CyberHelm

by Cybeta

Avoiding Alert Fatigue

Prioritizing Cyber Threat Remediation in the Maritime Industry

CIO Forum
Bergen, Norway
November 27, 2019

Fredrik Munck
fredrik.munck@cybeta.com

WHO WE ARE:

Cybeta

- **Pre-emptive cyber security service**
  - ✧ Predictive algorithms identify assets most vulnerable to specific cyber attacks
- **Built by security experts**
  - ✧ US Intelligence & anti-terrorism experience
- **Continuous monitoring**
  - ✧ Canvass Deep & Dark web for threats and Zero-day vulnerabilities

CyberHelm

- **Maritime application**
  - ✧ Proprietary database of ship-based operating technologies not covered by CNA alerts
  - ✧ Includes shore-side analysis and alerts for entire digital enterprise
  - ✧ Ever-expanding database as maritime technologies come under increasing attack

CYBER ATTACKS ➡ On the rise in the maritime industry

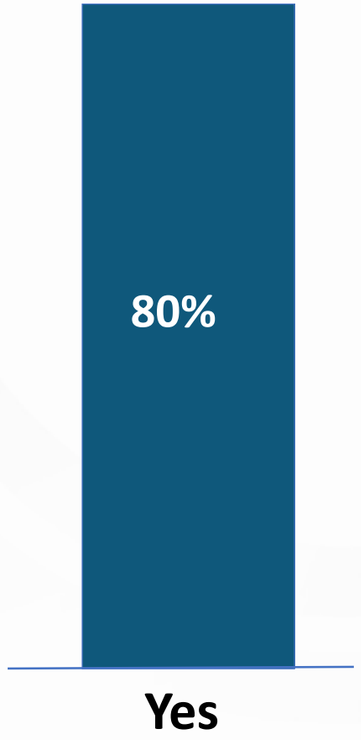
MAERSK
Collateral victim of NotPetya 2017

PORT OF SAN DIEGO
Malware 2018

AIS POSITIONING
Hacked 2013

CLARKSON PLC
Ransomware 2017

Has your **company** been a target of cyber attacks?*



** Jones Walker Insurance Agency, Data Privacy Group survey of 126 maritime industry executives*

MARITIME CYBER SECURITY CHALLENGES

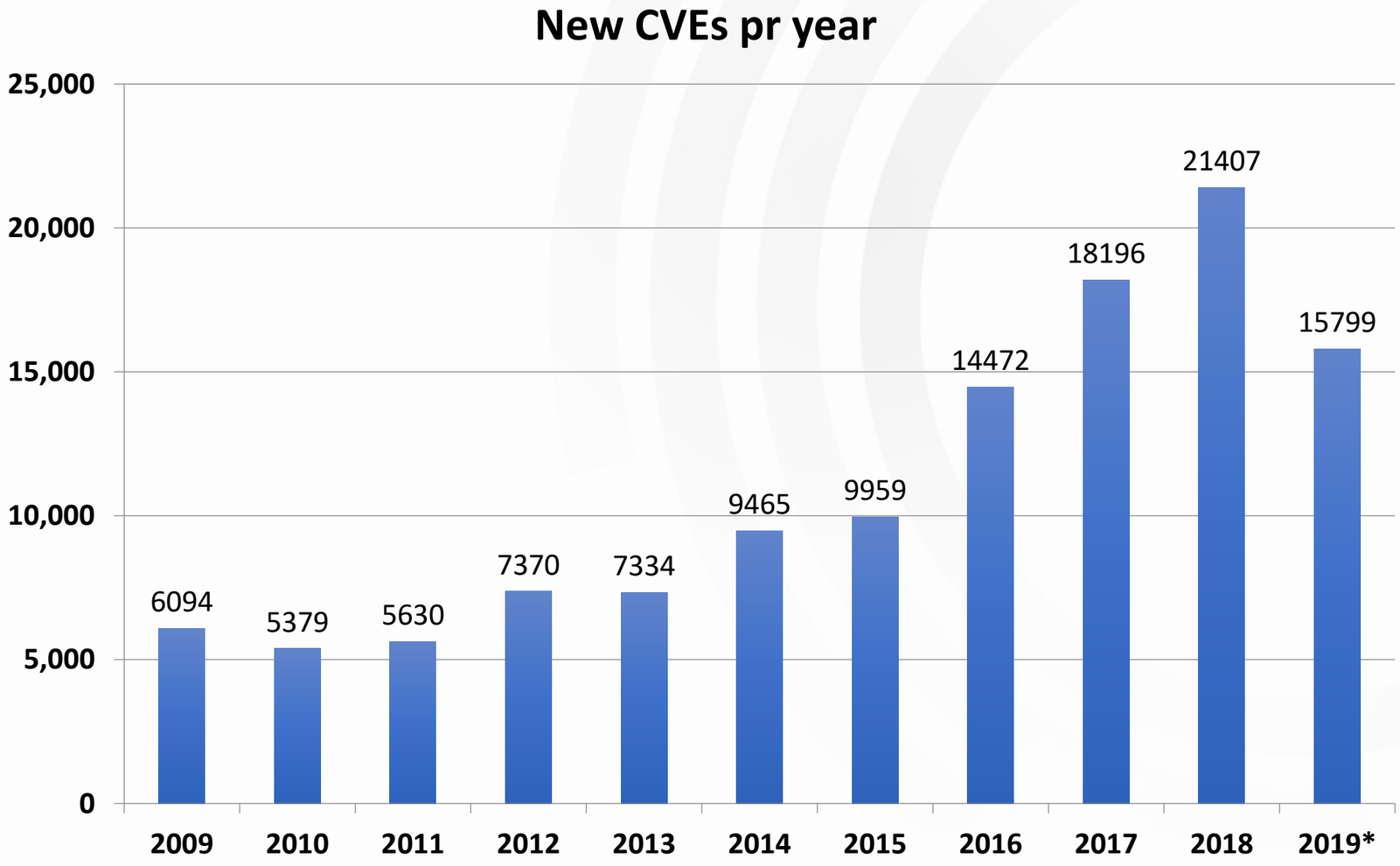
BEHAVIORAL “Hygiene”

- Fractured IT interaction (crews, passengers, ports, staff, partners…)

TECHNOLOGY “Hygiene”

1. **ALERT FATIGUE**
   - ~5,000+ new CVE alerts issued per quarter
2. **SHIP-SIDE OPERATING TECHNOLOGIES**
   - Hundreds of technologies not tracked by CNAs
3. **MANY ATTACK VECTORS**
   - Large Technology Footprints (Offices, Vessels, Agents, Terminals etc.)

