Don't Give Up The Ship!

Maritime SOC/NOC

Phil Acosta, GuROO

Cliff Neve, MAD Security

MAD Security

GuROO

DEFCON 32
ICS Village,
10 Aug 2024

Cliff's Background

Cliff Neve, CISSP, C|CISO, CISA, PMP

Experience

- 30+ Years in Information Technology/Cybersecurity
- Retired Active Duty CG Commander
- Currently Deputy Director, CG Auxiliary Cybersecurity Directorate
- Adjunct Professor University of New Haven Graduate School of Business

Ships/Maritime

- Coast Guard National Security Cutter ATOs/SCIF/SOC
- MARAD National Security Multi-mission Vessels (ATO/SOC)
- Port terminal risk assessments CONUS/OCONUS (Guam, Alaska, Hawaii, etc.)
- Deck Watch Officer/Navigator of Coast Guard 180' Ship
- Established Coast Guard SOC as CGCYBER Plankowner
- Established MAD Security's Maritime SOC

MADSecurity

MADSecurity
Making A Difference

GuROO

Phil's Background

Philip Acosta, PMP, PgMP

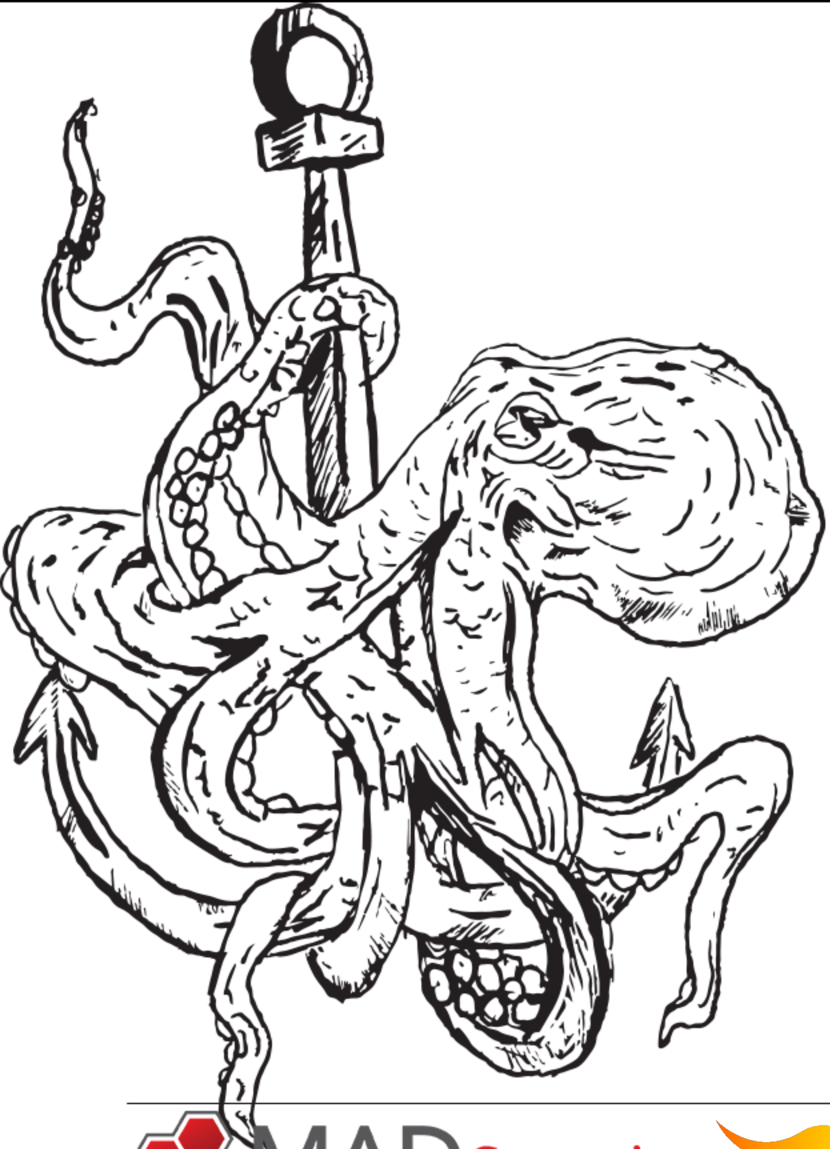
Experience

- Founder / CEO of GuROO LLC
- 20+ years working….
- JMU Alumni
- National Security community comms lead for a prestigious NLCC community group for a decade
- Developed a virtualization platform for building networks

Ships/Maritime

- Let's talk about HOW data transport adds VALUE to the MARITIME INDUSTRY.
- National Security Multi-Mission Vessel (NSMV) – Duel-hatted, multi-mission, multiple users.
- Maritime surface drones – long-dwell, oceanographic monitoring, multi-mission… if connected.
- Commercial IT components layered for peer / near-peer data transport data security.
- Every-"THING" is now a data warehouse and transporting data where it can be optimally utilized.
- Maritime is a TOUGH ENVIRONMENT - Network operations is sometimes at odds with Network security.

