WEBINAR

THE JOURNEY TO BETTER CYBERSECURITY IN 2022 AND BEYOND

18TH AUGUST 2022 | 11.00 AM - 12.30 PM

ORGANISED BY:

Varuna Marine Services

Smart Sustainable Shipping

MODERATORS

Ms.Yipaerguli.Waili(Ipar)

Sustainability and Business Development Manager - Varuna Marine Services B.V.

Ms. Richa Dutt Nandan

Marketing Manager - Varuna Marine Services B.V.

BEFORE WE START...

The webinar will run about 1 hour.
Last 15 mins for Q&A.

This webinar is recorded, and we will share the recording in a blog article after the webinar

Use the Q&A function to send you questions anytime during the Webinar.


MARITIME CYBER SECURITY

PANELISTS FOR TODAY

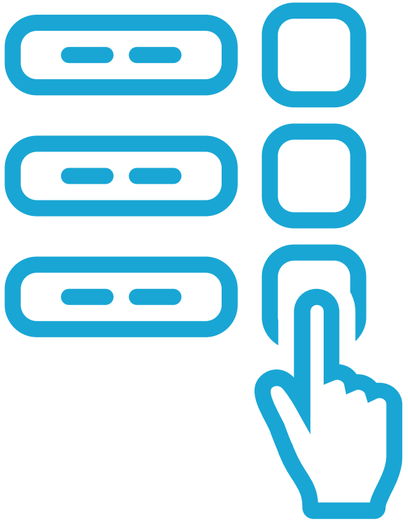
MR. PANAGIOTIS ANASTASIOU

CYBERSECURITY TECHNICAL LEADER - BUREAU VERITAS MARINE & OFFSHORE

MR. SANJEEV WEWERINKE-SINGH

DIRECTOR - VARUNA MARINE SERVICES B.V.

POLL QUESTIONS



The results of the polls will be published along with the in a blog article after the webinar

WHAT'S NEXT??

MR. PANAGIOTIS ANASTASIOU

CYBERSECURITY TECHNICAL LEADER -
BUREAU VERITAS MARINE & OFFSHORE

THE JOURNEY TO BETTER CYBERSECURITY IN 2020 & BEYOND

BUREAU VERITAS MARINE & OFFSHORE

2022

AGENDA

01

TRENDS AND LESSONS

02

KEY VULNERABILITIES

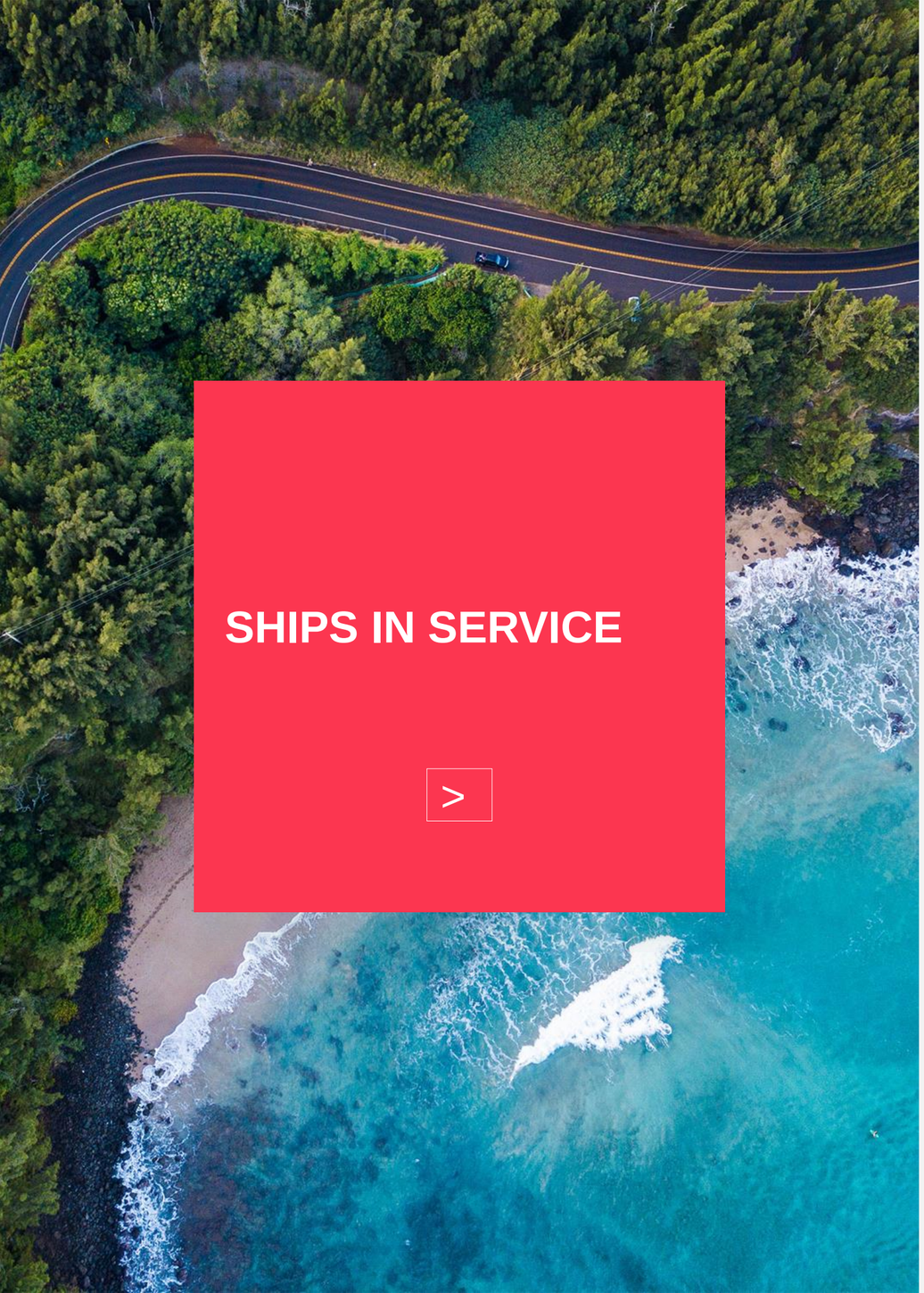
03

WAY FORWARD

01

TRENDS AND LESSONS

LEARNT FROM INSPECTIONS, CLASS NOTATION GRANTS AND AUDITS



SHIPS IN SERVICE

>

REGULATION

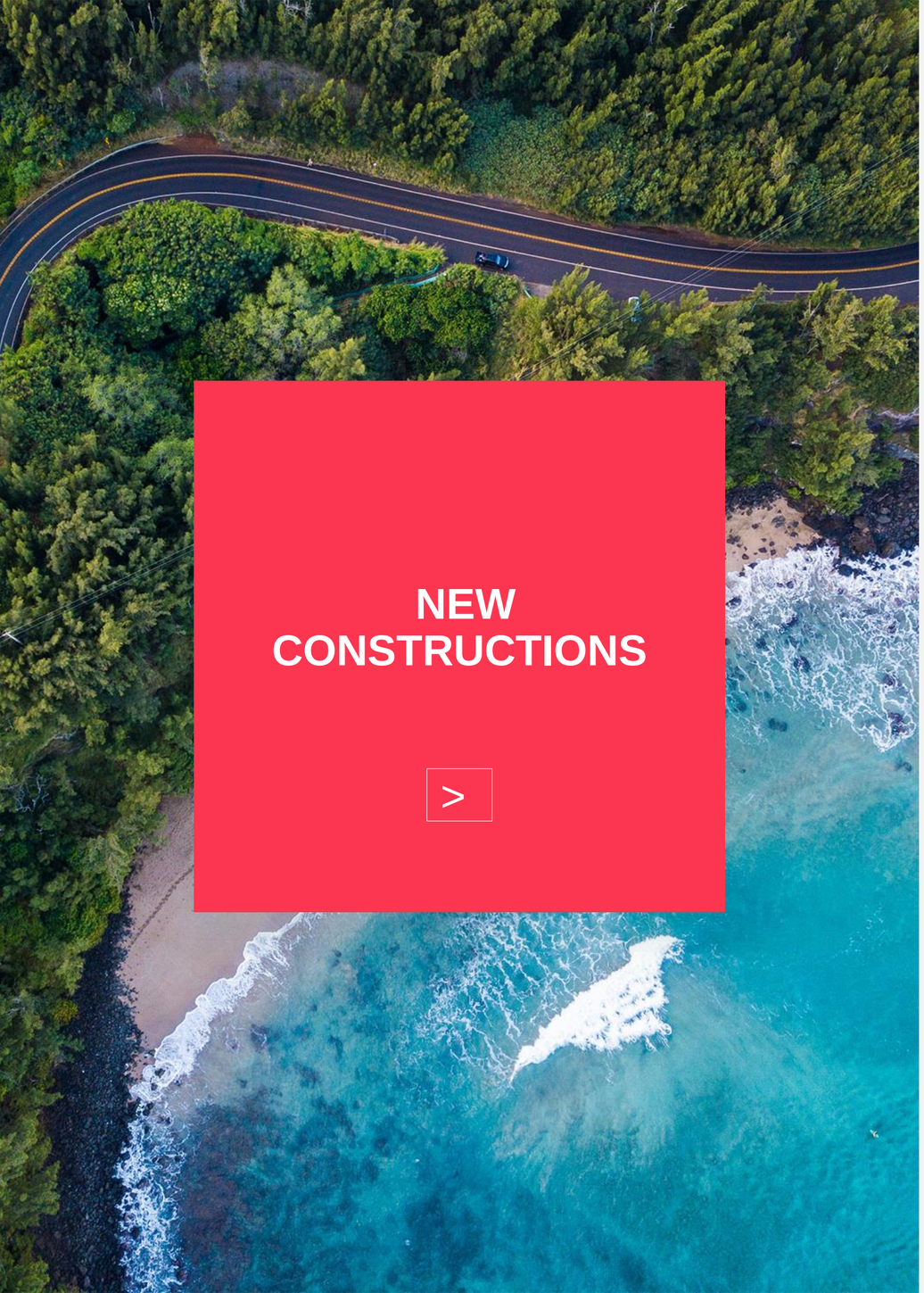
- IMO Resolution 428(98) enforced since Jan 1st 2021

MARKET

- Growing awareness around technical risks
- But still only targeting ISM compliance