1. ALERT FATIGUE ➡ more than 50 new CVEs issued per day..and growing



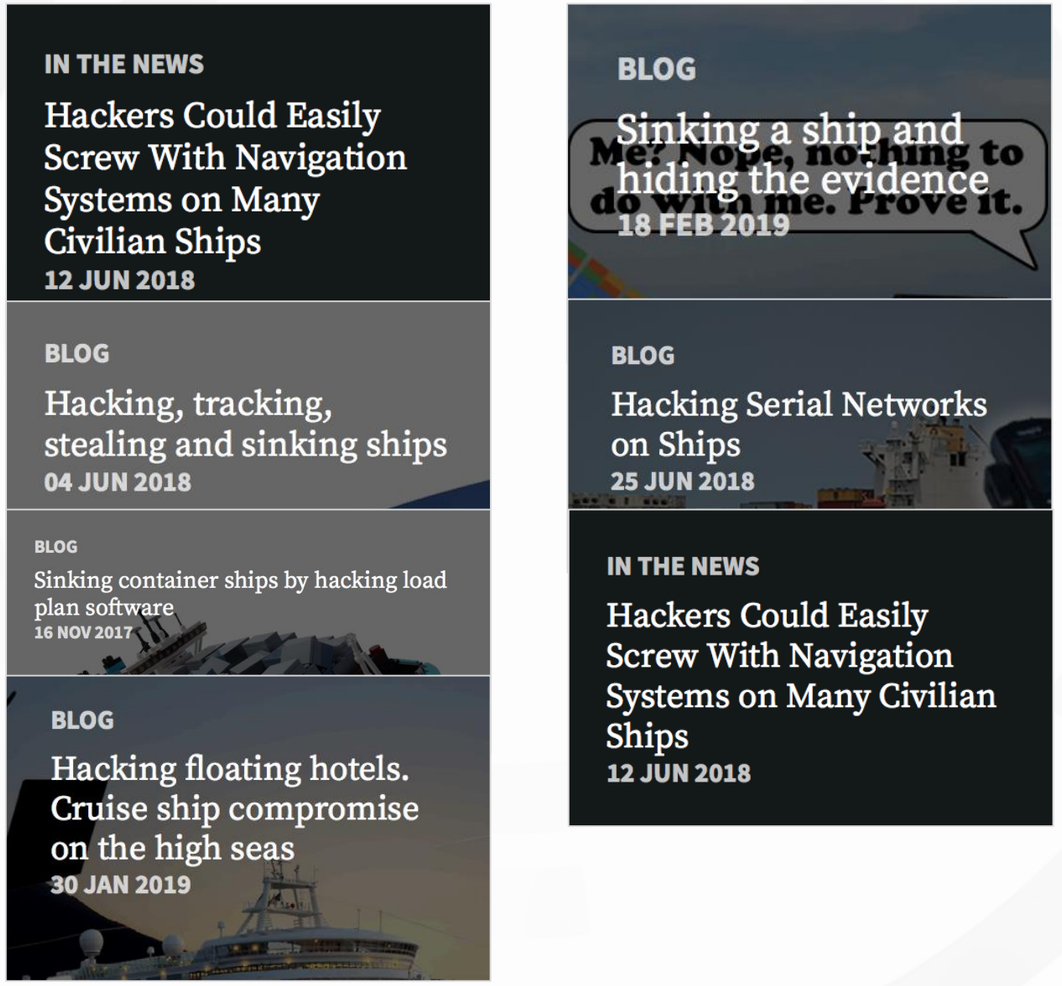
SOURCE: Mitre.org

2. SHIP-SIDE OPERATING SYSTEMS ➡ Easy prey for threat actors

US COAST GUARD Safety Alert (July 2019)

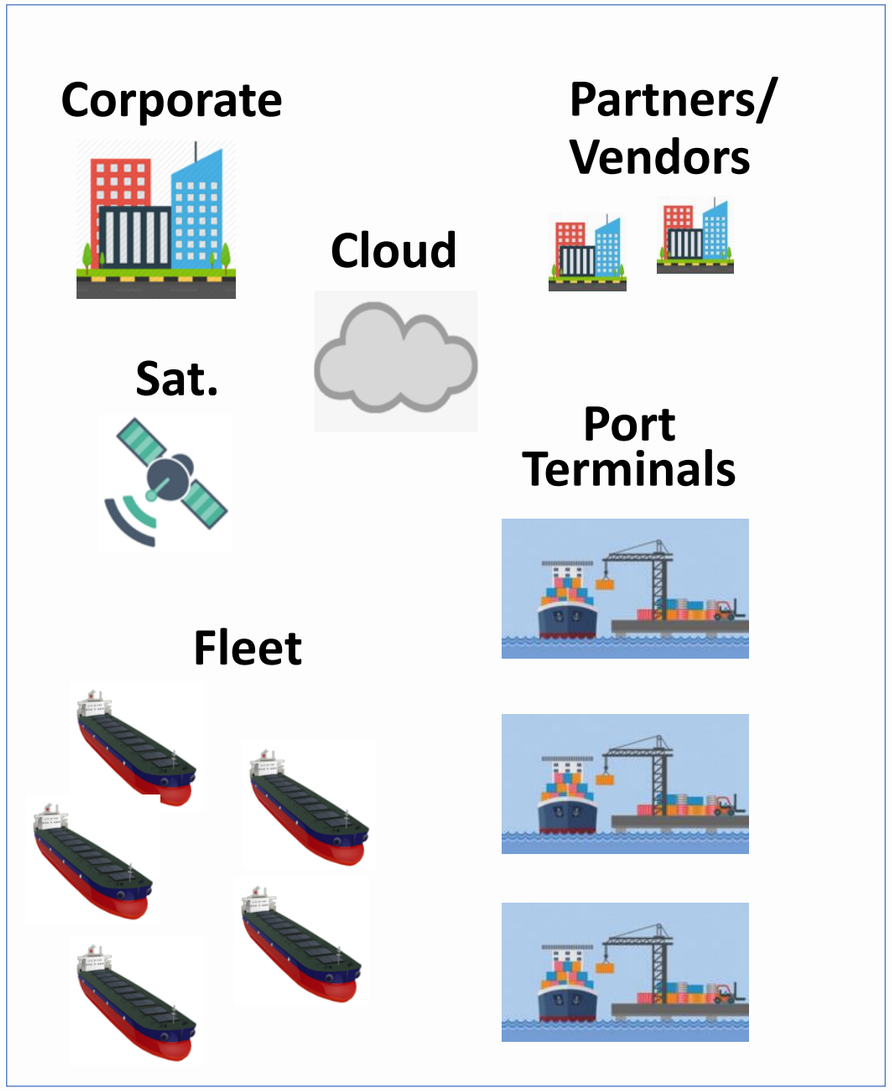
- Deep draft vessel en route towards port of NY/NJ needed assistance from Coast Gard…
- "..malware significantly degraded functionality of onboard computer system…»
- *"..common practice for cargo data to be transferred at pier, via a USB drive."*