GuROO



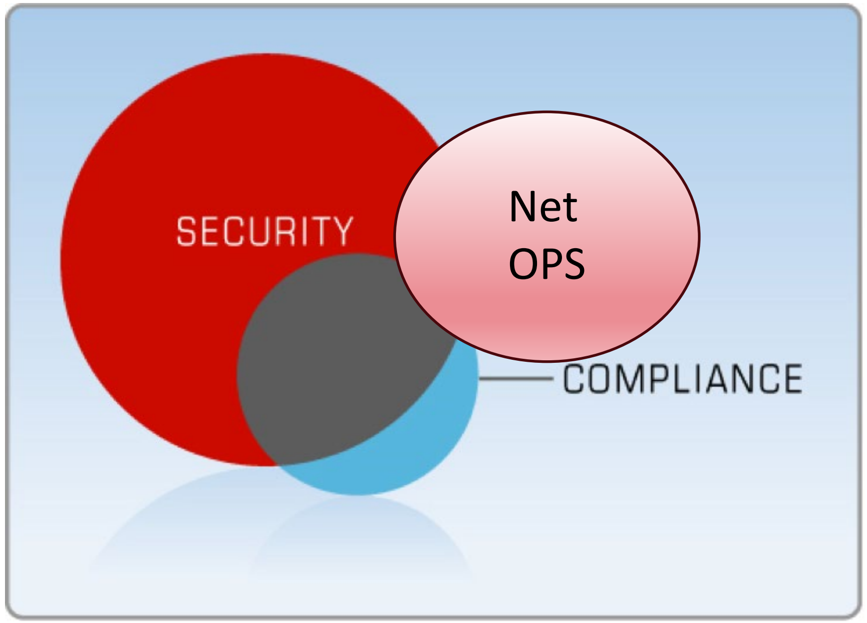
Agenda

- Requirements/Scope
- Considerations
- Communications
- Strategies
- Technology
- Implantation and Lessons Learned

Must Be Secure…and Compliant…and oh by the way, USABLE

Operations delivers data from the source to the users for creating value

- Confidentiality, Integrity, Availability.
- Tools, processes, practices… Innovation!
- Key metrics, performance, modernization.



Compliance meets regulatory requirements, but is not reflective of the current risk landscape:

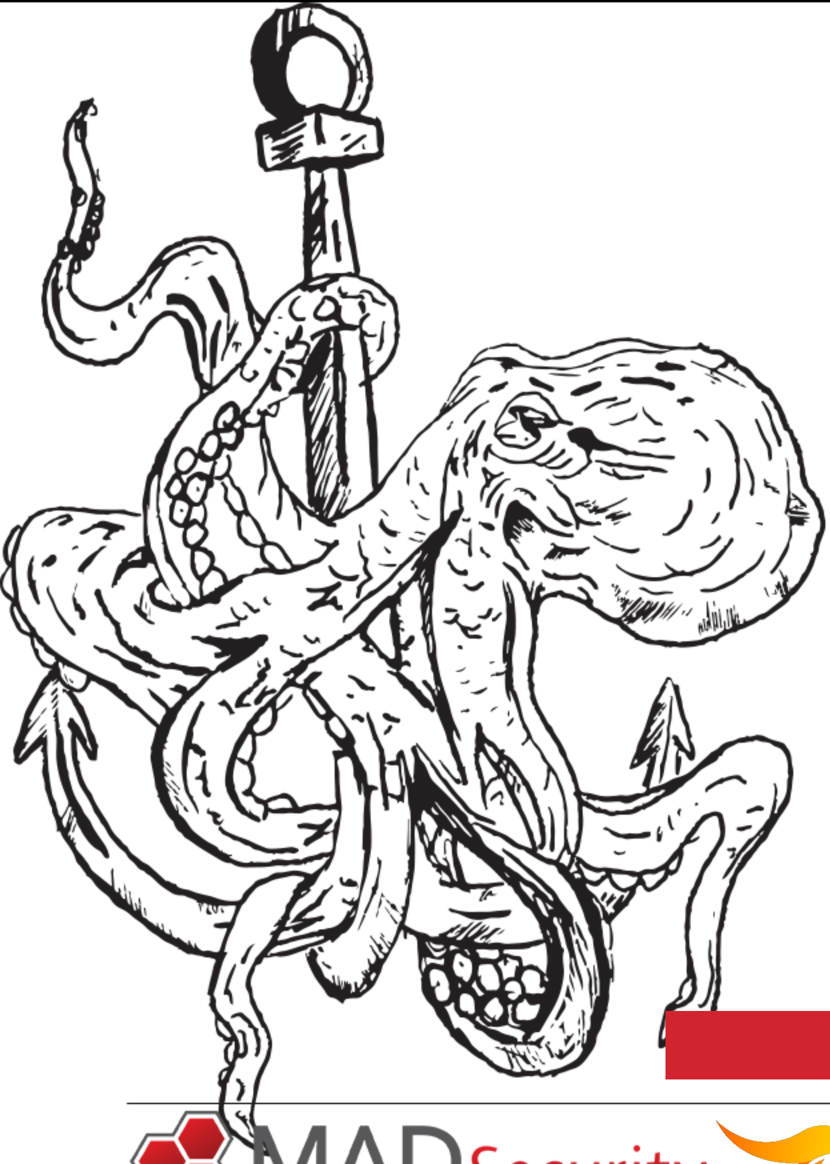
- Written documentation – policies & procedures
- Periodic scans

Security builds the capacity to identify, protect, detect, respond and recover from cyber risks:

- Provides prioritized implementation approach for NIST controls based on measured risk profile
- Manages real world risks, including:
  - Ransomware and malware attacks (e.g. NotPetya, SamSam, etc.)
  - Social engineering attacks (e.g. accounts payable, wire transfers, etc.)

Compliance satisfies an audit and is a cost center, while security meets strategic/Board of Directors requirements.

The Challenge



- Scope. Scope. Scope. Lots of systems.
- User requirements. Always a challenge.
- Must understand all compliance requirements.
    - ATO/NIST? IACS? Coast Guard? IMO?
- Must ALSO understand communications nodes and RACI

Can’t just start deploying technologies!

