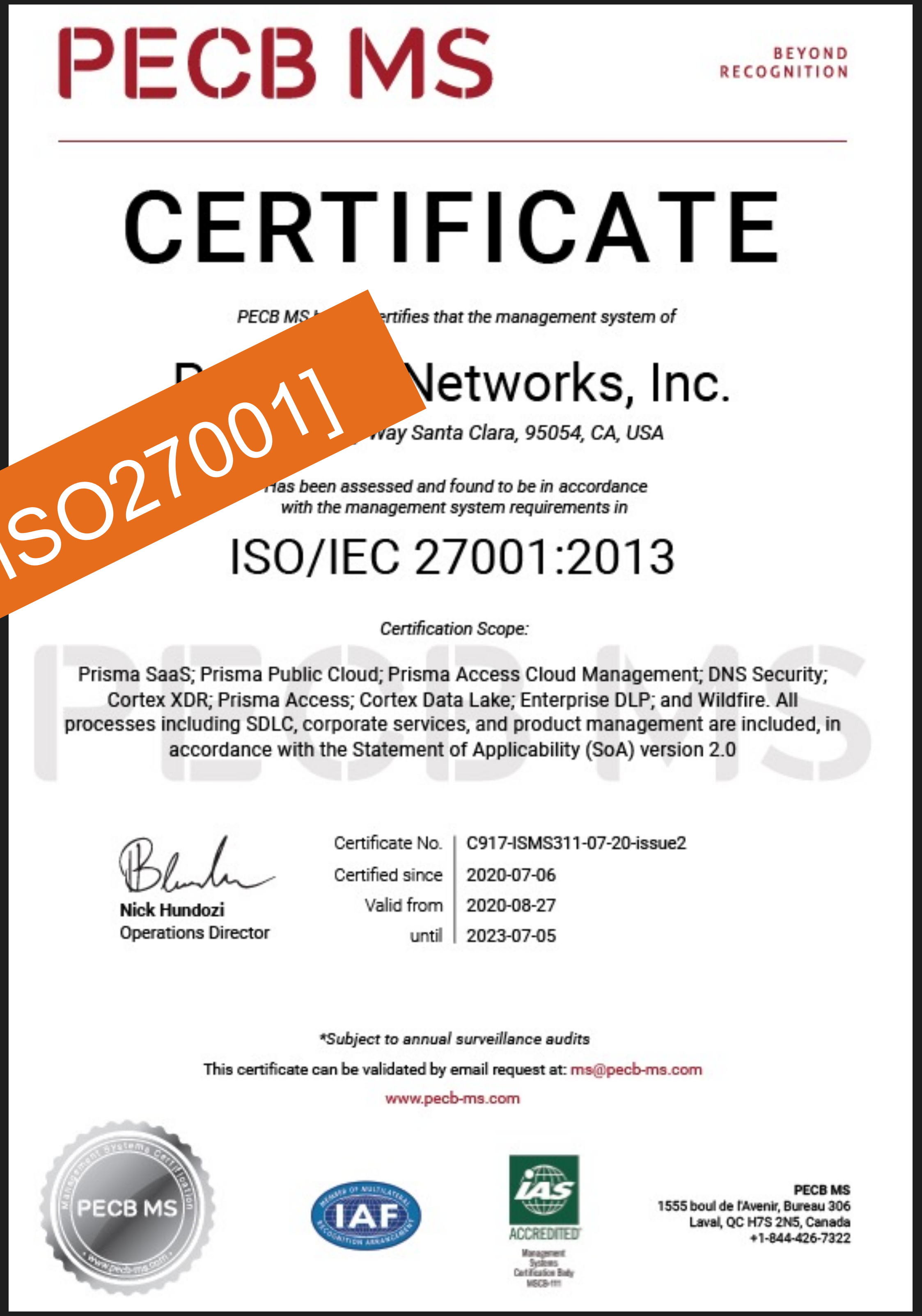


Palo Alto Networks Mapping to the NIST Cybersecurity Framework

Table 1: Identify (ID)			
Category	**Subcategory**	**Palo Alto Networks**	**Products and Subscriptions**
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-2: Software platforms and applications within the organization are inventoried	Palo Alto Networks can support this requirement with our native App-ID™ technology. Multiple identification techniques are used to determine the exact identity of applications traversing your network. Applications using encryption or that attempt to masquerade as legitimate traffic are also correctly identified, assisting with the inventory process. In addition, Prisma™ SaaS is a multi-mode cloud access security broker (CASB) service that allows you to govern sanctioned SaaS application usage across all users in your organization and prevent the risk from breaches and noncompliance.	Next-Generation Firewall, VM-Series, Prisma Access, Prisma SaaS
	ID.AM-3: Organizational communication and data flows are mapped	Palo Alto Networks App-ID enables visibility into the applications on the network, so you can learn how they work and understand their behavioral characteristics and their relative risk. This application knowledge allows you to create and enforce security policy rules to enable, inspect, and shape desired applications and block unwanted applications. When you define policy rules to allow traffic, App-ID begins to classify traffic without any additional configuration. Thi[illegible] mapping is key to creating Zero Trust networks.	Next-Generat[illegible] Fire[illegible] V[illegible]