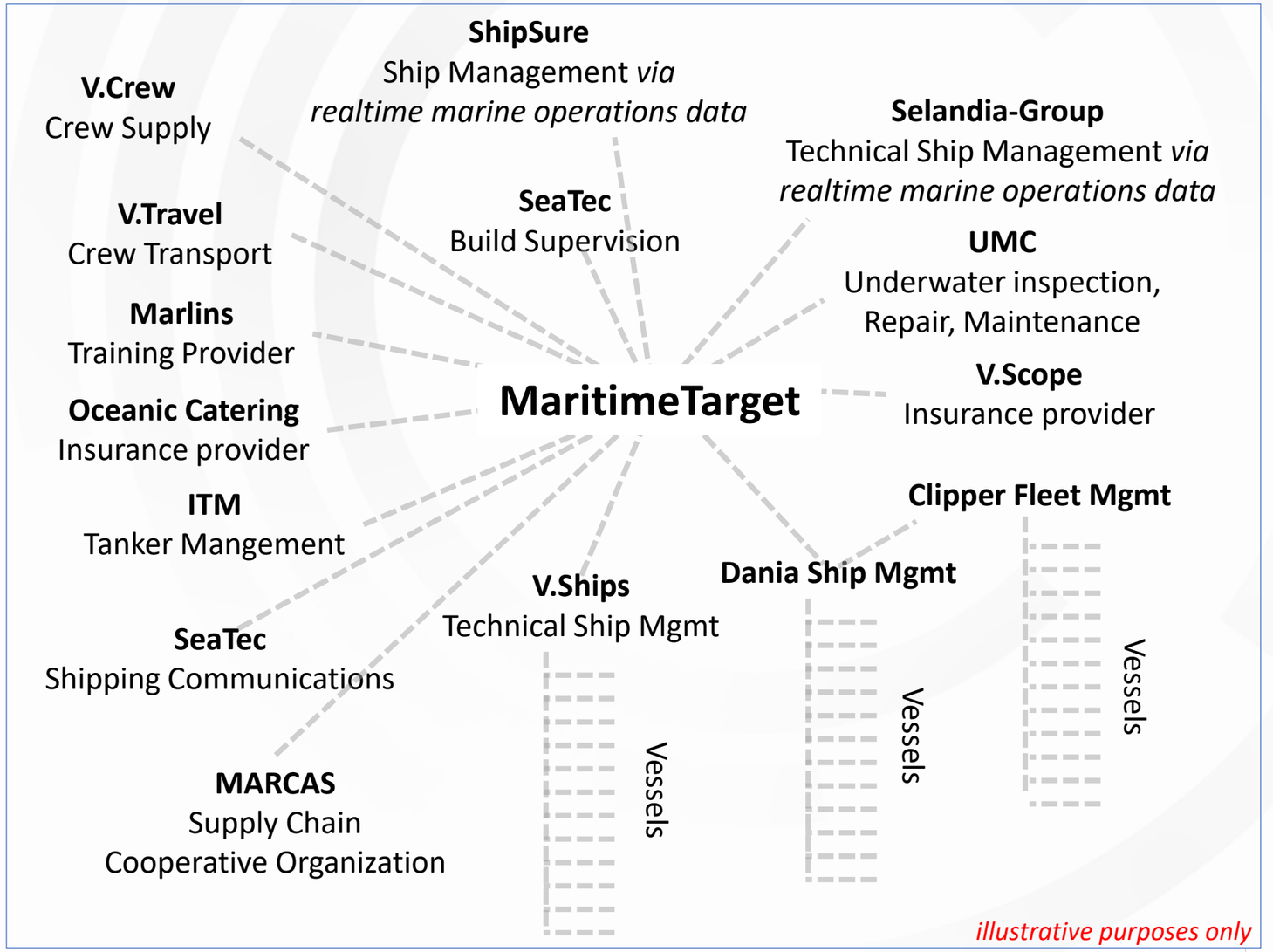
Increased Deep & Dark Web Activity



3. LARGE ATTACK VECTOR SURFACE

Maritime companies have large digital footprint → Many attack vectors





NEEDED ➡ Simplification and Prioritization

- ✧ ALERT OVERLOAD/CVE FATIGUE
- ✧ SHIP OT VULNERABILITIES
- ✧ ATTACK VECTOR OVERLOAD

➡

CyberHelm

- ✧ THREATBETA PRIORITIZATION
- ✧ PROPRIETARY DATABASE OF RELEVANT MARITIME Ots
- ✧ REAL-TIME DASHBOARD w/CONTINUOUS OVERWATCH

CYBERHELM A key component in a multi-layer cyber threat defense

PREDICTIVE:

CyberHelm

PROACTIVE:

Penetration Tests | Secure Gateway | Training & Policies | •••

Firewalls | Air Gaps | Identity/Access Mgmt. | Patch Management | VPN

DETECTIVE:

Anti virus | Anti spam | Database Monitoring | Anti Malware | •••

REACTIVE:

Escalation Management | Digital Forensics | DLP | CIRT | Cyber Insurance






1. AVOIDING ALERT FATIGUE ➡ Threatβeta identifies the most urgent threats

“Threat Beta Predicts Future Cyber Events 1 to 12 months in advance”

NORTHWESTERN UNIVERSITY

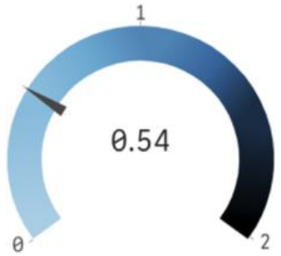
Kellogg School of Management

Threatβeta™

How severe is my overall cyber attack vulnerability relative to others?

