



Digital Ship Athens Spring Conference 2022

Cybersecurity in maritime is like swimming with the Cthulhu

Chara Vassiliadou
chvassiliadou@census-labs.com)

www.census-labs.com





Digital Ship Athens Spring Conference 2022

Cybersecurity in maritime is like swimming with the Cthulhu

Chara Vassiliadou
chvassiliadou@census-labs.com

www.census-labs.com

Agenda

- ◆ CENSUS at a glance
- ◆ What is Cthulhu
- ◆ The sea
- ◆ The monsters
- ◆ Swimming with monsters



Digital Ship Athens 2022

Cybersecurity in maritime is like swimming with the Cthulhu

CENSUS at a glance

- ◆ **CENSUS** is an **internationally acclaimed** Cybersecurity services provider, supporting the needs of **multiple industries**.
- ◆ We are offering state-of-the-art services to organizations **worldwide** to cover the complex needs of today's **IT & OT ecosystems**:
 - ◆ Organisation Security
 - ◆ Product Security Assessments
 - ◆ Secure Systems Development Lifecycle
 - ◆ Vulnerability Research
 - ◆ Information Security Consulting
- ◆ Services built upon the **company's leading research** to provide high quality InfoSec services.
- ◆ We are very proud of our **ethos**, as we care about **quality (in) systems**.

70

Security engineers

12+

Years of innovation

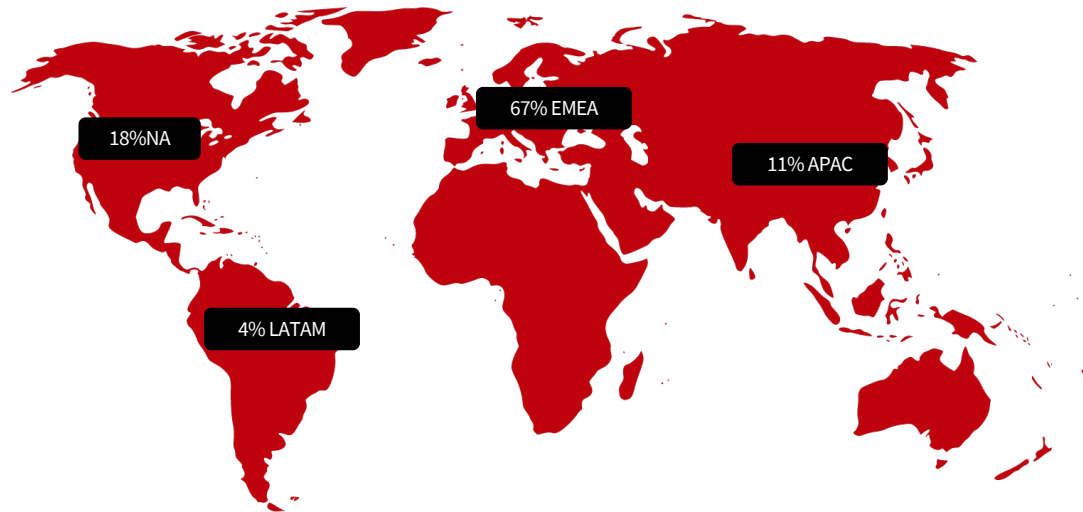
Company certified for quality and security management systems



CENSUS at a glance

Global Presence

We help clients with their **cybersecurity maturity journey** by providing **end to end** state of the art **assessment of their security posture** to improve their **cyber resilience** and leverage the benefits of **digital transformation**.













19+

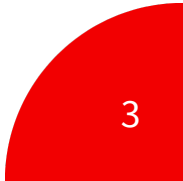
Countries

~400

Clients
80+ Fortune 500

In multiple market sectors

-  Aerospace & Defence
-  Government
-  Healthcare
-  Maritime
-  Transportation
-  Banking, Finance & Insurance
-  Industrial & Internet of Things
-  Energy & Utilities
-  Software Companies
-  Application Developers



CENSUS at a glance

Why we are different



Research

Working with our global partner network, we deliver the best, most proven services to de-risk technology investments.



World-class talent

We regularly present our research to major IT security conferences including Black Hat, OWASP AppSec, DEFCON and ZeroNights.



Innovation

We've helped shape the Secure SDLC methodology followed by international software vendors. We've contributed code to major software projects such as Linux, FreeBSD and the Metasploit Framework.