MARITIME ATTACKS

- Maritime Cyber Attacks have increased by 900% in three years
- Leaked and disclosed ballast water management systems cyber attacks scenarios
- Infected VPNs



NEW CONSTRUCTIONS

>

SHIPYARDS

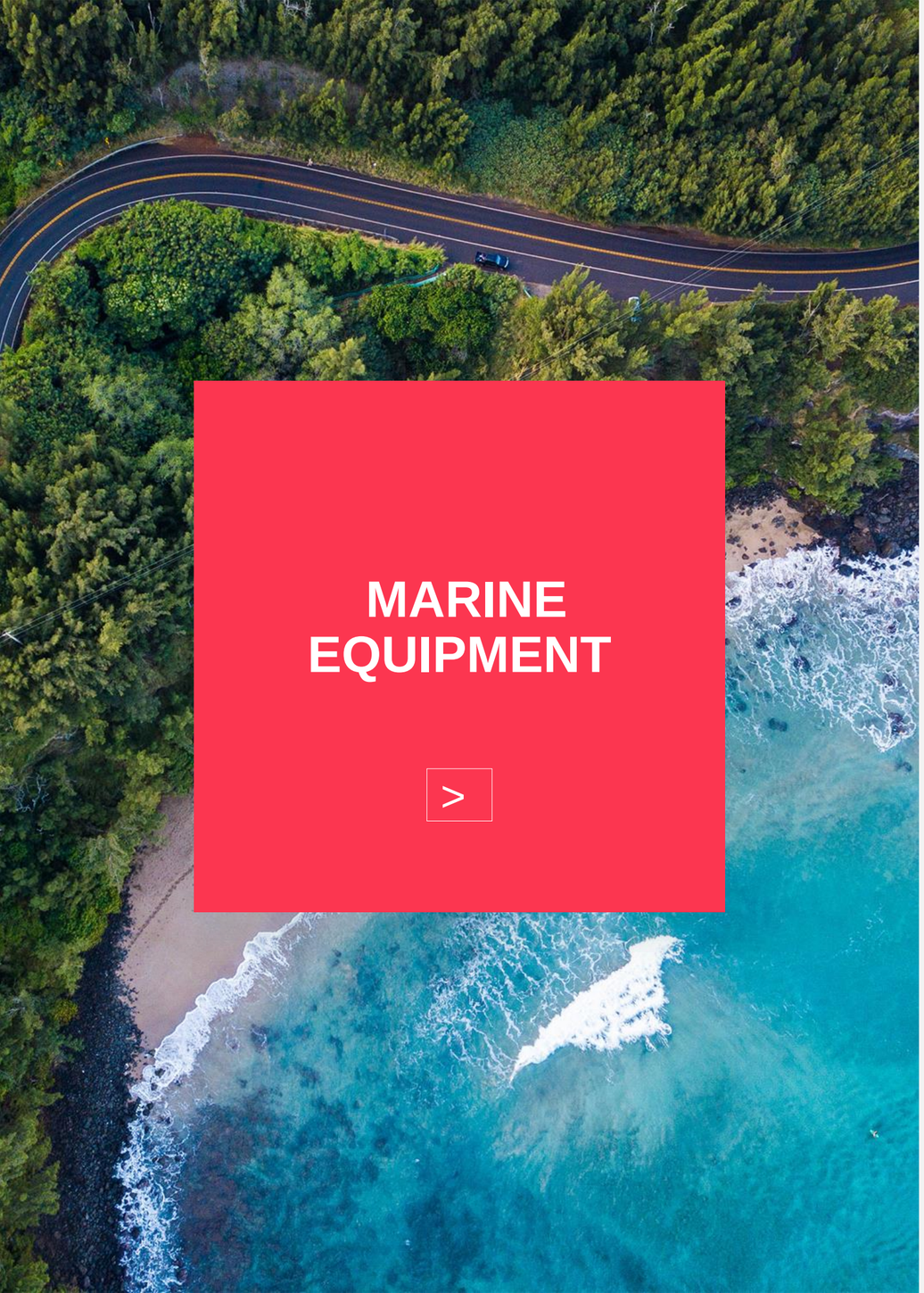
- Scarce investments to introduce cyber security by design

MARKET

- Pending entry into force of the IACS regulation
- Some welcome active initiatives from cutting-edge shipyard

REGULATION

- New UR E26 will enter into force 1st of January 2024
  - Cyber resilience of ships



MARINE EQUIPMENT

>

ISSUES

- Lack of standards
- False beliefs and underestimation about risk of attacks
- Nearly nonexistent support on vulnerabilities
- Growing interactions with cloud-based solutions

MARKET

- Demand is increasing
- With already some investments

REGULATION

- New UR E27 will enter into force 1st of January 2024
  - Cyber resilience of on-board systems and equipment

02

KEY VULNERABILITIES

AND RISKS THAT KEEP BEING UNCOVERED

NEW MARITIME THREATS

Larger attack surface

- Digitalization complexity + software obsolescence
- Connected propulsion or navigation systems

New threats

- 3000% surge in IoT malware activity between Q3 2019 and Q4 2020 (Source: IBM)
- Attack on manufacturers could impact simultaneously all vessels using the same equipment all over the world

Impacts

- Cargo loss
- Time of restoration

FUTURE MARITIME CHALLENGES

Piracy

- Hijacked vessel sea routes and ship manifests lead to a modern form of maritime piracy.
- Criminal organization could invest against shipping industry
- Growing usage of Zero-days (16 in 2018, 32 in 2020, 80 in 2021, Source: MANDIANT)
- Cyber kinetic attacks though OT malware development

Challenges

- Maintain the level of cybersecurity on in-service vessels.
- Prepare Cyber secure vessels by design
- Push the limits to enable autonomous systems

03

NEXT TWO YEARS

TOWARDS CYBERSECURITY COMPLIANCE

MARITIME DIGITAL EVOLUTION

FROM 2017 TO 2024

<2018

Globalised Shipping Management

Performance monitoring

- Vessels operations are digitalized and managed from the shore

2019

Growing connectivity

On-board networks interconnections

- Connected propulsion or navigation systems
- SatCom provide growing access to any part of the vessels

2020

Smart Shipping

Predictive Maintenance

- Sensors & IoT
- Efficiency
- Remote Maintenance
- Real-Time monitoring
- Data Science

2021

2022

Digital Twin

Accurate Prediction

- Correlation with external sources
- Machine Learning
- Minimized risk of human error
- Enhanced port & terminal operations
- End-to-end supply chain optimization

2023

Unmanned Vessels

Fully remotely controlled

- All systems remotely operated
- No more manual ship handing over

2024+

Autonomous Vessels

Artificial Intelligence

- Operations and safety rely at 100% on onboard systems

BUREAU VERITAS

REGULATION EVOLUTION
FROM 2017 TO 2024

BV NR 659
Additional class notations
for NS, NC, equipment

IACS Rec 166
Recommendations
for NC and equipment

IMO Res 428
Cyber Security
for NS

MANDATORY
+ PORT STATE CONTROLS

IACS UR E26
IACS UR E27
Requirements
for NC and equipment

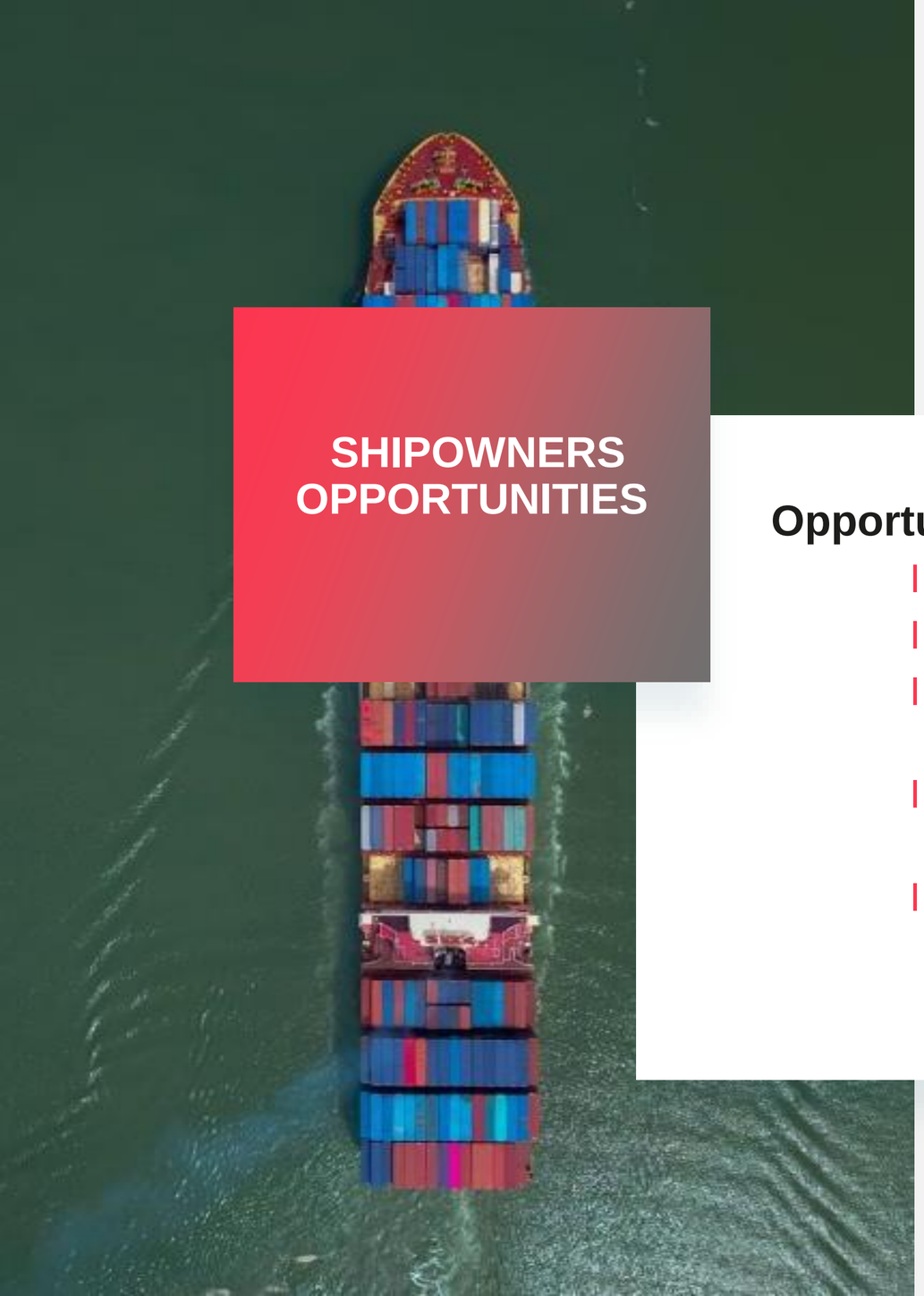
Rec. 171
Cybersecurity in SMS
(IMO Res 428 Mandatory)