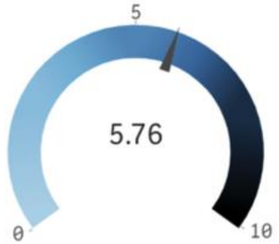
Threat Surface

How big a target am I on the internet?



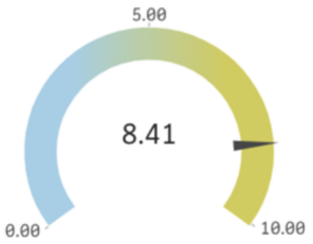
Vulnerability Score

What is the severity of the detected vulnerabilities?

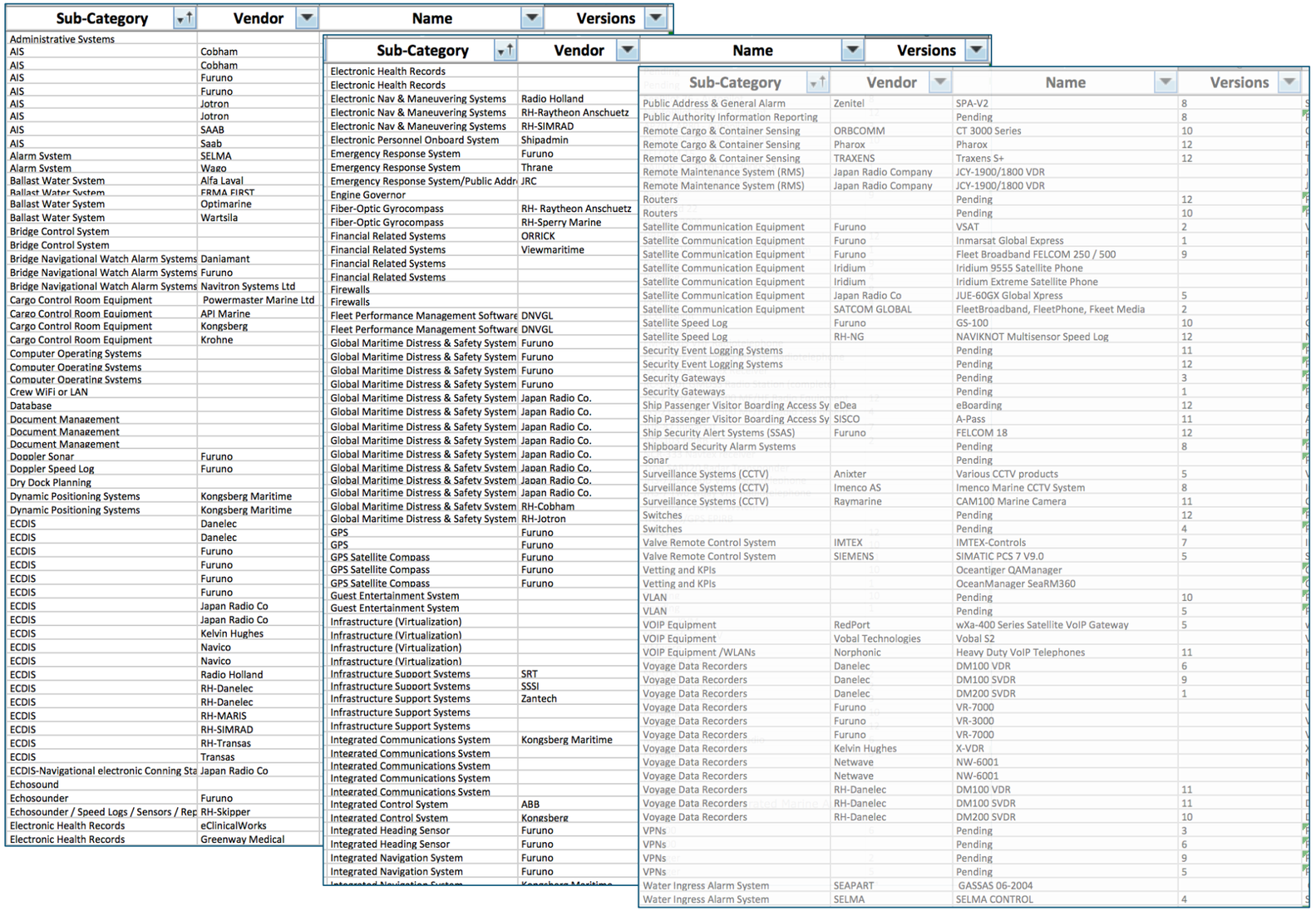


Attack Likelihood

What is the likelihood of me being attacked or probed?