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	Palo Alto Networks provides a redundant a[illegible] able architecture to maintain contin[illegible] organization's services and inf[illegible] virtualized firewalls can be [illegible] with redundant components and [illegible] en Prisma Access deploys corporate acce[illegible] security processing nodes in a location, the nodes [illegible] by default in a high availability active/passive design. You can configure both service connections and remote network connections to use a secondary WAN IPsec tunnel, and a second internet connection on your on-premises device to use the secondary WAN. If the primary WAN IPsec tunnel fails, the secondary WAN IPsec takes tunnel over as the active tunnel. This design uses an active/passive method.	Next-Generation Firewall, VM-Series, Prisma and Cortex cloud-delivered applications and services
Governance (ID.GV): The		Palo Alto Networks offers Prisma™ Cloud, a cloud native security platform that provides comprehensive visibility,	

IMO Compliant [NIST + ISO27001]

COMPLIANCY PER CATEGORY



PECB MS

BEYOND RECOGNITION

CERTIFICATE

PECB MS [illegible]ertifies that the management system of

P[illegible] Networks, Inc.

[illegible]way Santa Clara, 95054, CA, USA

Has been assessed and found to be in accordance with the management system requirements in

ISO/IEC 27001:2013

Certification Scope:

Prisma SaaS; Prisma Public Cloud; Prisma Access Cloud Management; DNS Security; Cortex XDR; Prisma Access; Cortex Data Lake; Enterprise DLP; and Wildfire. All processes including SDLC, corporate services, and product management are included, in accordance with the Statement of Applicability (SoA) version 2.0

Nick Hundozi
Operations Director

Certificate No.	C917-ISMS311-07-20-issue2
Certified since	2020-07-06
Valid from	2020-08-27
until	2023-07-05

**Subject to annual surveillance audits*

This certificate can be validated by email request at: ms@pecb-ms.com

www.pecb-ms.com

PECB MS · IAF · IAS ACCREDITED

PECB MS
1555 boul de l'Avenir, Bureau 306
Laval, QC H7S 2N5, Canada
+1-844-426-7322