Proud members of



Ladies and gentlemen, the Cthulhu

Cthulhu is a fictional cosmic entity created by writer H. P. Lovecraft.

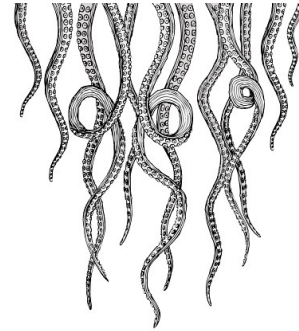
The short story that first mentions Cthulhu, "The Call of Cthulhu" established the character as a malevolent entity, hibernating within R'lyeh, an underwater city in the South Pacific. The imprisoned Cthulhu is apparently the source of constant subconscious anxiety for all mankind. / source: Wikipedia /



And what 's Cthulhu got to do, got to do with the Maritime?

...the source of
constant
subconscious
anxiety for all
maritime.





The sea



A whole new world

New technologies, New products, New markets, Pandemic, Automation and AI



Legal and regulatory frameworks

Legal and regulatory framework including from IT procedures and policies to insurance coverage



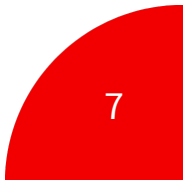
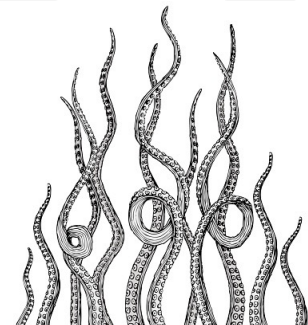
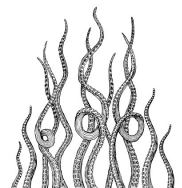
OT and IT security

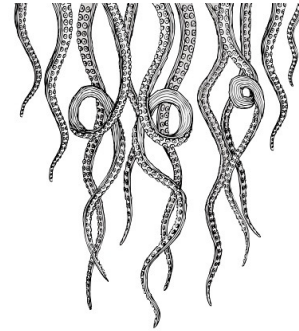
They are getting more and more connected but still a black box



Supply Chain

They are getting more and more connected but still a black box





Zooming in on A whole new world

New technologies

Physical Security

People

New products

Remote Administration

Sustainability

Pandemic

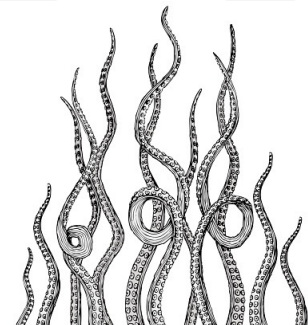
A really wide Network

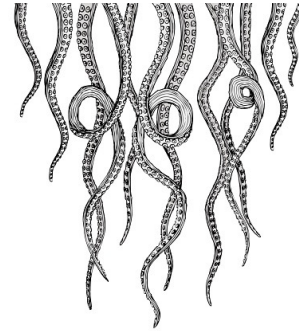
API based platforms

AI and Autonomous

Communications

Privacy Renaissance





Zooming in on The Legal and regulatory and other frameworks

IMO

BIMCO / Guidelines on Cyber Security on board Ships – fourth version' (BIMCO et al., 2021).2

NIST

Various multilateral agreements (WTO TFA and the IMO FAL Convention)

Maritime Single Windows

ISM CODE and ISPS Code

MASS

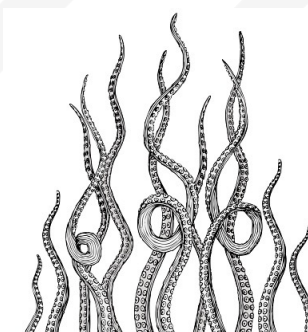
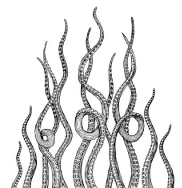
National Trade Facilitation Committees

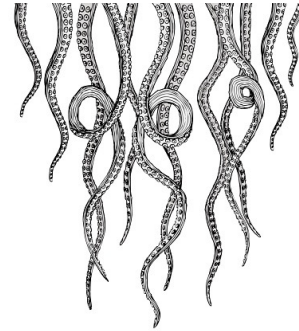
Digital Container Shipping Association's Implementation Guide for Cyber Security on Vessels v1.0

Reducing GHG emissions

International Association for Classification Societies (IACS)