2. SHIP OPERATING TECHNOLOGIES ➡ Proprietary database of 100's of OTs - monitored for Deep & Dark Web Activity



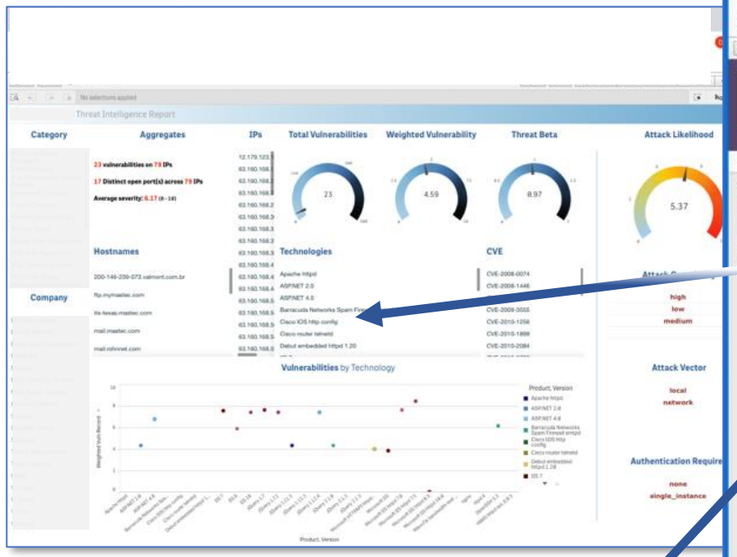
Sub-Category	Vendor	Name	Versions
Administrative Systems			
AIS	Cobham		
AIS	Cobham		
AIS	Furuno		
AIS	Furuno		
AIS	Jotron		
AIS	Jotron		
AIS	SAAB		
AIS	Saab		
Alarm System	SELMA		
Alarm System	Wago		
Ballast Water System	Alfa Laval		
Ballast Water System	ERMA FIRST		
Ballast Water System	Optimarine		
Ballast Water System	Wartsila		
Bridge Control System			
Bridge Control System			
Bridge Navigational Watch Alarm Systems	Daniamant		
Bridge Navigational Watch Alarm Systems	Furuno		
Bridge Navigational Watch Alarm Systems	Navitron Systems Ltd		
Cargo Control Room Equipment	Powermaster Marine Ltd		
Cargo Control Room Equipment	API Marine		
Cargo Control Room Equipment	Kongsberg		
Cargo Control Room Equipment	Krohne		
Computer Operating Systems			
Computer Operating Systems			
Computer Operating Systems			
Crew WiFi or LAN			
Database			
Document Management			
Document Management			
Document Management			
Doppler Sonar	Furuno		
Doppler Speed Log	Furuno		
Dry Dock Planning			
Dynamic Positioning Systems	Kongsberg Maritime		
Dynamic Positioning Systems	Kongsberg Maritime		
ECDIS	Danelec		
ECDIS	Danelec		
ECDIS	Furuno		
ECDIS	Furuno		
ECDIS	Furuno		
ECDIS	Furuno		
ECDIS	Japan Radio Co		
ECDIS	Japan Radio Co		
ECDIS	Kelvin Hughes		
ECDIS	Navico		
ECDIS	Navico		
ECDIS	Radio Holland		
ECDIS	RH-Danelec		
ECDIS	RH-Danelec		
ECDIS	RH-MARIS		
ECDIS	RH-SIMRAD		
ECDIS	RH-Transas		
ECDIS	Transas		
ECDIS-Navigational electronic Conning Sta	Japan Radio Co		
Echosound			
Echosounder	Furuno		
Echosounder / Speed Logs / Sensors / Rep	RH-Skipper		
Electronic Health Records	eClinicalWorks		
Electronic Health Records	Greenway Medical		

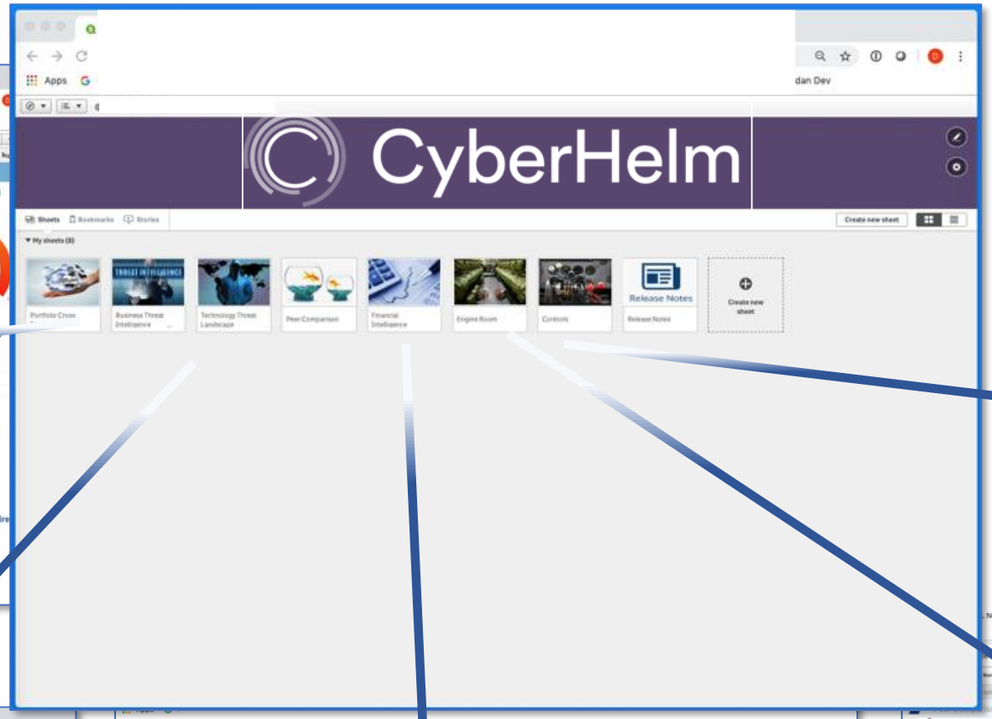
Sub-Category	Vendor	Name	Versions
Electronic Health Records			
Electronic Health Records			
Electronic Nav & Maneuvering Systems	Radio Holland		
Electronic Nav & Maneuvering Systems	RH-Raytheon Anschuetz		
Electronic Nav & Maneuvering Systems	RH-SIMRAD		
Electronic Personnel Onboard System	Shipadmin		
Emergency Response System	Furuno		
Emergency Response System	Thrane		
Emergency Response System/Public Addr	JRC		
Engine Governor			
Fiber-Optic Gyrocompass	RH- Raytheon Anschuetz		
Fiber-Optic Gyrocompass	RH-Sperry Marine		
Financial Related Systems	ORRICK		
Financial Related Systems	Viewmaritime		
Financial Related Systems			
Financial Related Systems			
Firewalls			
Firewalls			
Fleet Performance Management Software	DNVGL		
Fleet Performance Management Software	DNVGL		
Global Maritime Distress & Safety System	Furuno		
Global Maritime Distress & Safety System	Furuno		
Global Maritime Distress & Safety System	Furuno		
Global Maritime Distress & Safety System	Furuno		
Global Maritime Distress & Safety System	Japan Radio Co.		
Global Maritime Distress & Safety System	Japan Radio Co.		
Global Maritime Distress & Safety System	Japan Radio Co.		
Global Maritime Distress & Safety System	Japan Radio Co.		
Global Maritime Distress & Safety System	Japan Radio Co.		
Global Maritime Distress & Safety System	Japan Radio Co.		
Global Maritime Distress & Safety System	Japan Radio Co.		
Global Maritime Distress & Safety System	Japan Radio Co.		
Global Maritime Distress & Safety System	RH-Cobham		
Global Maritime Distress & Safety System	RH-Jotron		
GPS	Furuno		
GPS	Furuno		
GPS Satellite Compass	Furuno		
GPS Satellite Compass	Furuno		
GPS Satellite Compass	Furuno		
Guest Entertainment System			
Guest Entertainment System			
Infrastructure (Virtualization)			
Infrastructure (Virtualization)			
Infrastructure (Virtualization)			
Infrastructure (Virtualization)			
Infrastructure Support Systems	SRT		
Infrastructure Support Systems	SSSI		
Infrastructure Support Systems	Zantech		
Infrastructure Support Systems			
Infrastructure Support Systems			
Integrated Communications System	Kongsberg Maritime		
Integrated Communications System			
Integrated Communications System			
Integrated Communications System			
Integrated Communications System			
Integrated Control System	ABB		
Integrated Control System	Kongsberg		
Integrated Heading Sensor	Furuno		
Integrated Heading Sensor	Furuno		
Integrated Navigation System	Furuno		
Integrated Navigation System	Furuno		