Implementation phase

MANDATORY CYBER SECURITY REQUIREMENTS
All Class Societies
NC and Equipment

2018	2019	2020	2021	2022	2023	2024

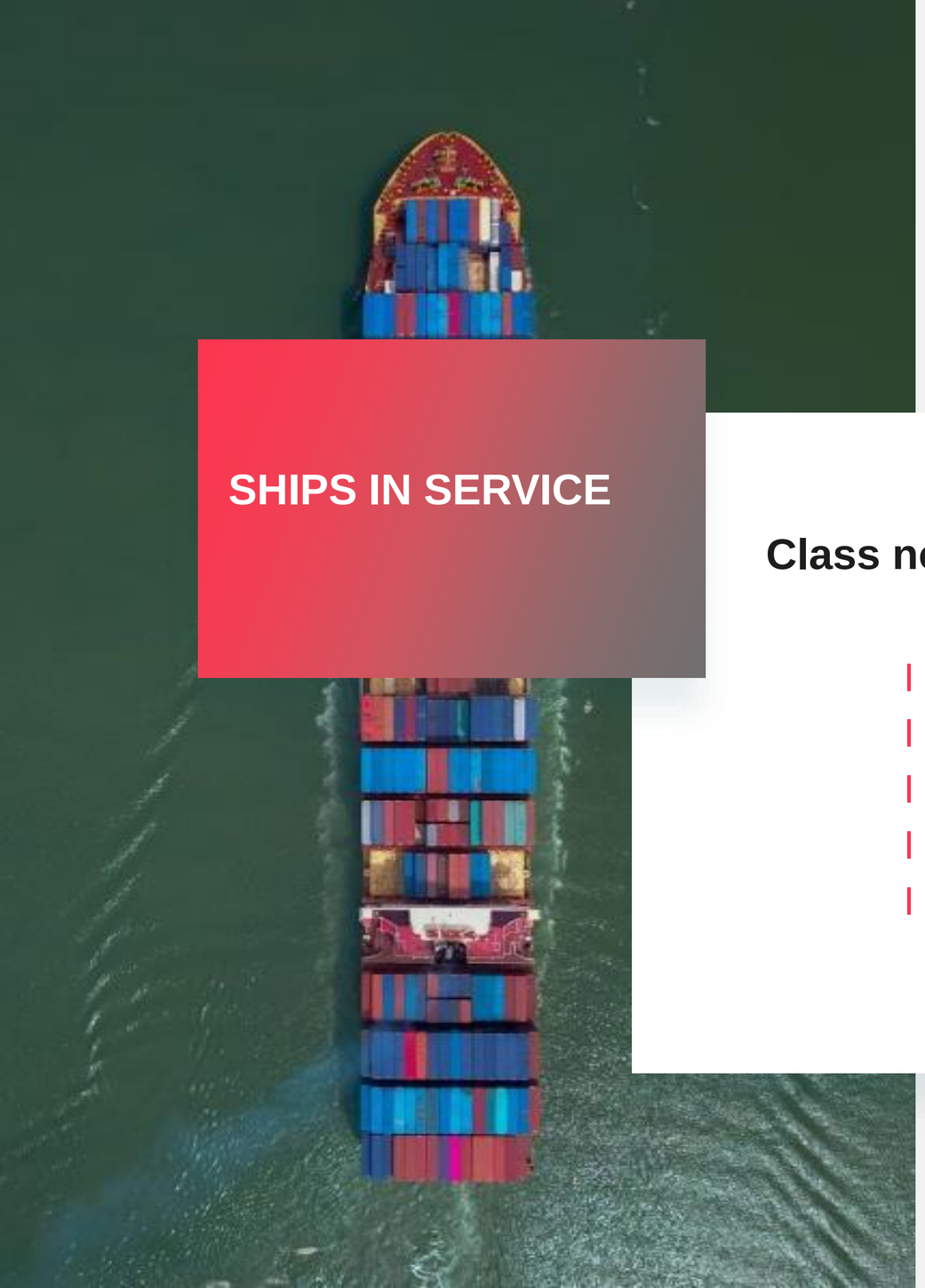
BUREAU VERITAS



SHIPOWNERS OPPORTUNITIES

Opportunities

- See the cyber effort as an enabler, not a constraint
- Protect both company and vessels from cyberattacks
- Retain rare experienced teams involved in maritime cyber security
- Reinforce cyber security on existing vessels to give added value when reselling
- As of today, ask for cyber securing new construction by design to distinguish from competitors



SHIPS IN SERVICE

Class notation in line with IMO Regulation

- Identification of assets & risks
- Protection of critical assets
- Detection through procedures
- Incident response / recovering procedures
- Crew training

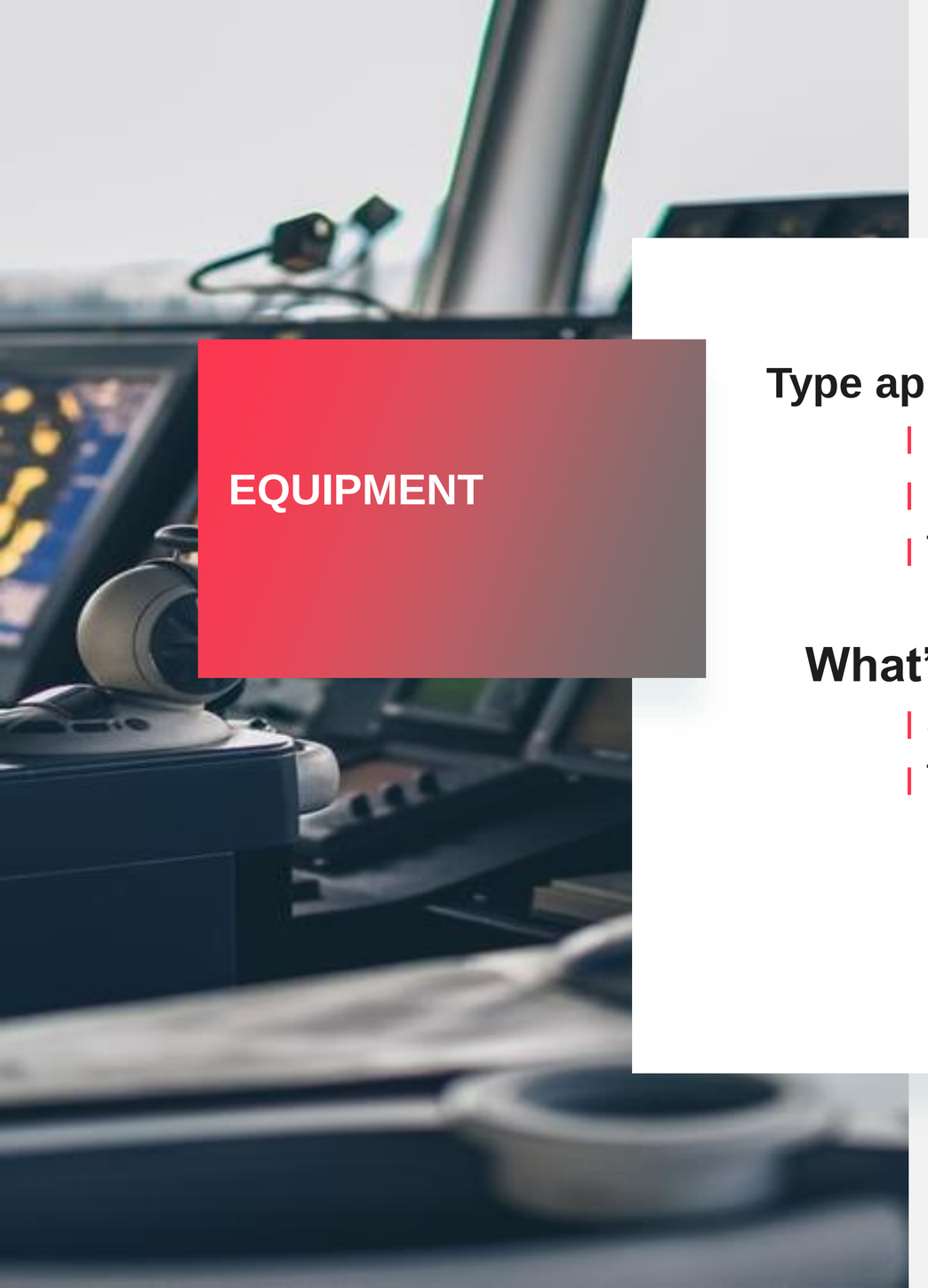
NEW CONSTRUCTION

Class notation in line with IACS UR E26

- Network segmentation
- Network traffic protection
- Logical and physical access management
- Remote access to onboard equipment
- Cyber incidents detection
- Restoration & resilience

What's next?

- Support for shipyards during 'pilot' phase
- Design review



EQUIPMENT

Type approval in accordance with IACS UR E27

- Software hardening
- Logical and physical connectivity
- Testing

What's next?

- Support for manufacturers during 'pilot' phase
- Type approval certification

CONTACT US

PANAGIOTIS ANASTASIOU

Cybersecurity Technical Leader

Member of IACS Cyber Panel

panagiotis.anastasiou@bureauveritas.com

mocybermail@bureauveritas.com

BUREAU VERITAS MARINE & OFFSHORE

WWW.BUREAUVERITAS.COM

POLL 01

WEBINAR

THE JOURNEY TO BETTER CYBERSECURITY IN 2022 AND BEYOND

18TH AUGUST 2022 | 11.00 AM - 12.30 PM

ORGANISED BY:

Varuna Marine Services

Smart Sustainable Shipping

POLL 02

MR. SANJEEV WEWERINKE-SINGH

DIRECTOR - VARUNA MARINE SERVICES B.V.