REFERENCE STANDARDS

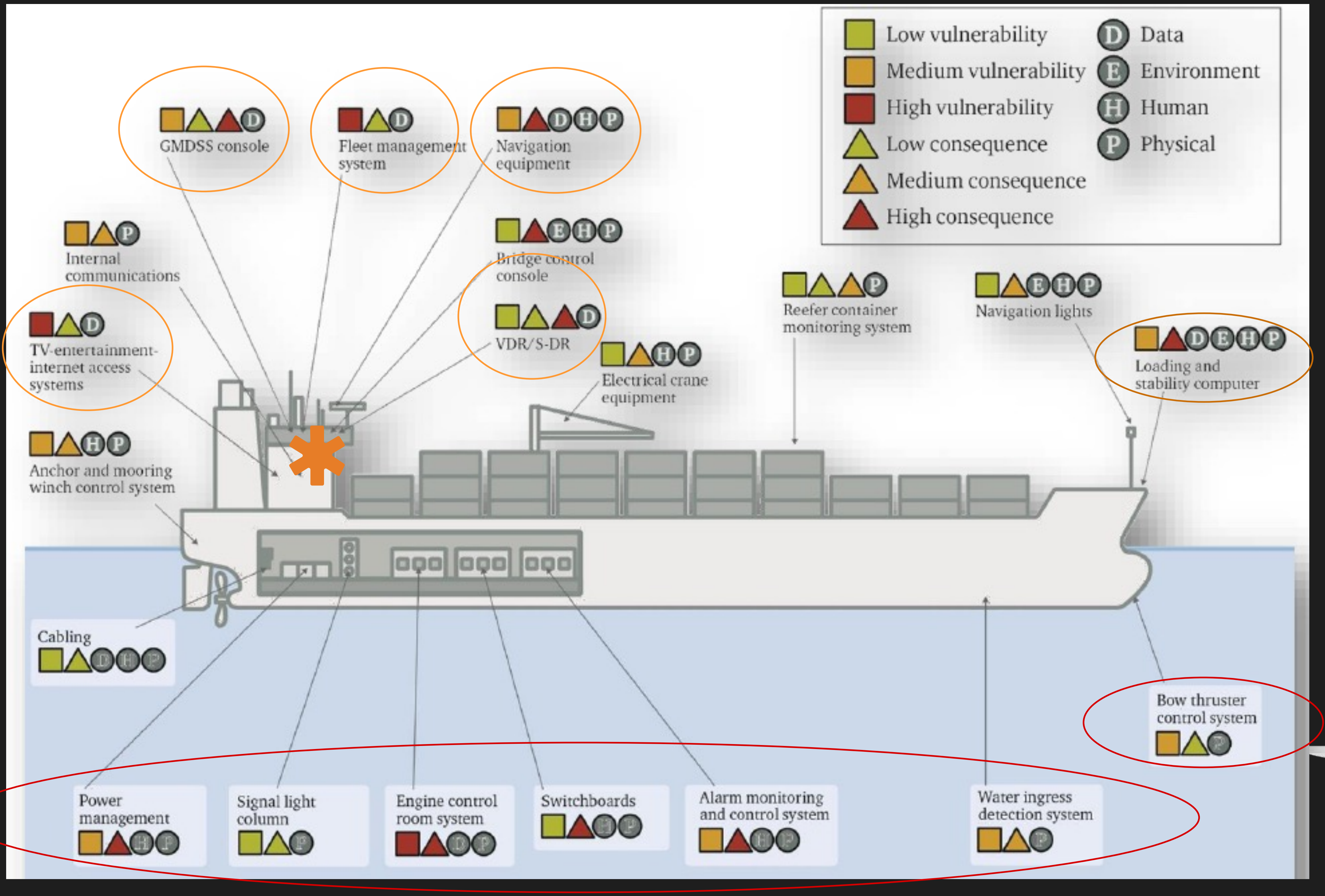
Cyber OnBoarding

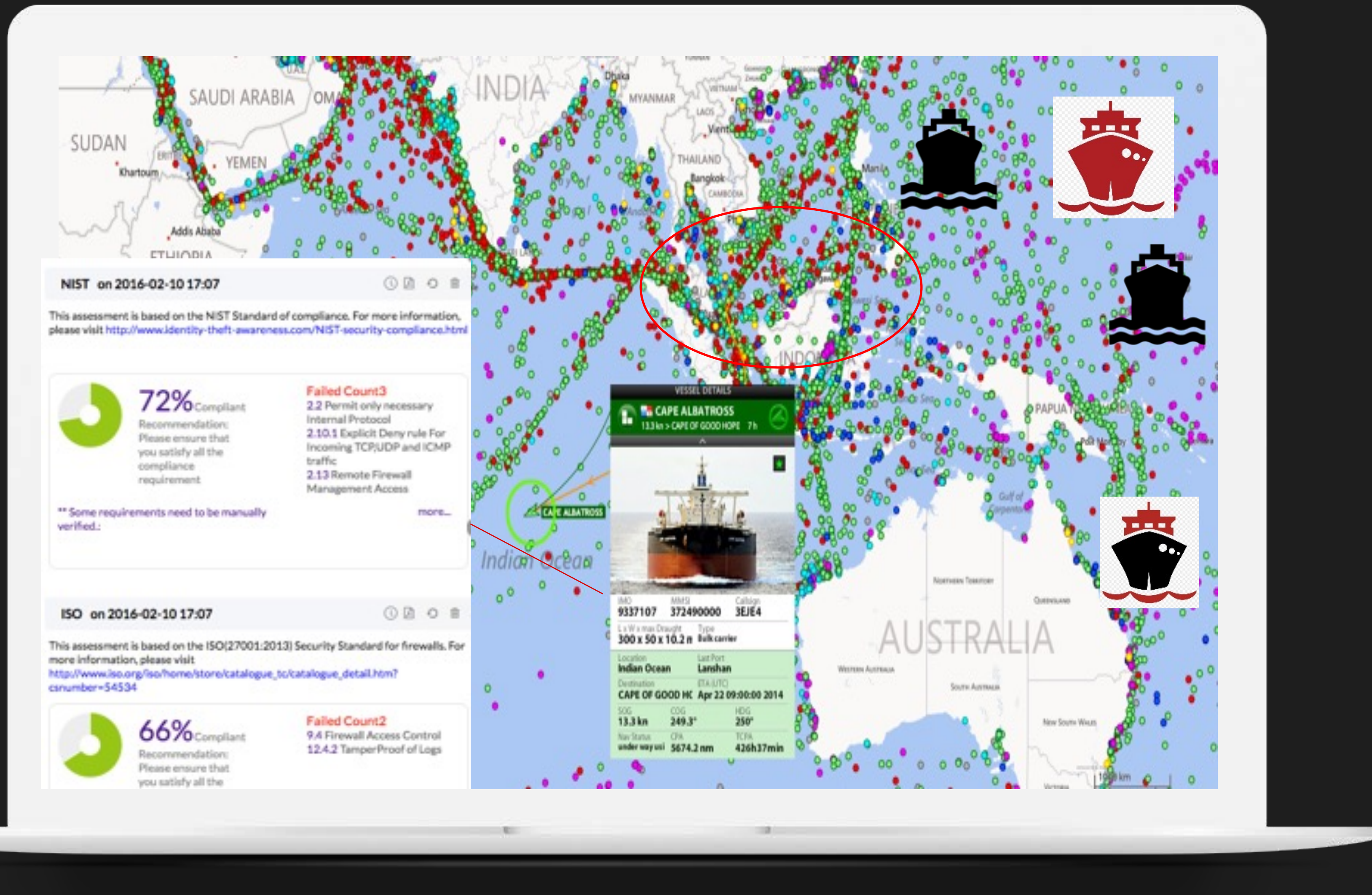
New Habits

Digestible Info

- Information regarding Cybersecurity heatmap across FLEET
- Full visibility on IT & OT systems onboard vessels

Data analytics & Fleet Performance


🟩 Low vulnerability
🟧 Medium vulnerability
🟥 High vulnerability
△ Low consequence
△ Medium consequence
△ High consequence
D Data
E Environment
H Human
P Physical
GMDSS console D
Fleet management system D
Navigation equipment D H P
Internal communications P
Bridge control console E H P
VDR/S-DR D
TV-entertainment-internet access systems D
Electrical crane equipment H P
Reefer container monitoring system P
Navigation lights E H P
Loading and stability computer D E H P
Anchor and mooring winch control system H P
Cabling
Bow thruster control system
Power management
Signal light column
Engine control room system
Switchboards
Alarm monitoring and control system
Water ingress detection system



NIST on 2016-02-10 17:07

This assessment is based on the NIST Standard of compliance. For more information, please visit http://www.identity-theft-awareness.com/NIST-security-compliance.html