Sub-Category	Vendor	Name	Versions
Public Address & General Alarm	Zenitel	SPA-V2	8
Public Authority Information Reporting		Pending	8
Remote Cargo & Container Sensing	ORBCOMM	CT 3000 Series	10
Remote Cargo & Container Sensing	Pharox	Pharox	12
Remote Cargo & Container Sensing	TRAXENS	Traxens S+	12
Remote Maintenance System (RMS)	Japan Radio Company	JCY-1900/1800 VDR	
Remote Maintenance System (RMS)	Japan Radio Company	JCY-1900/1800 VDR	
Routers		Pending	12
Routers		Pending	10
Satellite Communication Equipment	Furuno	VSAT	2
Satellite Communication Equipment	Furuno	Inmarsat Global Express	1
Satellite Communication Equipment	Furuno	Fleet Broadband FELCOM 250 / 500	9
Satellite Communication Equipment	Iridium	Iridium 9555 Satellite Phone	
Satellite Communication Equipment	Iridium	Iridium Extreme Satellite Phone	
Satellite Communication Equipment	Japan Radio Co	JUE-60GX Global Xpress	5
Satellite Communication Equipment	SATCOM GLOBAL	FleetBroadband, FleetPhone, Fkeet Media	2
Satellite Speed Log	Furuno	GS-100	10
Satellite Speed Log	RH-NG	NAVIKNOT Multisensor Speed Log	12
Security Event Logging Systems		Pending	11
Security Event Logging Systems		Pending	12
Security Gateways		Pending	3
Security Gateways		Pending	1
Ship Passenger Visitor Boarding Access Sy	eDea	eBoarding	12
Ship Passenger Visitor Boarding Access Sy	SISCO	A-Pass	11
Ship Security Alert Systems (SSAS)	Furuno	FELCOM 18	12
Shipboard Security Alarm Systems		Pending	8
Sonar		Pending	
Surveillance Systems (CCTV)	Anixter	Various CCTV products	5
Surveillance Systems (CCTV)	Imenco AS	Imenco Marine CCTV System	8
Surveillance Systems (CCTV)	Raymarine	CAM100 Marine Camera	11
Switches		Pending	12
Switches		Pending	4
Valve Remote Control System	IMTEX	IMTEX-Controls	7
Valve Remote Control System	SIEMENS	SIMATIC PCS 7 V9.0	5
Vetting and KPIs		Oceantiger QAManager	
Vetting and KPIs		OceanManager SeaRM360	
VLAN		Pending	10
VLAN		Pending	5
VOIP Equipment	RedPort	wXa-400 Series Satellite VoIP Gateway	5
VOIP Equipment	Vobal Technologies	Vobal S2	
VOIP Equipment /WLANs	Norphonic	Heavy Duty VoIP Telephones	11
Voyage Data Recorders	Danelec	DM100 VDR	6
Voyage Data Recorders	Danelec	DM100 SVDR	9
Voyage Data Recorders	Danelec	DM200 SVDR	1
Voyage Data Recorders	Furuno	VR-7000	
Voyage Data Recorders	Furuno	VR-3000	
Voyage Data Recorders	Furuno	VR-7000	
Voyage Data Recorders	Kelvin Hughes	X-VDR	
Voyage Data Recorders	Netwave	NW-6001	
Voyage Data Recorders	Netwave	NW-6001	
Voyage Data Recorders	RH-Danelec	DM100 VDR	11
Voyage Data Recorders	RH-Danelec	DM100 SVDR	11
Voyage Data Recorders	RH-Danelec	DM200 SVDR	10
VPNs		Pending	3
VPNs		Pending	6
VPNs		Pending	9
VPNs		Pending	5
Water Ingress Alarm System	SEAPART	GASSAS 06-2004	
Water Ingress Alarm System	SELMA	SELMA CONTROL	4

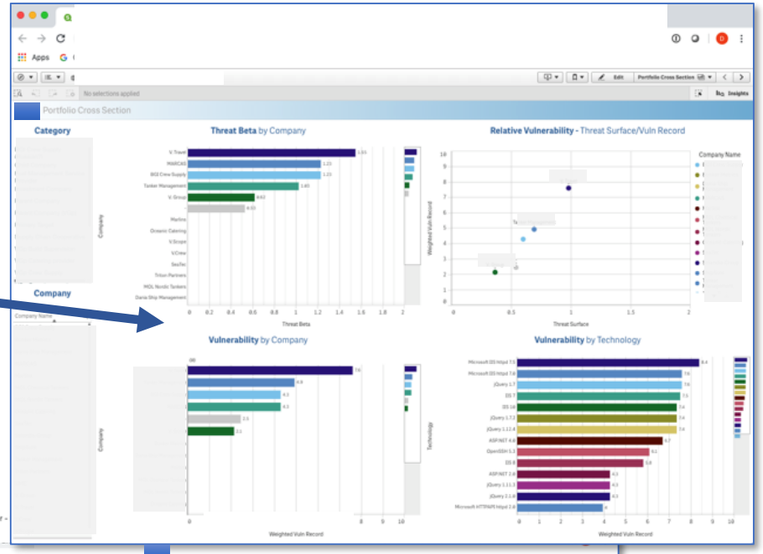
3. VECTOR OVERLOAD ➡ Dashboard for Remediation & Compliance Mngmt