Varuna Marine Services

Smart Sustainable Shipping

Cyber Waves

Rolling Out Solutions

WILL IT AFFECT US?

All four of the largest maritime shipping companies have all been hit by a ransomware attack between 2017 and Sept 2020.

- French shipping giant CMA CGM has been hit by a ransomware attack Sept 2020.
- Mediterranean Shipping Company - hit in April 2020 by an unnamed malware strain that brought down its data center for days.
- COSCO - brought down for weeks by ransomware in July 2018.
- APM-Maersk - taken down for weeks by the NotPetya ransomware/wiper in 2017.

WHAT SHALL CYBER RISK MANAGEMENT INCLUDE?

Identify threats

Understand the external cybersecurity threats to the ship. Understand the internal cybersecurity the threat posed by inappropriate use and poor cyber security practices.

Respond to and recover from cyber security incidents

Respond to and recover from cybersecurity incidents using the contingency plan. Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.

Identify vulnerabilities

Develop inventories of onboard systems with direct and indirect communications links. Understand the consequences of a cyber security threat on these systems. Understand the capabilities and limitations of existing protection measures.

Establish response plans

Develop contingency plans to effectively respond to identified cyber risks.

Assess risk exposure

Determine the likelihood of vulnerabilities being exploited by external threats. Determine the likelihood of vulnerabilities being exposed by inappropriate use. Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.

Develop protection and detection measures

Reduce the likelihood of vulnerabilities being exploited through protection measures. Reduce the potential impact of a vulnerability being exploited.

IACS UR ER 26 and ER 27

- This Unified Requirement is to be uniformly implemented by IACS Societies on ships contracted for construction on or after 1 January 2024 and may be used for other ships as non-mandatory guidance.

- Primary goals is to achieve cyber resilience of ships

  - Identify : Inventory of hardware and software. Inventory to be updated for entire life of ship.
  - Protect : Security zones, Network Protection Safeguard, Antimalware, Access control, Wireless communication, remote access control and communication with untrusted network and use of mobile and potable devices
  - Detect :
    - **Network Operation Monitoring** , Monitoring and recording of device management activities. A monitoring system that can detect anomalies in networks and that can use post-incident analysis provides the ability to appropriately respond and further recover from a cyber event.
    - **Diagnostic functions of CBS and networks** :The ability to verify intended operation of the security functions is important to support management of cyber resilience in the lifetime of the ship. Tools for diagnostic functions may comprise automatic or manual functions such as self-diagnostics capabilities of each device, or tools for network monitoring (such as ping, traceroute, ipconfig, netstat, nslookup, Wireshark, nmap, etc.).
  - Respond : Incident response plan , Local ,independent and/or manual operation , Network isolation, fall back to a minimal risk condition.
  - Recover : Recovery plan , back up and restore capability , Controlled shut down, reset , roll back and restart.

IACS UR ER 26 and ER 27

- **Test Plan for performance evaluation and testing :**

  - During operational life of the ship, the Shipowner, with the support of Systems Integrator and Suppliers, shall keep the Test Plan up to date and aligned with the CBSs onboard the ship and the networks connecting such systems to each other and to other CBSs not onboard (e.g. ashore).
  - The Shipowner shall update the Test Plan considering the changes occurred on CBSs and networks onboard, possible emerging risks related to such changes, new threats, new vulnerabilities and other possible changes in the ship's operational environment.
  - The Shipowner shall retain onboard a copy of results of execution of tests and an updated Test Plan and make them available to the Classification Society.

- **Risk Assessment**

  - A risk assessment shall be carried out in case any of the CBSs falling under the scope of applicability of this UR is excluded from the application of relevant requirements. The risk assessment shall provide evidence of the acceptable risk level associated to the excluded CBSs.
  - Such exclusion can be accepted by the Classification Society only if evidence is given that the risk level associated to the operation of the CBS is under an acceptable threshold by means of specific risk assessment.
  - During the operational life of the ship, the Shipowner shall update the risk assessment considering the constant changes in the cyber scenario and new weaknesses identified in CBS onboard in a process of continuous improvement.

Challenges with existing solutions

- Firewalls
- NAC
- Vulnerability scanners
- Agents

Perimeter protection only

Complex configuration and maintenance

Limited visibility

Limited IoT understanding

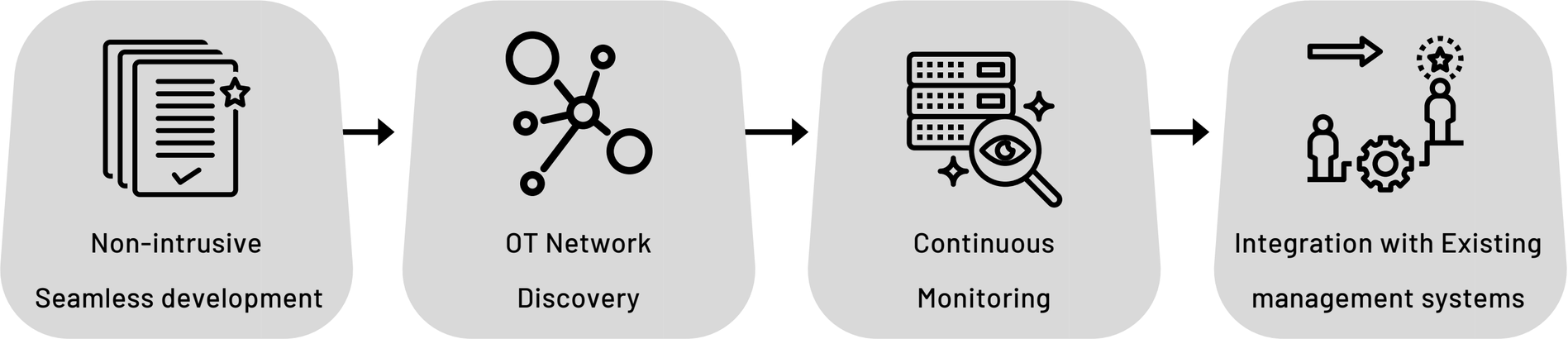
Unable to detect emerging threats

24/7 Network Monitoring : CyberShell

It requires a shift in the security mindset from

"How can I air gap or isolate?" to "How can I stay secure while connected?"

How it works:

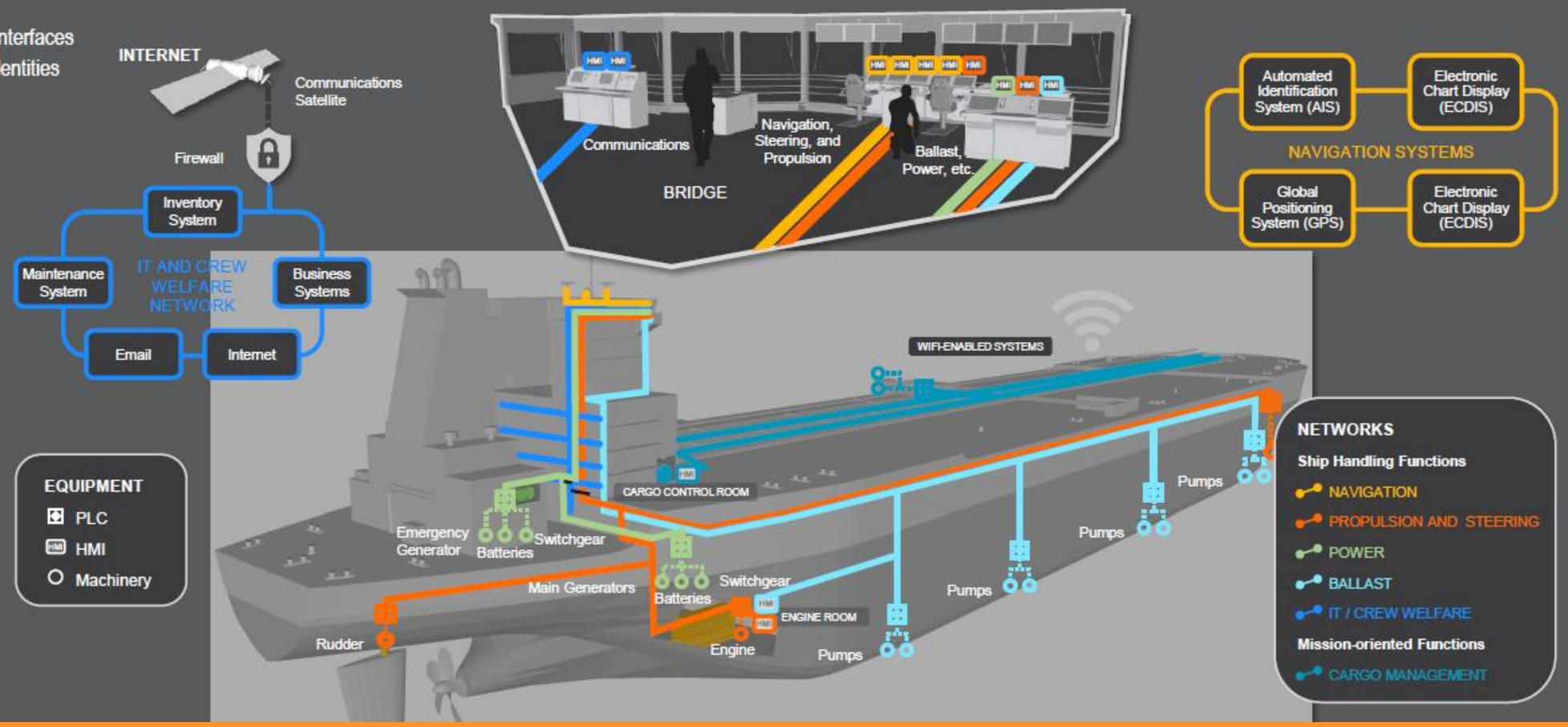


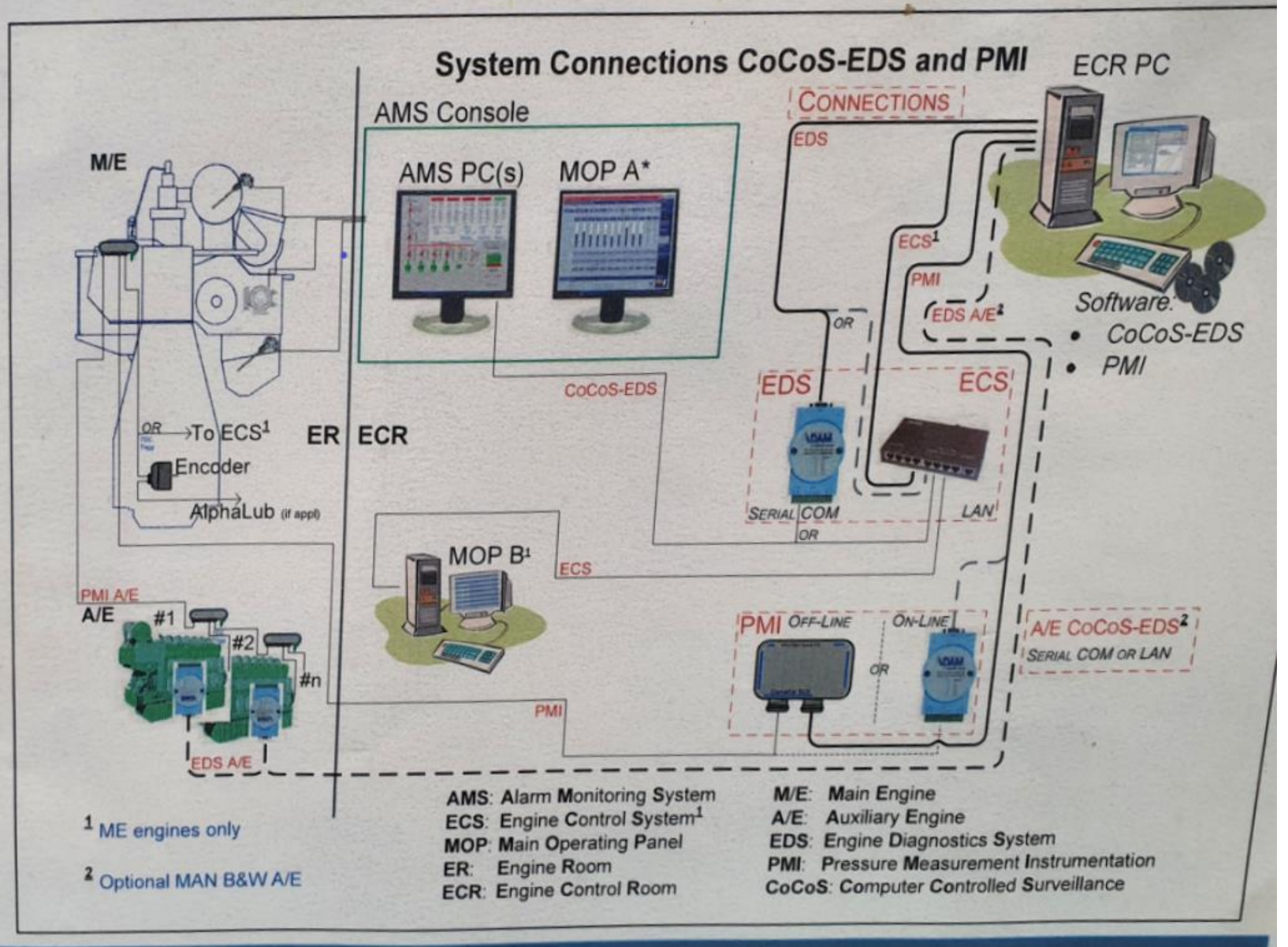
The Virtual Asset

Maritime assets are designed to perform a specific set of functions. For vessels, these include both ship handling and mission-oriented functions. This diagram illustrates several representative functions for a tanker ship and how they are implemented using various onboard networks.

The cyber security risk exposure of an asset is highly dependent on the number of:

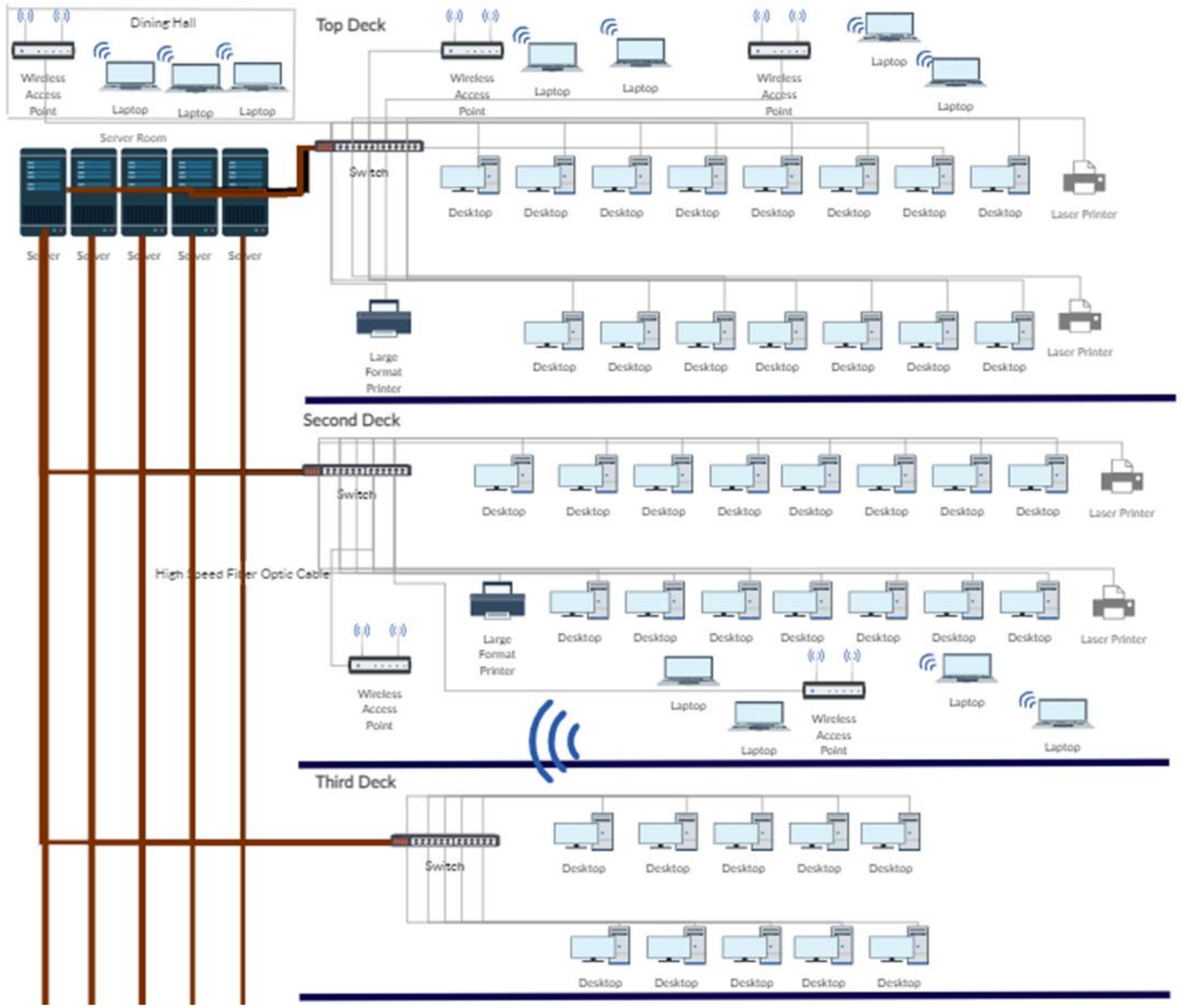
1. Safety-critical functions
2. Network connections and interfaces
3. Authorized/unauthorized identities




System Connections CoCoS-EDS and PMI
ECR PC
CONNECTIONS
AMS Console
AMS PC(s)
MOP A*
M/E
EDS
ECS1
PMI
EDS A/E2
OR
Software:
• CoCoS-EDS
• PMI
CoCoS-EDS
EDS
ECS
OR
To ECS1
ER
ECR
Encoder
AlphaLub (if appl)
SERIAL COM
OR
LAN
MOP B1
ECS
PMI A/E
A/E
#1
#2
#n
PMI OFF-LINE
ON-LINE
OR
A/E CoCoS-EDS2
SERIAL COM OR LAN
PMI
EDS A/E
1 ME engines only
2 Optional MAN B&W A/E
AMS: Alarm Monitoring System
ECS: Engine Control System1
MOP: Main Operating Panel
ER: Engine Room
ECR: Engine Control Room
M/E: Main Engine
A/E: Auxiliary Engine
EDS: Engine Diagnostics System
PMI: Pressure Measurement Instrumentation
CoCoS: Computer Controlled Surveillance