72% Compliant

Recommendation: Please ensure that you satisfy all the compliance requirement

Failed Count3

2.2 Permit only necessary Internal Protocol

2.10.1 Explicit Deny rule For Incoming TCP,UDP and ICMP traffic

2.13 Remote Firewall Management Access

** Some requirements need to be manually verified.: more...

ISO on 2016-02-10 17:07

This assessment is based on the ISO(27001:2013) Security Standard for firewalls. For more information, please visit http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

66% Compliant

Recommendation: Please ensure that you satisfy all the

Failed Count2

9.4 Firewall Access Control

12.4.2 TamperProof of Logs

VESSEL DETAILS

CAPE ALBATROSS

13.3 kn > CAPE OF GOOD HOPE 7h

IMO	MMSI	Callsign
9337107	372490000	3EJE4
L x W x max Draught	Type	
300 x 50 x 10.2 m	Bulk carrier	
Location	Last Port	
Indian Ocean	Lanshan	
Destination	ETA (UTC)	
CAPE OF GOOD HC	Apr 22 09:00:00 2014	
SOG	COG	HDG
13.3 kn	249.3°	250°
Nav Status	CPA	TCPA
under way usi	5674.2 nm	426h37min

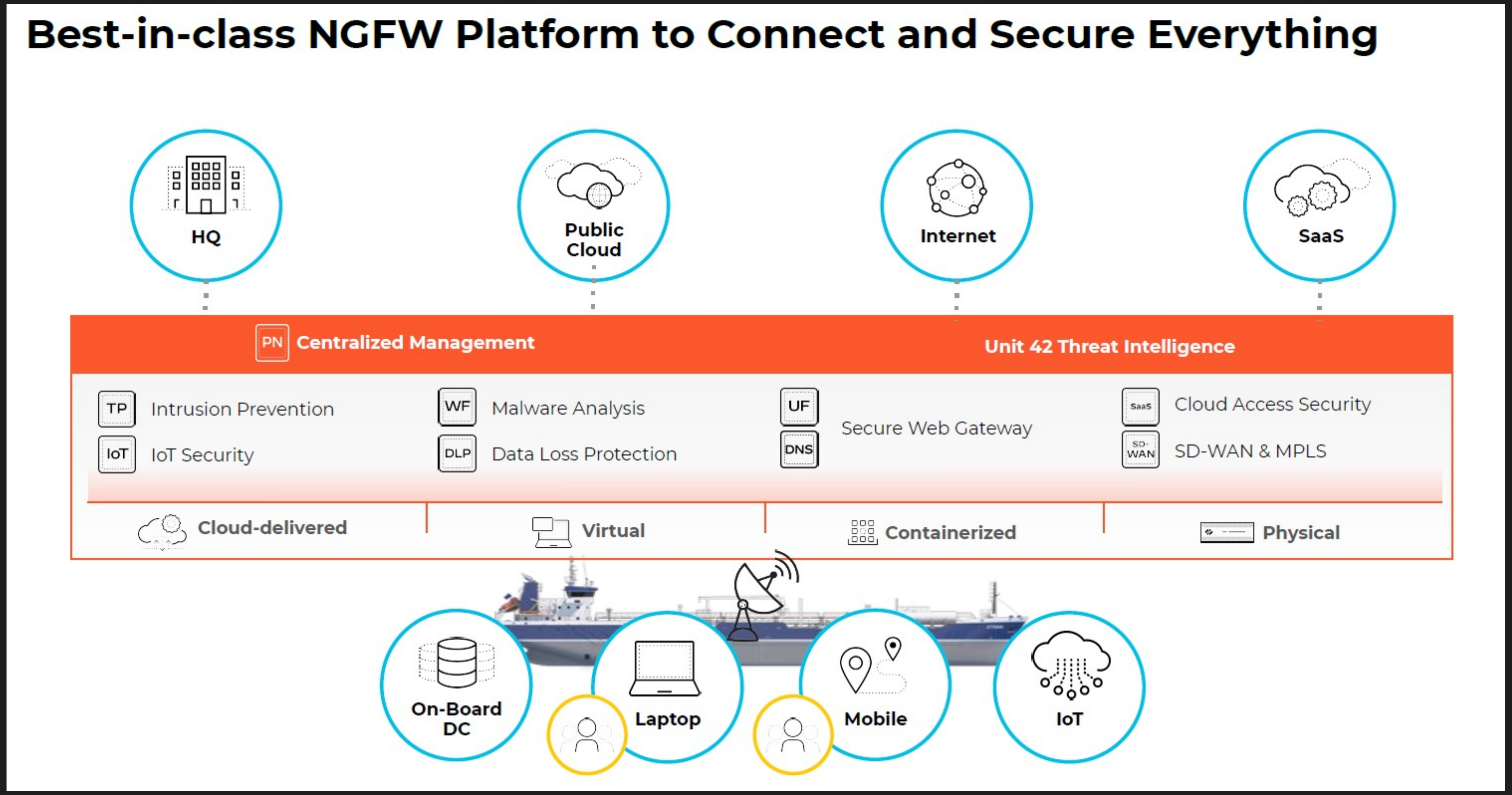
Cyber OnBoarding

New Habits

pylones* we got IT | paloalto NETWORKS

Cybersecure your fleet

- Safeguard your IT & OT infrastructure onboard
- Satcom bandwidth prioritization and utilization
- ₿ transactions – Ransomware prevention



Best-in-class NGFW Platform to Connect and Secure Everything

Cybersecurity

*Pylones at a glance

Turnover: >8.5m Euros (steadily increasing for the past 9 years)

Focuses 95% in Private Sector (Corporate & Enterprise ICT Market)

>45 Full Time Employees (25% more than 10 years with the company)

ISO 9001:2008