Enterprise Summary Metrics

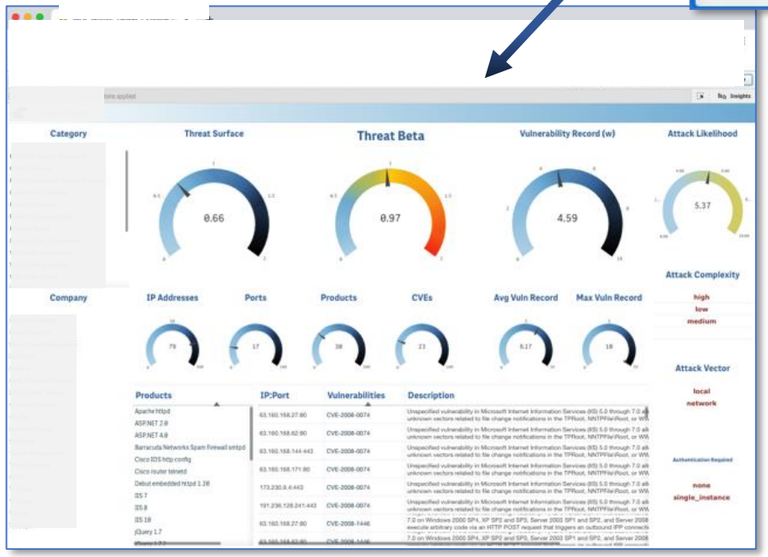


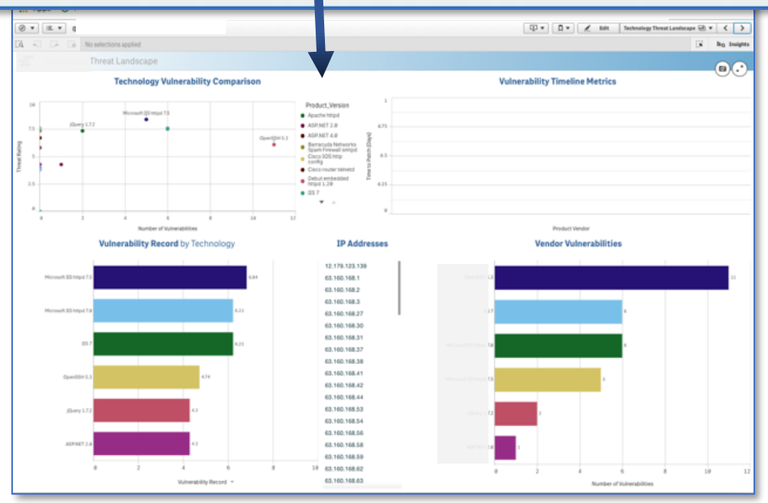


What-if Scenarios

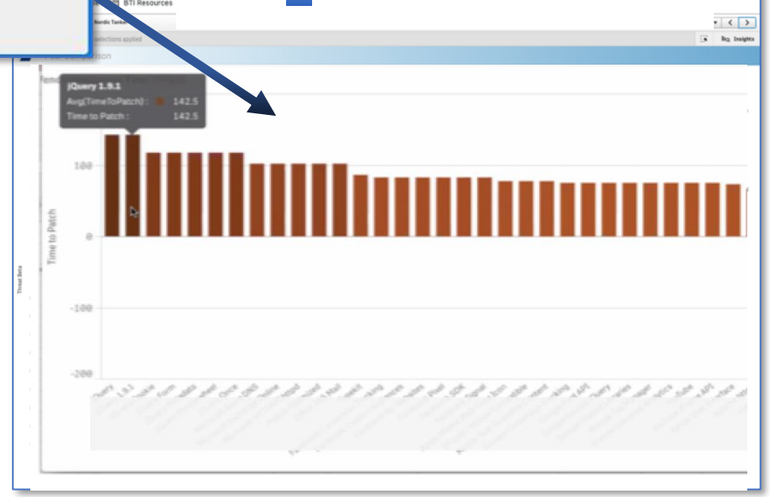


Drill-down by entity (vessel)





Technology Details



Time to Patch Monitoring

Dashboard drill-down

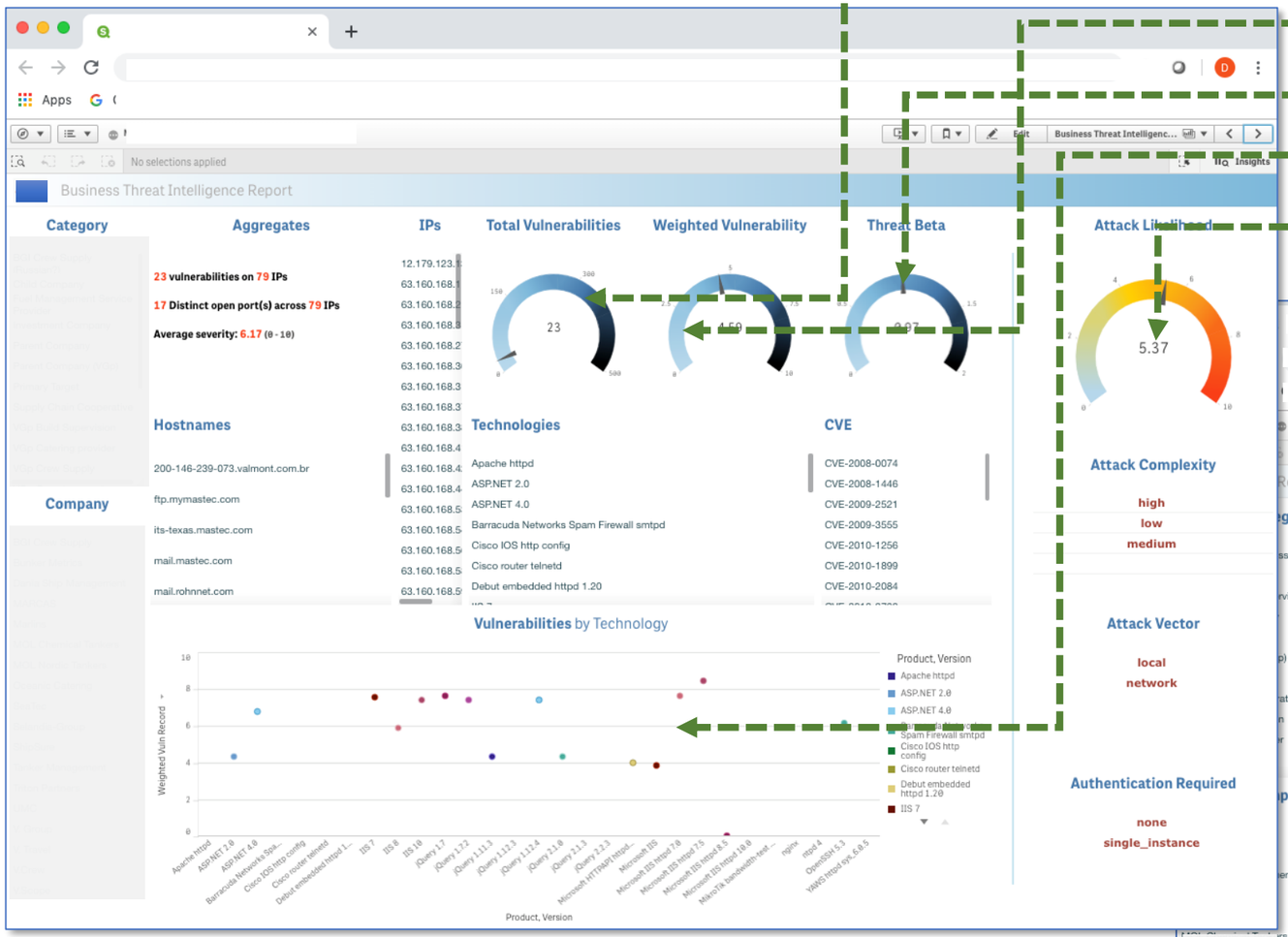
How many security holes are in my enterprise?