Business Impacts & What Needs Protecting

Service Level Agreements

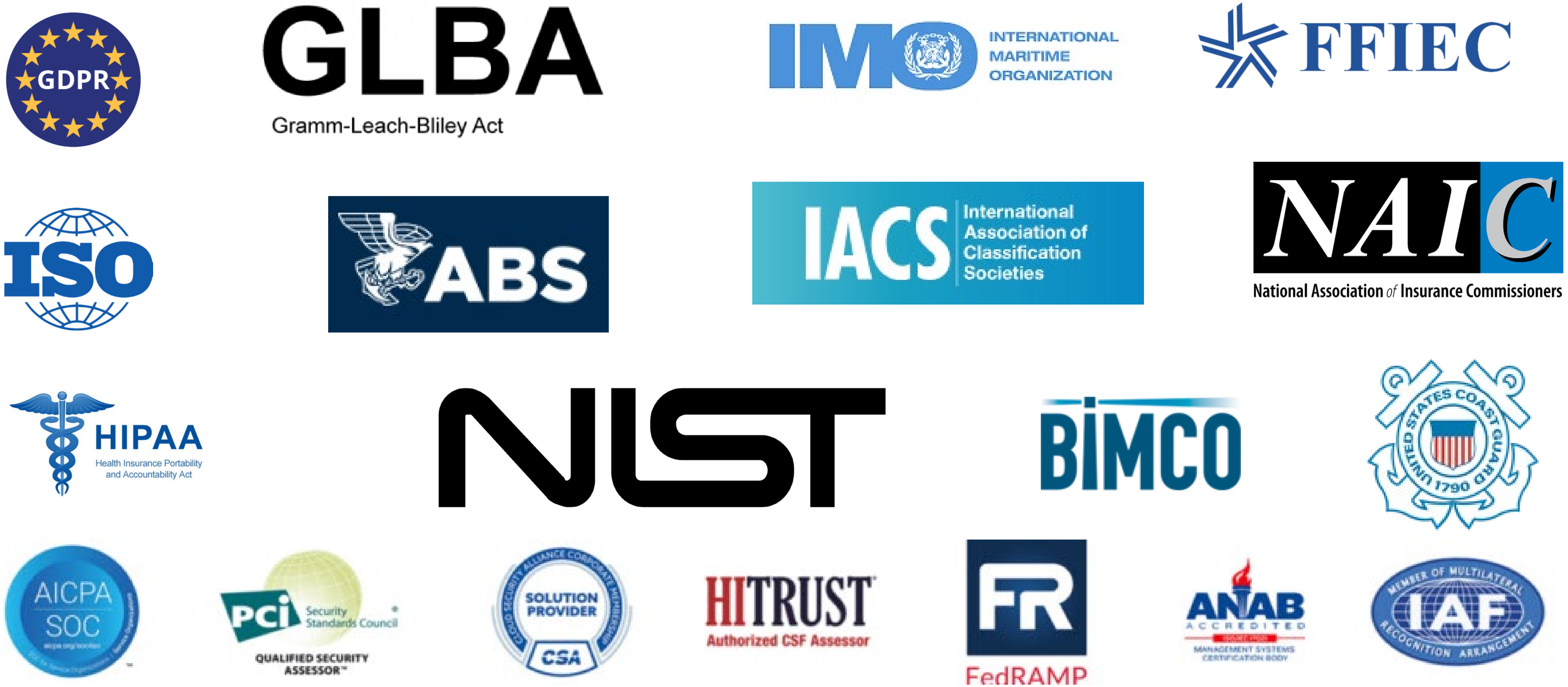
What systems have uptime requirements and what are those requirements?

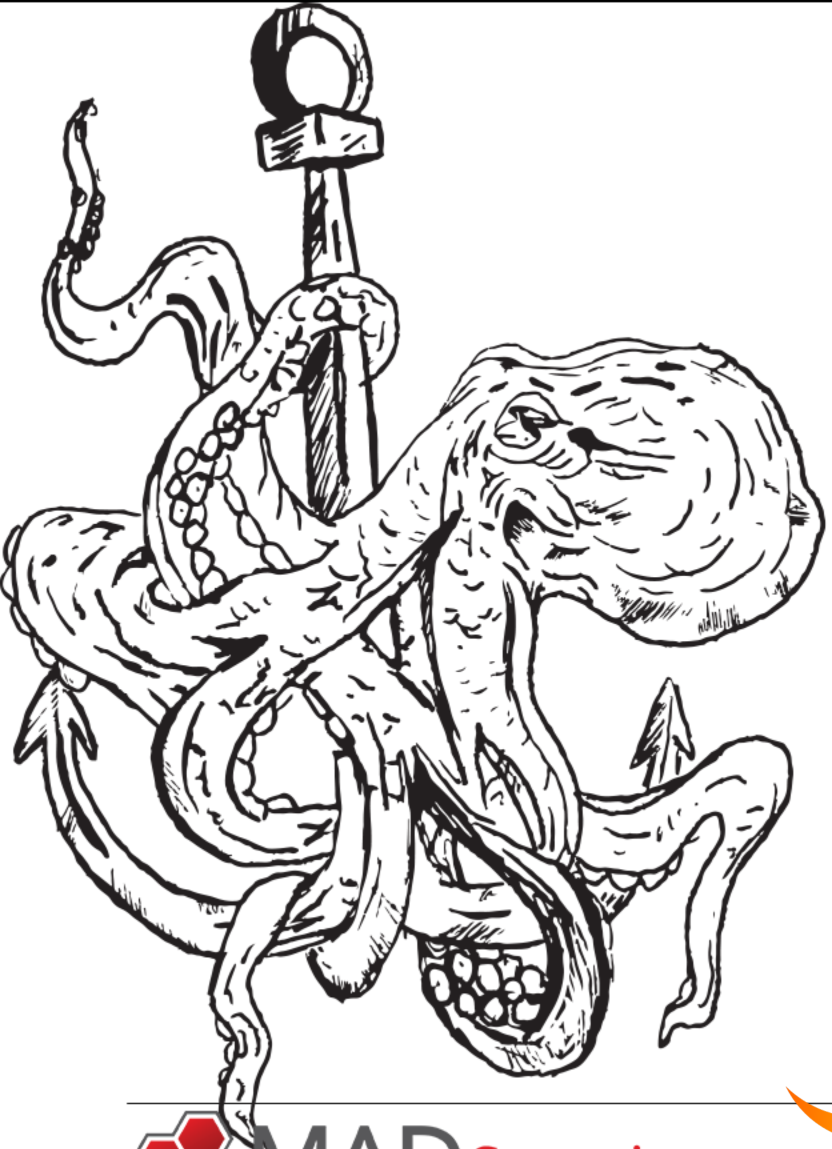
- Operational technologies requiring ~100% uptime?
- Video systems?
- Call centers?
- Weapons systems?
- Law enforcement/emergency systems?