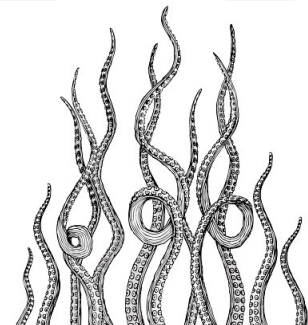
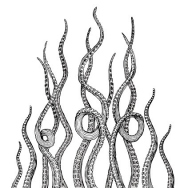
...and the list goes on

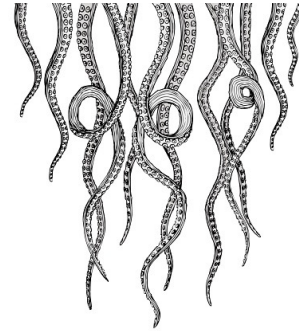




Zooming in on OT and IT Security

	IT	OT
Purpose	Highly flexible, designed to run any application	Designed for purpose, deterministic logic for monitoring and control
Security / Availability	Security is high priority / Security Critical	Availability is highest priority / Safety Critical
Lifecycle refresh (Avg)	3-5 years	20+ years
Architecture	Homogenous – standard hardware and software across the enterprise	Highly heterogenous – a hodgepodge of hardware and operating systems from multitude of vendors
Openness	Open systems with published APIs, large pool of expert resources	Closed and proprietary systems, scarce resources





Zooming in on Supply Chain

Data Protection

Third party risk

Data Locality

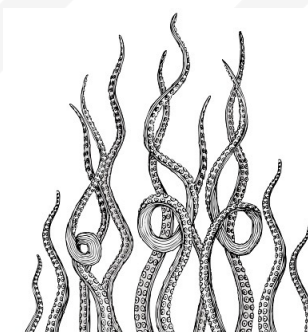
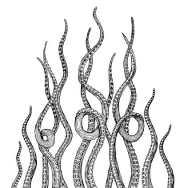
Security is high priority / Security Critical

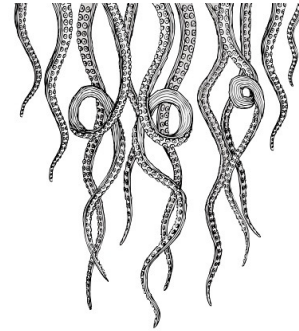
Data visibility

Data Governance

Fraud prevention

...and this list also goes on





The Monsters

Data transfer from the company to the vessel / gaining access from the HQ

Non- specialized personnel on-board

SODANE enumerating all IoT and SCADA devices

Impersonating port authority

Take over a remote management tool on a vessel

Sensitive equipment like sensors

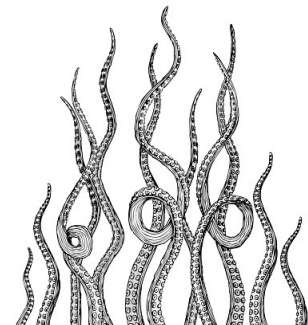
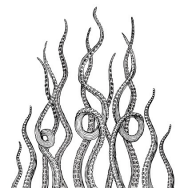
Targeted phishing emails to the vessel's crew

Poor management involvement and commitment on cyber security

Captain is the king of the world. He should be. But he needs training

Lack of information security experts

Malware installation on a vessel



Swimming with the monsters

INFORMATION SECURITY STRATEGY

POLICIES AND PROCEDURES

risk assessment, security policies, review and adjust, talk simple

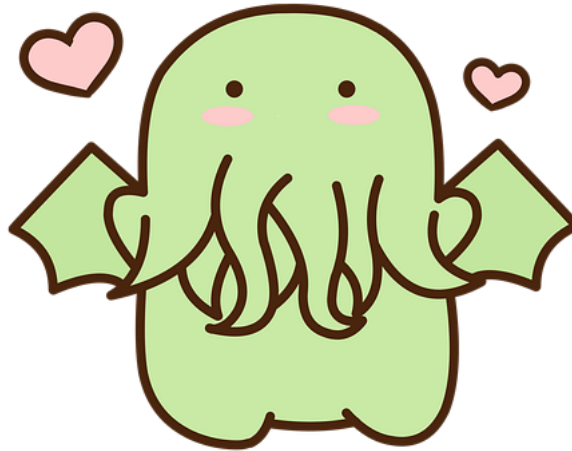
PEOPLE

management involvement/ security awareness / metrics

TECHNOLOGY

identify all the assets (IT and OT), threat modelling, budget, expertise required, test everything

Ladies and gentlemen, the Cthulhu





Thank you!