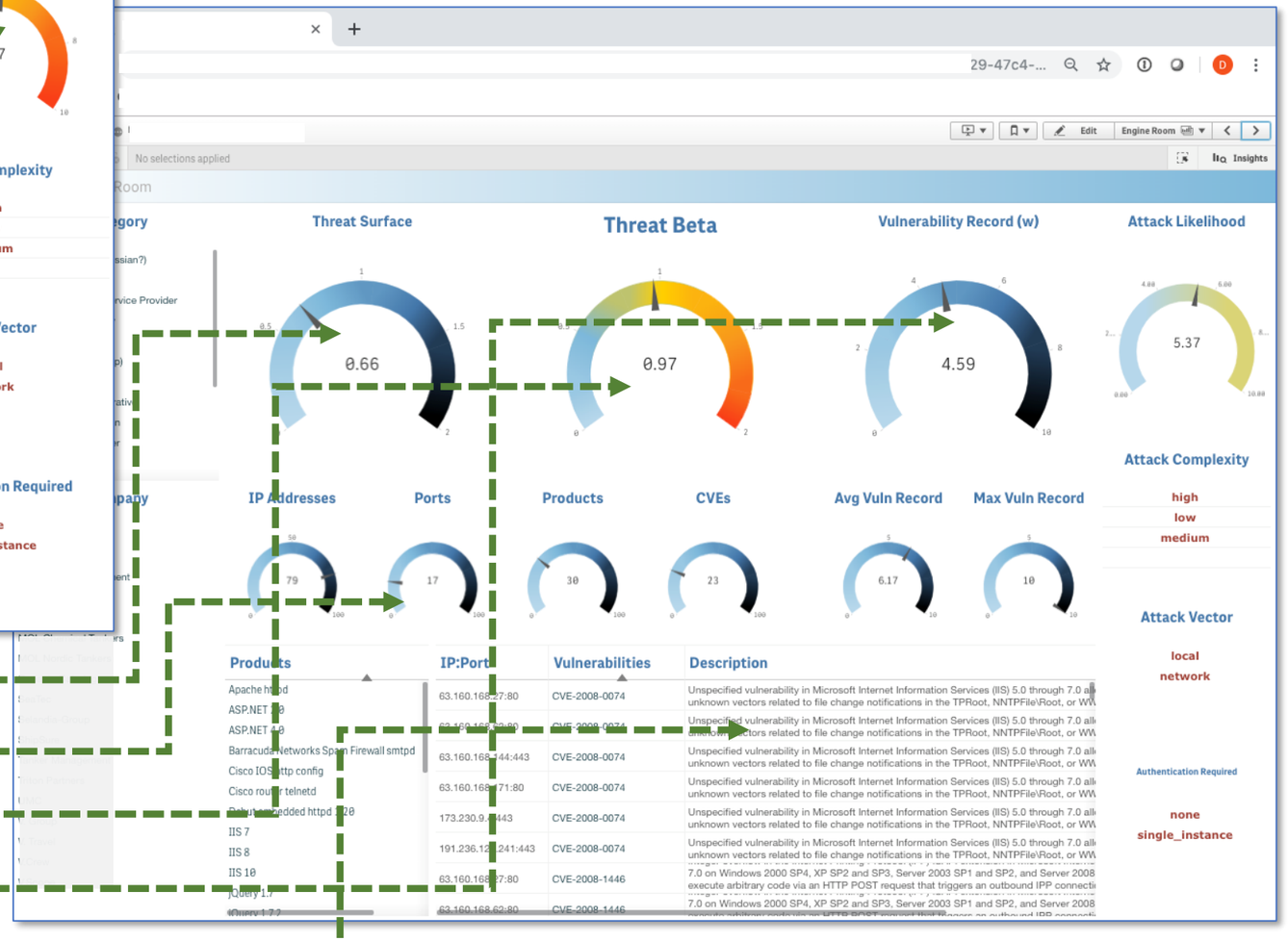
What is their certified ***severity***?

What is my ***quantified, relative vulnerability***?

Which technologies are leaving me at-risk?

What is the ***likelihood of being attacked*** or probed





How **big a target** am I on the Internet?

Which **IP addresses are my weakest** technologies on?

What is my **quantified, relative vulnerability**?

How **severe** are my vulnerabilities?

How do we fix the problems?

For more information please contact:

fredrik.munck@cybeta.com