Importance of Confidentiality/Integrity/Availability

- Where is the emphasis for each IT/ICS system?
- For HR systems: confidentiality may be most important
- For Industrial Control Systems, availability generally trumps confidentiality

“The great thing about standards is there are so many to choose from.”—Andrew Tannenbaum

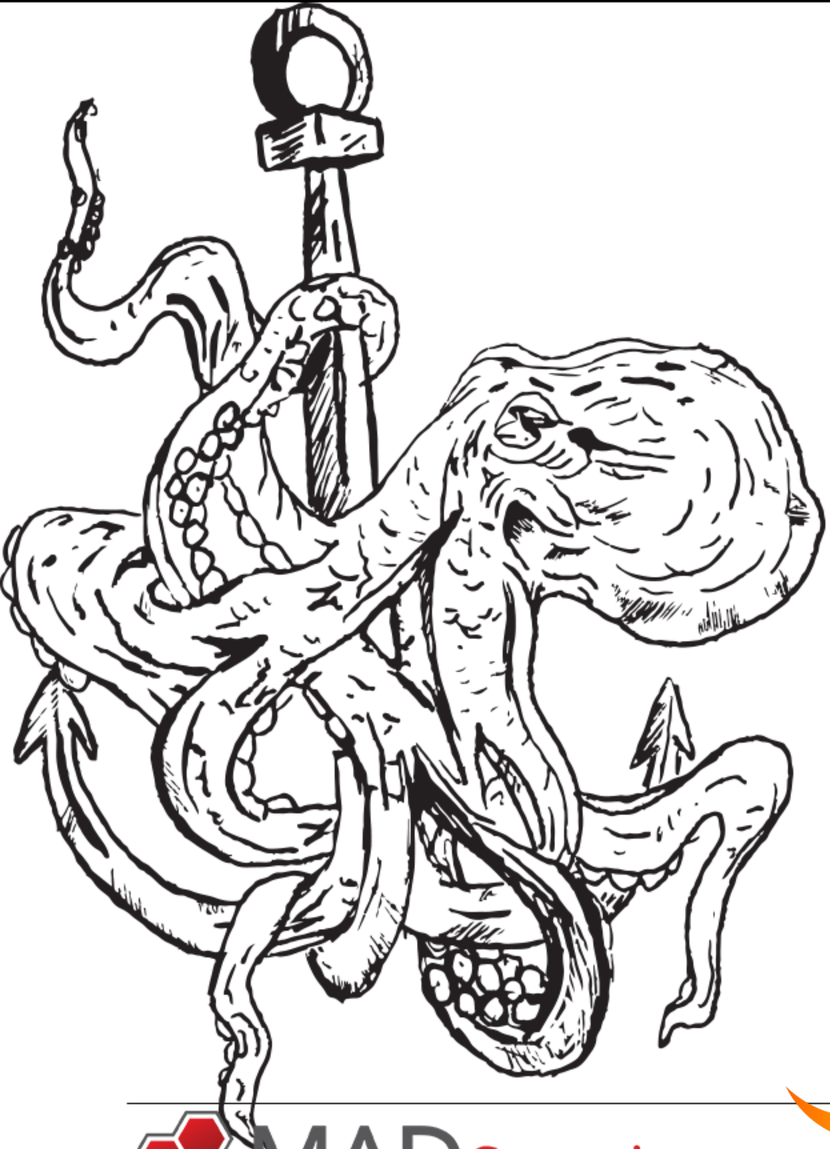

GDPR
GLBA
Gramm-Leach-Bliley Act
IMO
INTERNATIONAL MARITIME ORGANIZATION
FFIEC
ISO
ABS
IACS
International Association of Classification Societies
NAIC
National Association of Insurance Commissioners
HIPAA
Health Insurance Portability and Accountability Act
NIST
BIMCO
UNITED STATES COAST GUARD 1790
AICPA SOC
pci Security Standards Council
QUALIFIED SECURITY ASSESSOR™
SOLUTION PROVIDER
CLOUD SECURITY ALLIANCE CORPORATE MEMBERSHIP
CSA
HITRUST
Authorized CSF Assessor
FR
FedRAMP
ANAB
ACCREDITED
MANAGEMENT SYSTEMS CERTIFICATION BODY
IAF
MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT

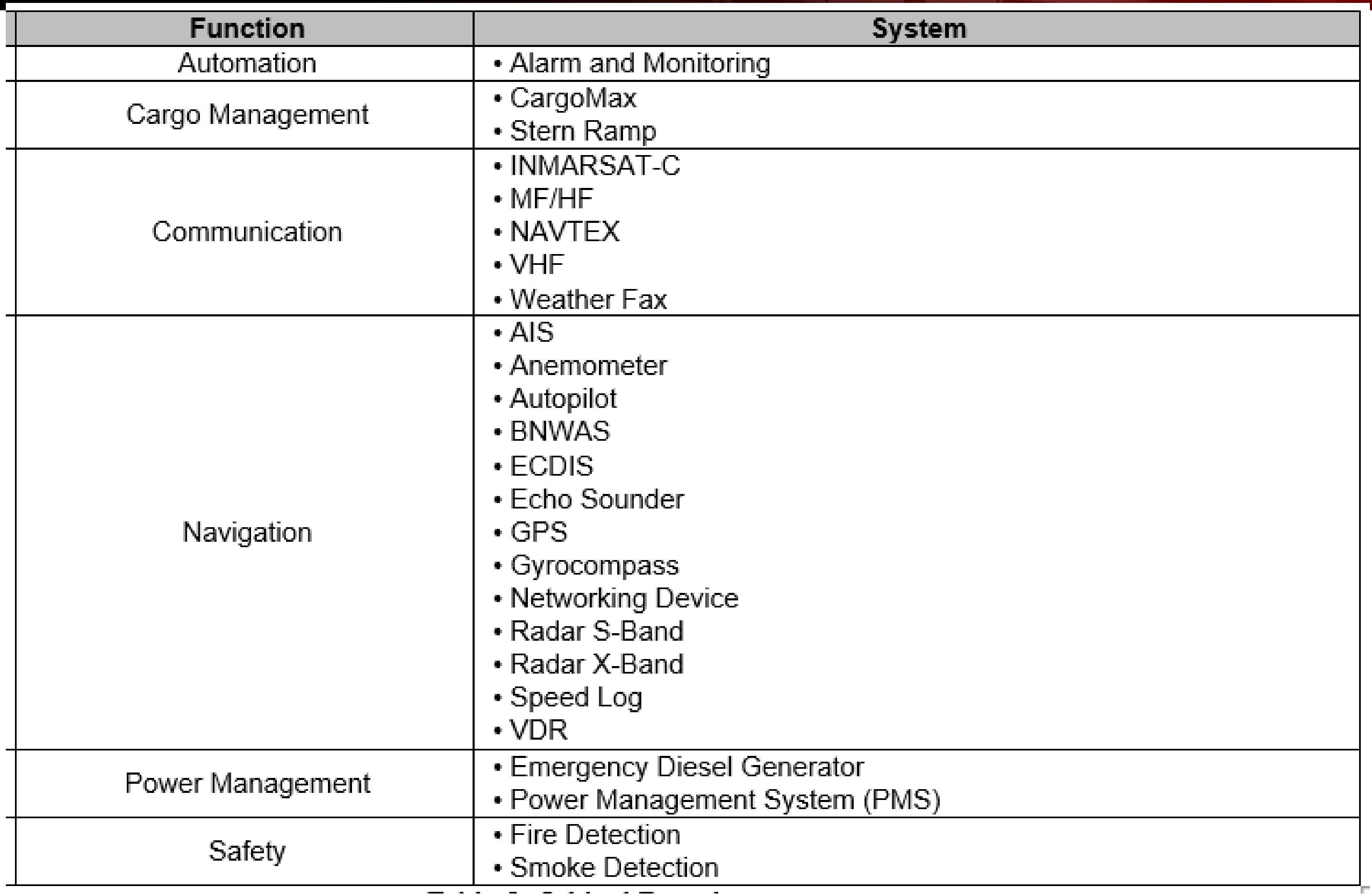


Shipboard Environment

- Power Outages
- Heat/HVAC
- Testing challenges
- Rotating crew
- Curious sailors

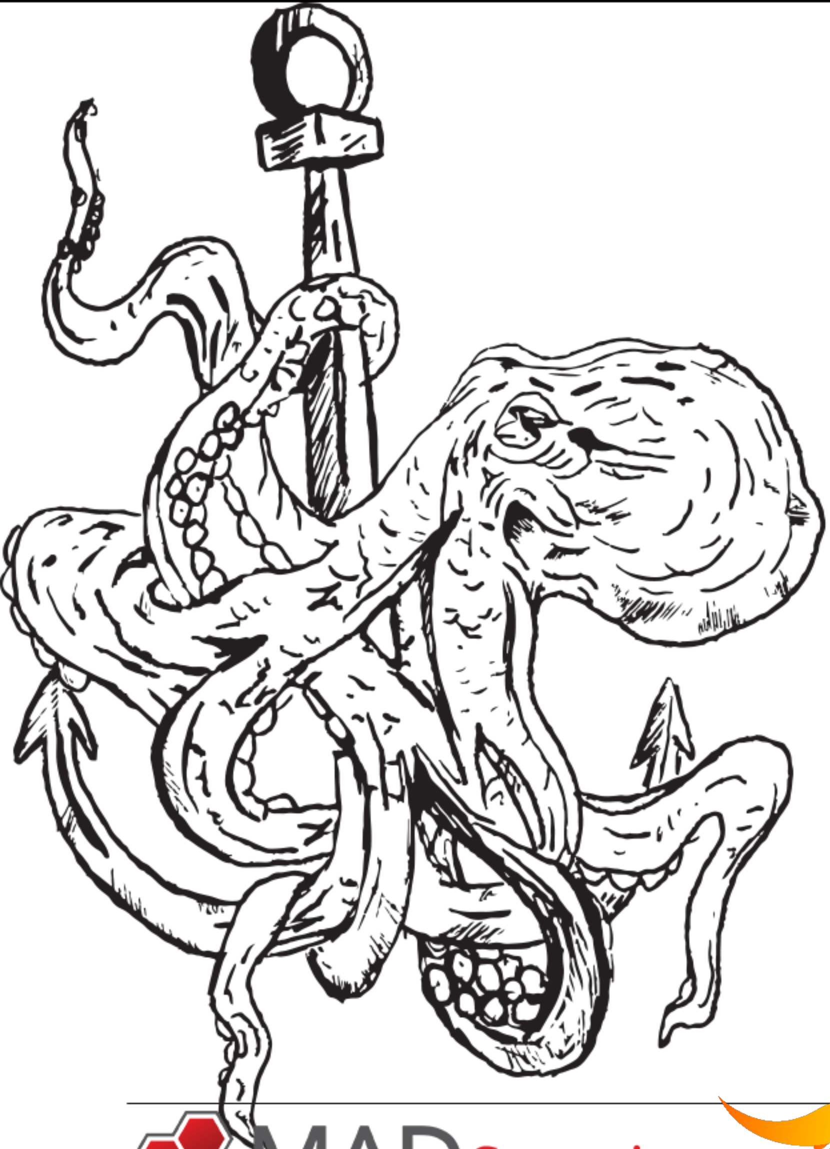
KNOW YOUR SHIP





Function	System
Automation	• Alarm and Monitoring
Cargo Management	• CargoMax • Stern Ramp
Communication	• INMARSAT-C • MF/HF • NAVTEX • VHF • Weather Fax
Navigation	• AIS • Anemometer • Autopilot • BNWAS • ECDIS • Echo Sounder • GPS • Gyrocompass • Networking Device • Radar S-Band • Radar X-Band • Speed Log • VDR
Power Management	• Emergency Diesel Generator • Power Management System (PMS)
Safety	• Fire Detection • Smoke Detection