VSAT RACK
KVH
ONLINE
TRACKING 60.1E
D-Link
D-Link

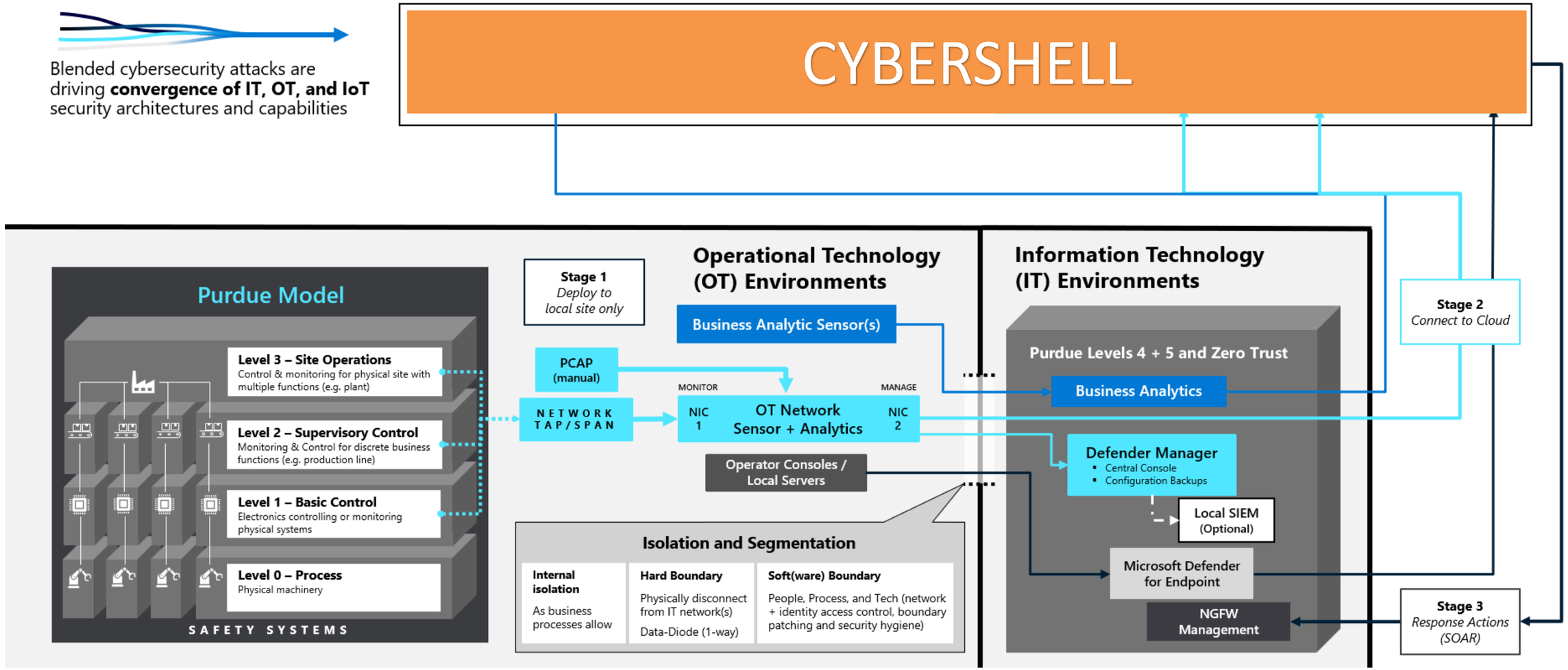
Network Mapping Sample



Operational Technology (OT) Deployment Options

Apply zero trust principles to securing OT and industrial IoT environments

Blended cybersecurity attacks are driving **convergence of IT, OT, and IoT** security architectures and capabilities



Ecosystem momentum

IHV → Device → Connectivity Provider → ISV → Service Provider → SI → Professional Services → Consulting → Managed Services → Customer

Microsoft Partners	Varuna Marine Services – Smart Sustainable Shipping; Cyber Waves – Rolling Out Solutions
OT Landscape	GE; Rockwell Automation; ActionPoint – I.T. Services & Software Development; Hitachi Solutions; relayr – bring things to life; codit; Schneider Electric; energisme; SIEMENS; conplement; Johnson Controls; ptc; Schlumberger; Atos Worldline; DUNAV NET; COPADATA; Honeywell; SAP; ABB; esri; OSI; G3 IoT; ICONICS

Finished Intelligence

Turning raw data into finished, actionable intelligence.

CyberShell

Remote and Onsite OT Systems

Coverage

- OT and IT
- Fleet-wide / Company-wide
- Own Fleet
- Managed Fleet
- All Systems, Networks and Devices

Considerations

- Passive OT Monitoring (agentless)
- Low Bandwidth
- Secure Transmission

Finished Actionable Intelligence

Monitoring and Alert Management

- 24/7/365
- Tier 1 & Tier 2
- Explanation and direction

Analytics and Reporting

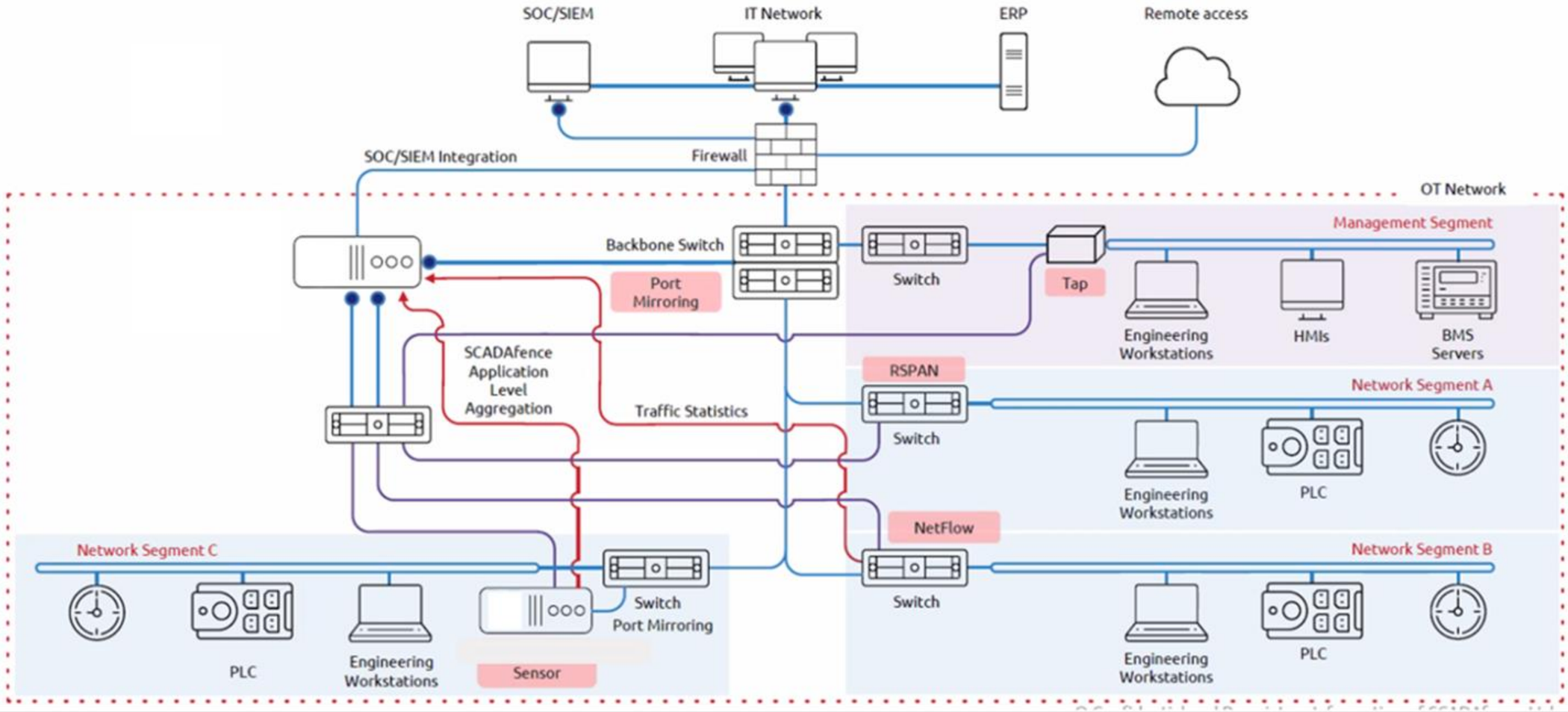
- Monthly/quarterly reports
- Insights and analysis
- Summarized and actionable

Threat Hunting

- Proactive searching
- Advanced threats
- Applied threat intelligence

Finished intelligence requires the right tools, technology and domain expertise

FLEXIBLE DEPLOYMENT OPTIONS



Dashboard

All data | SoC Dashboard

178	27	10	1.8 GB	8.2 GB	219	28.02 Kb/s	Critical
Total Assets	Controllers	HMIs	L3 Traffic	L2 Traffic	Alerts	Current bandwidth	Health

Mb/s

Top Alerts

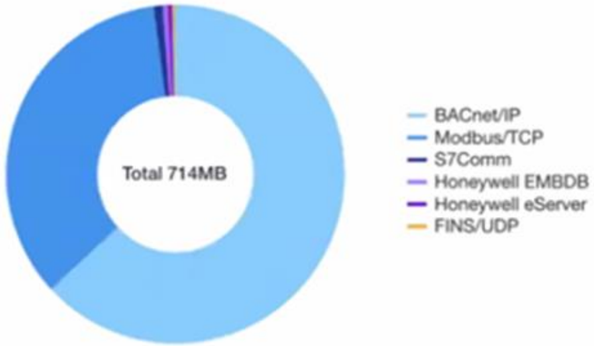
All Categories

- **Group-to-group communication**
  05/26/2020 18:02:25
- **Trickbot trojan communication detected**
  07/18/2020 07:33:16
  192.168.0.102
- **Security Incident Detected**
  05/20/2020 14:07:47
  192.168.0.222
- **SMB exploitation attempt - MS17-10 EternalBlue**
  06/11/2019 15:42:04
  192.168.1.24
- **Vulnerability assessment tool detected - Nessus**
  08/28/2017 11:22:38
  192.168.1.16
- **TeamViewer inbound connection estalished**
  08/16/2020 07:33:51
  192.168.1.135
- **TeamViewer inbound connection estalished**
  05/26/2020 16:17:08

Industrial Protocols

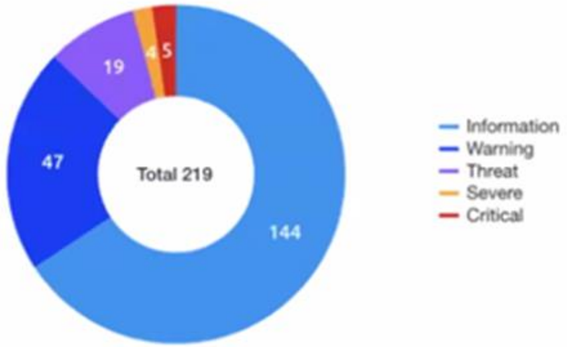
Show Others

Select Protocols | Protocols Report



Alerts

SEVERITY | TYPE | CATEGORY | DAILY



Alerts Pivot by Type

View Report by Type

Alert Type	Severity...	# of Alerts
API	●	2
Vulnerability assessment tool dete...	●	1
Trickbot trojan communication det...	●	1