ISO 27001:2013

Great Place To Work.
Europe's Best Workplaces
2021

>12 International Projects

40+ vendor certifications (F5 Networks, Palo Alto, HPE, IBM, AWS, Microsoft etc.)

Long term partnership with leading companies in the private sector

13 International Vendor partnerships

Founded in 1997

Owned by Cyprus based P.M. Tseriotis Group

Activities in Greece, Cyprus, Central & Southern Europe with numerous projects internationally

*International activity

Trusted clients around Europe - Middle East - Australia

Greece | Cyprus | Australia | UAE | Spain | Germany | France | Estonia | Malta | Poland | Romania| Bulgaria | Albania | Serbia | Croatia)

pylones*
we got IT

*Reference clients

Telco
Banking
Insurance

WIND

COSMOTE

vodafone

forthnet

cyta

ALPHA BANK

Eurobank

BANK OF CHANIA

PIRAEUS BANK

Bank of Cyprus

Groupama

Eurolife ERB
Ασφαλιστική

ΕΥΡΩΠΑΪΚΗ ΠΙΣΤΗ

sia

HELLAS DIRECT
RETHINK INSURANCE

ATHENS
INTERNATIONAL AIRPORT
ELEFTHERIOS VENIZELOS

HELLENIC
PETROLEUM

AVAX

οπαπ

attica

SUPERFAST
FERRIES

Blue Star
Ferries

TERNA
GEK TERNA GROUP

ΤΡΑΙΝΟΣΕ

FLEXOPACK

PeopleCert

nova

intralot

NATIONAL BANK
OF GREECE

ΙΑΤΡΟΠΟΛΙΣ
ΟΜΙΛΟΣ ΙΑΤΡΙΚΩΝ ΕΤΑΙΡΙΩΝ

INFORM

NISSAN
ΝΙΚ. Ι. ΘΕΟΧΑΡΑΚΗΣ Α.Ε.

UNICARS

KOSMOCAR

DIVANI COLLECTION
ATHENS CORFU METEORA LARISSA

bluelagoon
RESORT

YES
HOTELS
&RESTAURANTS

Alcatel·Lucent

ERICSSON

NN

ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΑΜΕΣΗΣ ΒΟΗΘΕΙΑΣ
Ε.Σ.Υ.

ICAP
GROUP

L'ORÉAL
PARiS

danaos

A
ALPHA BULKERS
SHIPMANAGEMENT INC.

CARDIFF
MARINE GROUP

HLS
HABTOOR
LEIGHTON
SPECON

“We make IT simple”

pylones*