Inventory (Master Equipment List)



Cluster 0:

Not externally serviceable

Cluster 1:

Serviceable only via USB/other portable media

Cluster 2:

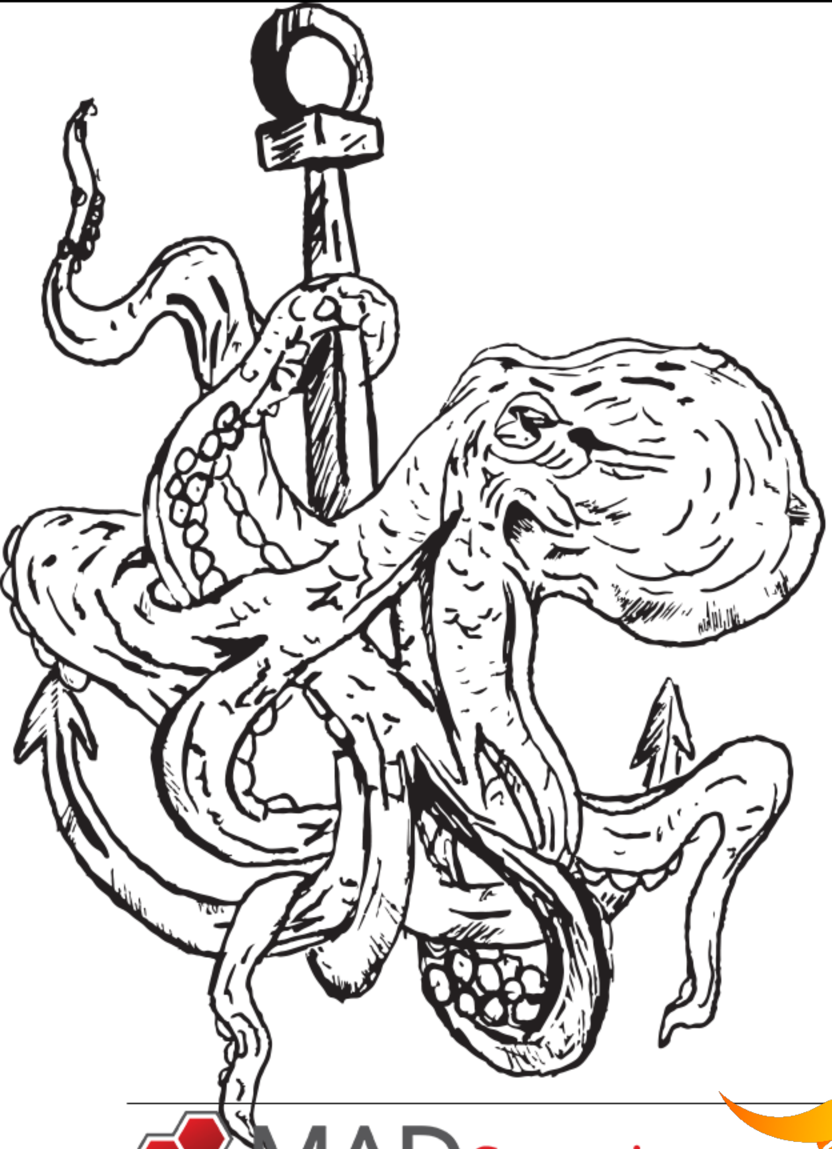
LAN Capable – Not configured

Cluster 3:

Own/self-contained LAN

Cluster 4:

Connectivity with LAN/WAN

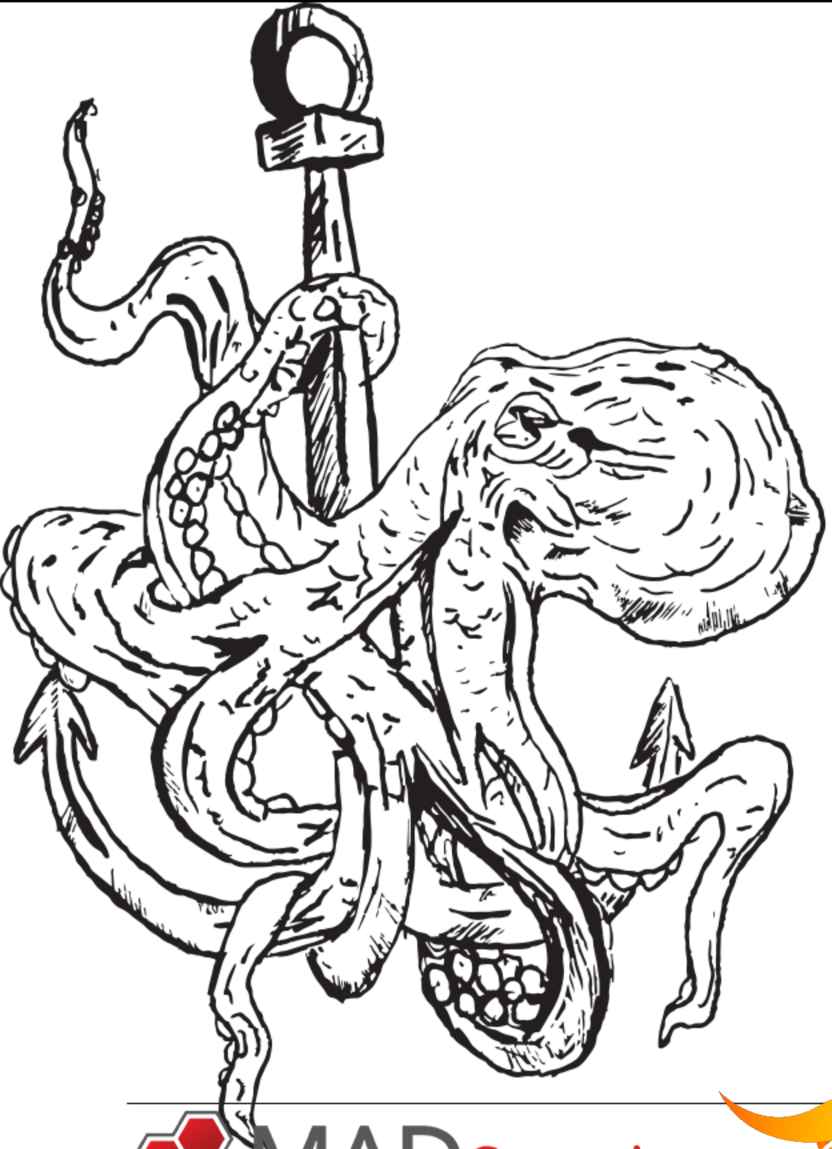


Cluster 4 Example

INMARSAT-F250 SATCOM SYSTEM

Connectivity with LAN/WAN

Eh,… we are all about STARLINK!

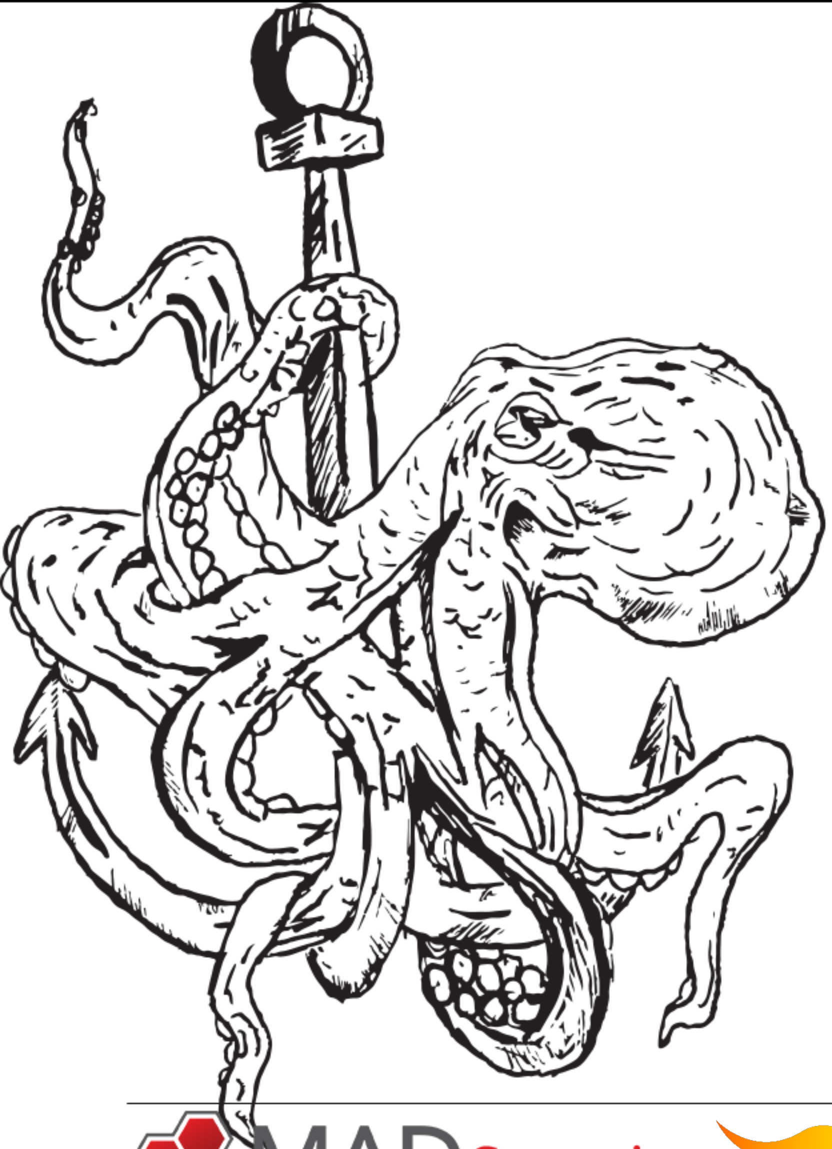


Cluster 3 Example

RADAR PLANT

Own/self-contained LAN but not connected to anything else.

Includes IP addressing and ethernet ports but not connected to Internet/IT Network