Assets Pivot

Select Dimension: Device type

Device type	Total ↓
Others	88
Workstation	24

Assets Manager

CVE Management WMI Hosts

L3 Assets | L2 Assets | External Hosts | Assets Pivot | Threat Assessment

Select Columns | All Types | Type exact IP

IP	Hostname	MAC	Vendor	OS	Device types	Alerts	# Int.	# Ext.	Total Traffi...	First seen	Last Seen
192.168.0.170	Mitsubishi ...	58:52:8A:B7:AB:...	Mitsubishi ...		PLC	1 1	4	0	11.27 MB	03/17/2019 12:29:14	04/24/2019 14:14:53
192.168.0.125	Eng_STA_6	00:0C:29:8B:18:D6	VMware, Inc.	Windows 7	Engineering...	2 1	2	0	11.21 MB	03/17/2019 13:53:28	03/17/2019 15:21:06
10.11.0.154		5C:F9:DD:73:FF:...	Dell Inc.	Windows	Engineering...	0	1	0	8.49 MB	08/28/2019 10:48:56	08/28/2019 10:49:52
192.168.0.155	PLC-9054e	00:24:59:0A:A9:C4	ABB Autom...		PLC	1	3	0	6.86 MB	03/17/2019 12:19:42	04/24/2019 14:09:15
192.168.0.123	Eng_STA_1	00:0C:29:17:D1:76	VMware, Inc.	Windows 7	Engineering...	1 1	8	0	6.17 MB	03/17/2019 12:19:43	03/17/2019 13:08:03
192.168.0.140	PLC-TE246	00:80:F4:1B:CD:22	Telemechan...		PLC	1	5	0	5.56 MB	03/17/2019 12:19:50	04/24/2019 14:16:50
10.11.0.202		F4:54:33:AD:39:7A	Rockwell A...		PLC	1 1	1	0	5.52 MB	05/26/2020 14:56:38	05/26/2020 15:27:04
192.168.0.107	Eng_STA_4	00:0C:29:58:97:76	VMware, Inc.	Windows 7	Engineering...	2	3	0	5.41 MB	03/17/2019 15:00:43	06/11/2019 15:42:04
192.168.0.135		AC:64:17:12:5C:51	Siemens AG		PLC	1 2	5	0	4.38 MB	03/17/2019 12:20:09	04/24/2019 14:16:52
10.117.2.17	xperion_srvb	00:10:18:C8:98:00	Broadcom	Windows S...	Experion eS...	1 1	43	0	3.5 MB	10/19/2020 14:32:02	10/27/2020 15:23:14
10.212.120.200		00:FF:84:41:5A:19	AP-NordVPN		VPN client	0	0	0	2.72 MB	04/10/2016 07:12:12	04/10/2016 07:33:19
10.117.1.11	xperion_srv...	00:10:18:C0:86:FC	Broadcom	Windows S...	Experion eS...	1 1	51	0	2.54 MB	10/19/2020 14:32:03	10/27/2020 15:22:14
192.168.0.141	Schneider_...	00:80:F4:1B:CD:22	Telemechan...			1	46	1	2.54 MB	03/17/2019 12:19:45	04/24/2019 14:09:14
192.168.0.130		28:63:36:7E:85:49	Siemens AG		PLC	1	6	0	2.48 MB	03/17/2019 12:19:43	04/24/2019 14:16:53
192.168.0.50	Eng_STA_2	00:0C:29:65:1C:29	VMware, Inc.	Windows 7	VoIP	1	1	0	2.41 MB	03/17/2019 13:23:18	03/17/2019 13:49:24

1 2 3 4 5 6 7 8 9 10 ...

16 - 30 of 178 items

Assets Manager > 192.168.0.170

192.168.0.170 (Mitsubishi R04)

1 Information 1 Threat **Connections:** 4 Internal 5 Exposure Groups

Device types:	PLC
OS:	
Hostname:	Mitsubishi R04
Vendor:	Mitsubishi Electric Corporation
MAC:	58:52:8A:B7:AB:EC
First seen:	March 17th 2019, 12:29:14
Last Seen:	April 24th 2019, 14:14:53
NIC Type:	Ethernet

Additional Details

Module name:	R04CPU

Organization Details

Criticality:	High
OU:	Substation_12
Owner:	Harry D.
Physical Location:	
Comment:	
Product for CVE:	
Version for CVE:	

Open Alerts

ID	Severity	Description	Status	Details	MITRE ATT&CK	Alert Time
190		PLC start command issued	In Progress	192.168.0.125 (Eng_STA_6) sent a PLC start command to PLC on 192.168....	Execution > Change Pr...	03/17/2019 14:06:47
116		New host detected	Created	New host detected: 192.168.0.170 (Mitsubishi R04) from source: ARP Packet.		03/17/2019 12:29:14

1

1 - 2 of 2 items

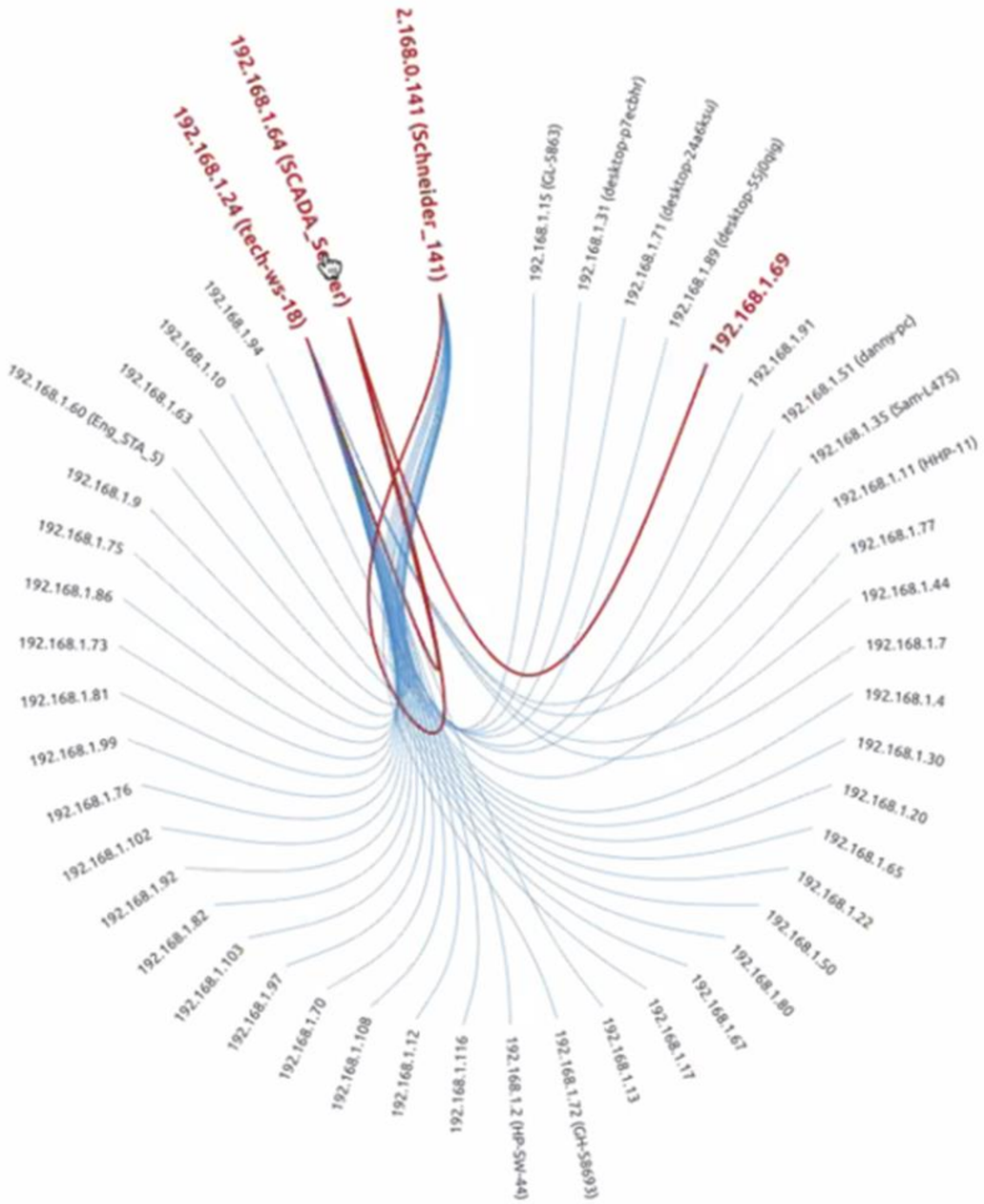
Network Maps Top Level > 192.168.1.x

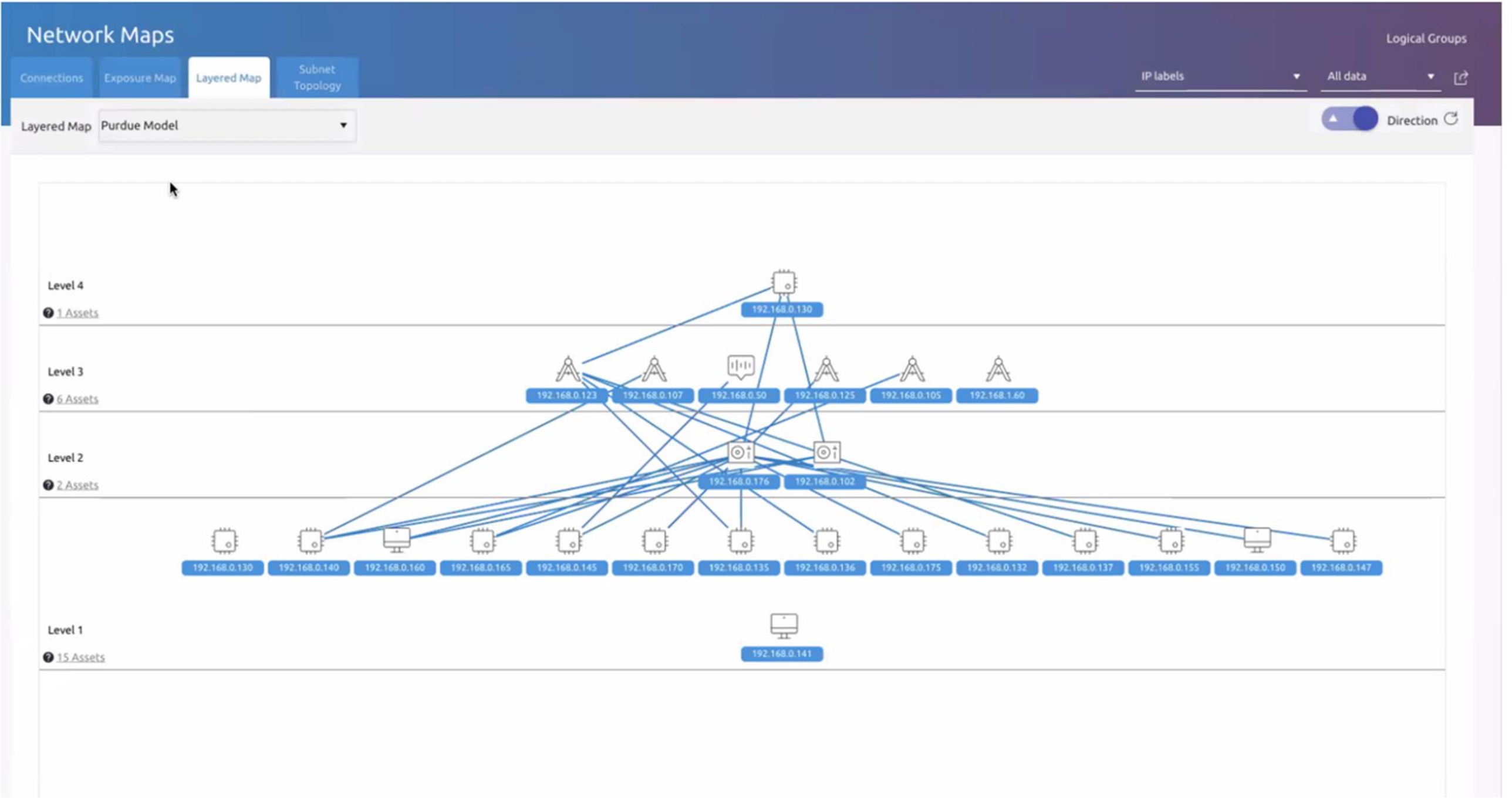
Logical Groups

Connections | Exposure Map | Layered Map | Subnet Topology

All Types | Search IP/Hostname | Hostname & IP address | All data

YES Connections only




Network Maps
Logical Groups
Connections
Exposure Map
Layered Map
Subnet Topology
IP labels
All data
Layered Map
Purdue Model
Direction
Level 4
1 Assets
192.168.0.130
Level 3
6 Assets
192.168.0.123
192.168.0.107
192.168.0.50
192.168.0.125
192.168.0.105
192.168.1.60
Level 2
2 Assets
192.168.0.176
192.168.0.102
192.168.0.130
192.168.0.140
192.168.0.160
192.168.0.165
192.168.0.145
192.168.0.170
192.168.0.135
192.168.0.136
192.168.0.175
192.168.0.132
192.168.0.137
192.168.0.155
192.168.0.150
192.168.0.147
Level 1
15 Assets
192.168.0.141

Traffic Analyzer

Protocols over Time

IP Conversations | TCP/UDP Conversations | Protocols | Industrial Protocols | Industrial Layer 2

All Protocols | Type Port | All data

Protocol	Dest. Port	Trans...	A to B Packets	B to A Packets	A to B Bytes	B to A Bytes	Total
BACnet/IP	47808	UDP	836.77K	831.72K	197.35 MB	253.34 MB	450.68 MB

Conv...	Source IP	Src. Port	Dest. IP	A to B Packets	B to A Packets	A to B Bytes	B to A Bytes	Total	In...
1	10.15.5.102	generic	10.15.5.111	124.44K	124.46K	82.2 MB	125.65 MB	207.85 MB	
1	10.15.5.111	47808	10.15.5.127	364.05K	364.03K	58.4 MB	45.79 MB	104.18 MB	
6	10.15.5.100	47809	10.15.5.111	107.59K	105.12K	19.92 MB	28.19 MB	48.1 MB	
1	10.15.5.102	generic	10.15.5.112	62.57K	62.53K	13.16 MB	20.02 MB	33.17 MB	
1	10.15.5.102	generic	10.15.5.113	61.91K	61.84K	13.12 MB	19.98 MB	33.1 MB	
6	10.15.5.100	47809	10.15.5.112	93.42K	91.8K	7.3 MB	8.89 MB	16.2 MB	
5	10.15.5.100	47809	10.15.5.113	16.86K	15.28K	2.71 MB	4.14 MB	6.85 MB	
2	192.168.0.180	47808	192.168.0.181	5.36K	5.98K	498.59 KB	629.29 KB	1.13 MB	
1	192.168.0.176	47808	192.168.0.180	444	444	32.76 KB	39.75 KB	72.5 KB	
1	192.168.0.20	65536	192.168.0.181	112	233	7.06 KB	16.64 KB	23.7 KB	

1 2

1 - 10 of 11 items

Protocol	Dest. Port	Trans...	A to B Packets	B to A Packets	A to B Bytes	B to A Bytes	Total
Modbus/TCP	502	TCP	2.28M	2.06M	135.72 MB	123.01 MB	248.54 MB
iPulse-ICS	20222	TCP	49.17K	85.17K	3.01 MB	101.41 MB	104.42 MB
HTTPS	443	TCP	102.99K	80.75K	12.69 MB	88.81 MB	101.5 MB
MS-SQL-s	1433	TCP	638.64K	637.78K	40.64 MB	41.37 MB	82.01 MB

Alerts Manager

Alerts Policy | Firewall Rules | Logs

Open 219 | Resolved 97 | Don't show 1 | Stale 90 | All 316 | Alerts Pivot

Select Columns | All Types | All Severities | Mark 0 selected as Resolved

ID	Severity ↓	Description	Status	IP	Hostname	Details	Last Event Time
50100		Group-to-group communication	In Progress			User rule "Unauthorized Traffic": Communication between group "DMZ_Plant...	05/26/2020 18:02:25
1446		Trickbot trojan communication detected	In Progress	192.168.0.102	desktop-cs7vbmu	192.168.0.102 (desktop-cs7vbmu) is communicating with a Trickbot C&C ser...	07/18/2020 07:33:16
554		Security Incident Detected	In Progress	192.168.0.222	WSTA_4	Multiple alerts on this IP.	05/20/2020 14:08:03
465		SMB exploitation attempt - MS17-10 Ete...	In Progress	192.168.1.24	tech-ws-18	SMB exploit detected - device 192.168.1.24 (tech-ws-18) sent an exploit to d...	02/19/2020 16:18:14
10		Vulnerability assessment tool detected - ...	In Progress	192.168.1.16	scadafence-pc	Nessus communication detected from 192.168.1.16 (scadafence-pc) to target...	02/12/2020 13:31:08
50103		TeamViewer inbound connection estalish...	In Progress	192.168.1.135	scadafence-rbi10d	TeamViewer inbound connection was established from device 213.227.181.1...	08/16/2020 07:34:08
51888		TeamViewer inbound connection estalish...	In Progress	10.11.0.200	powersvr1	TeamViewer inbound connection was established from device 192.168.1.135 (...	08/16/2020 07:34:08
559		Communication with vulnerable device	In Progress	192.168.0.132	plc_32	Industrial device 192.168.0.132 (plc_31) has communicated with device 192.1...	11/05/2020 13:12:37
518		Domain reputation alert	In Progress	192.168.0.101	WS-yk75	Device 192.168.0.101 (WS-yk75) tried to resolve a known malicious domain n...	02/12/2020 13:31:08
50102		New Source IP Connecting to industrial ...	In Progress	10.11.0.202		Unexpected conversation detected between IP address 10.11.0.154 (Enginee...	05/22/2020 08:22:29
50101		Industrial parameter value out of range	In Progress	10.11.38.100		User rule Analog Value Validation (profile-based): Device 10.11.38.100, report...	08/29/2017 02:59:23
51867		Programming read command detected	In Progress	10.11.0.202		10.11.0.200 (powersvr1) sent a programming read sequence to PLC on 10.11...	05/26/2020 15:07:34
50042		Programming write command detected	In Progress	10.77.60.131	PLC_131	10.77.1.60 (win-k4tva753kgg) sent a programming write sequence to PLC on ...	07/29/2018 10:44:20
50019		PLC stop command issued	In Progress	10.77.0.140	PLC_140	10.77.1.60 (win-k4tva753kgg) sent a PLC stop command to PLC on 10.77.0.1...	01/16/2019 13:30:38
50001		PLC stop command issued	In Progress	192.168.60.150		192.168.60.11 sent a PLC stop command to PLC on 192.168.60.150, using ...	05/17/2020 16:58:10

1 2 3 4 5 6 7 8 9 10 ...

1 - 15 of 219 items

Compliance Report

NIST-CSF | Production Lines: 1-3 | Max IPs (max 50) 50 | Display only relevant alerts | Generate | Export

- NERC-CIP
- ISO-27001
- NIST-1800-23
- NCSC-CAF
- CMMC5
- CMMC2
- CMMC Level 1

ce Governance Report

Site: Production Lines: 1-3

Standard: NIST-CSF

Report issued on: Jun 15, 2021

Issued by: admin

Security Reporting

Report Configuration

Export

Security Report Configuration

DISPLAY PARAMETERS | SECTION VISIBILITY | MAPS CONFIGURATION

- [x] Analysis Summary
- [x] Top IPs at Risk
- [x] Asset Inventory
- [x] Network Map
- [x] Exposure Models
- [x] Layered Maps
- [x] Protocol Statistics
- [x] Bandwidth Usage
- [x] Subnets Discovered
- [x] Open Security Alerts
- [x] Network Anomalies
- [x] Open CVEs
- [x] About SCADAfence

Cancel

Update Report

Tabl

THANK YOU!

You can reach us at:

- info@varunamarine.eu
- technical@varunamarine.eu
- tech@cyberwaves.eu

OR

Visit our website for more information:
www.varunamarine.eu

WEBINAR

THE JOURNEY TO BETTER CYBERSECURITY IN 2022 AND BEYOND

18TH AUGUST 2022 | 11.00 AM - 12.30 PM

ORGANISED BY:

Varuna Marine Services

Smart Sustainable Shipping

POLL 03


Q
A

WEBINAR

THE JOURNEY TO BETTER CYBERSECURITY IN 2022 AND BEYOND

18TH AUGUST 2022 | 11.00 AM - 12.30 PM

ORGANISED BY:

Varuna Marine Services

Smart Sustainable Shipping

POLL 04


KEY
TAKEAWAYS

Thank You

Varuna Marine Services

Smart Sustainable Shipping

CONTACT US AT:

info@varunamarine.eu

marketing@varunamarine.eu

www.varunamarine.eu

+ 31 107 640 935

FOLLOW US ON:

@Varunamarine

@varunamarineservices