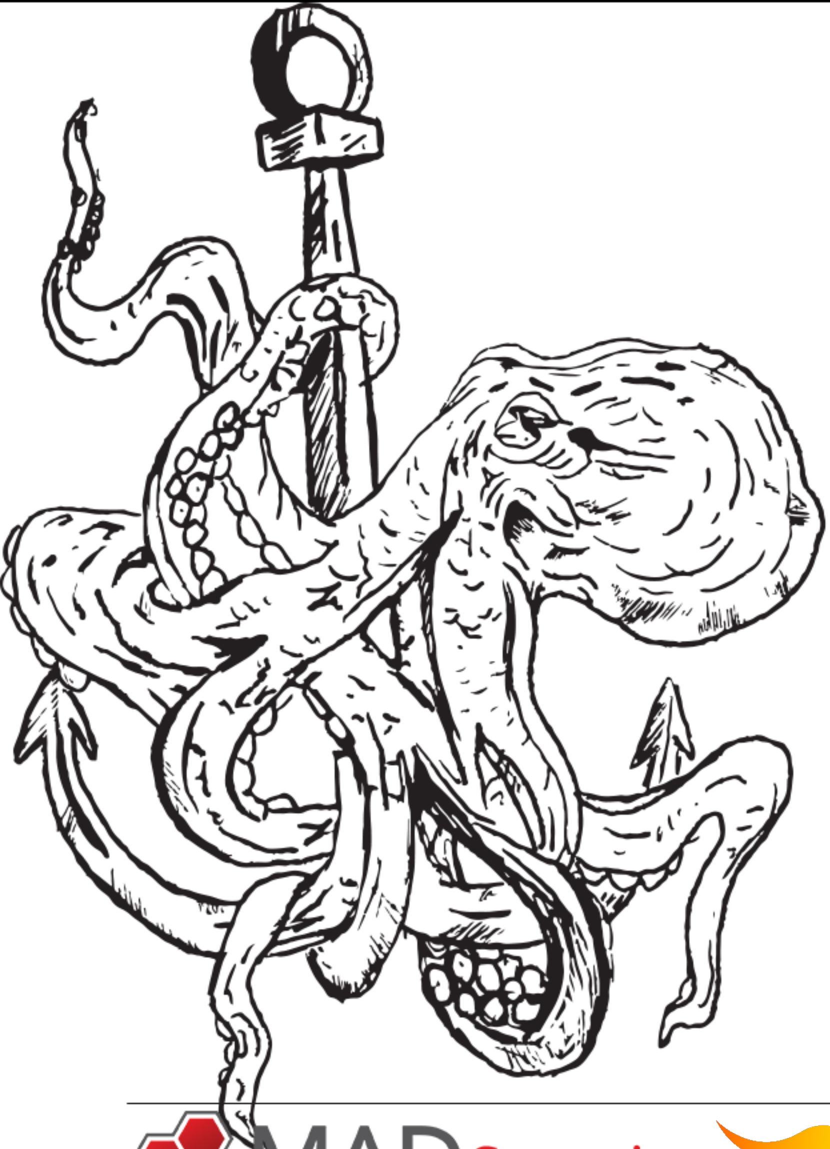


Cluster 2 Example

ECDIS

LAN Capable – Not configured

Contains connections or outputs setup for remote components, but not LAN connected

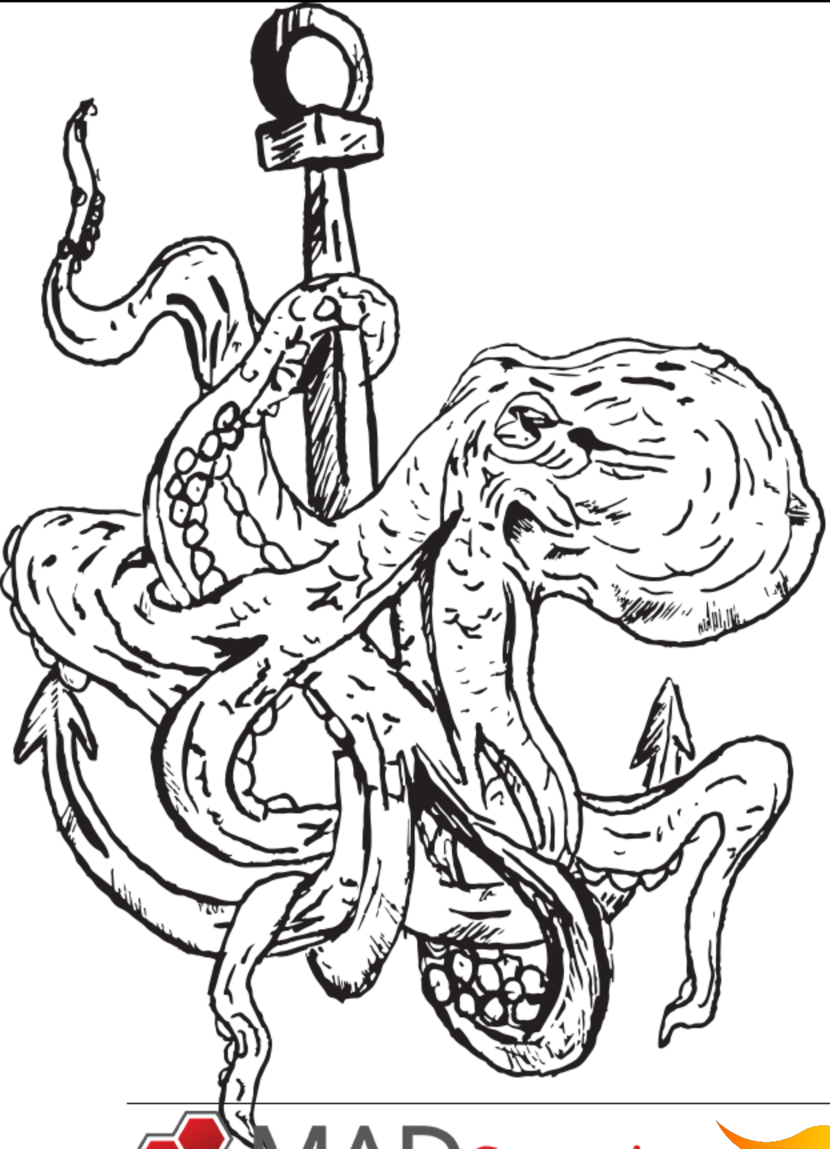


Cluster 1 Example

VHF RADIO TELEPHONE

Serviceable only via USB/other portable media

Limited physical serviceability with no networking capabilities



Cluster 0 Example

WHISTLE AND WHISTLE CONTROL SYSTEM

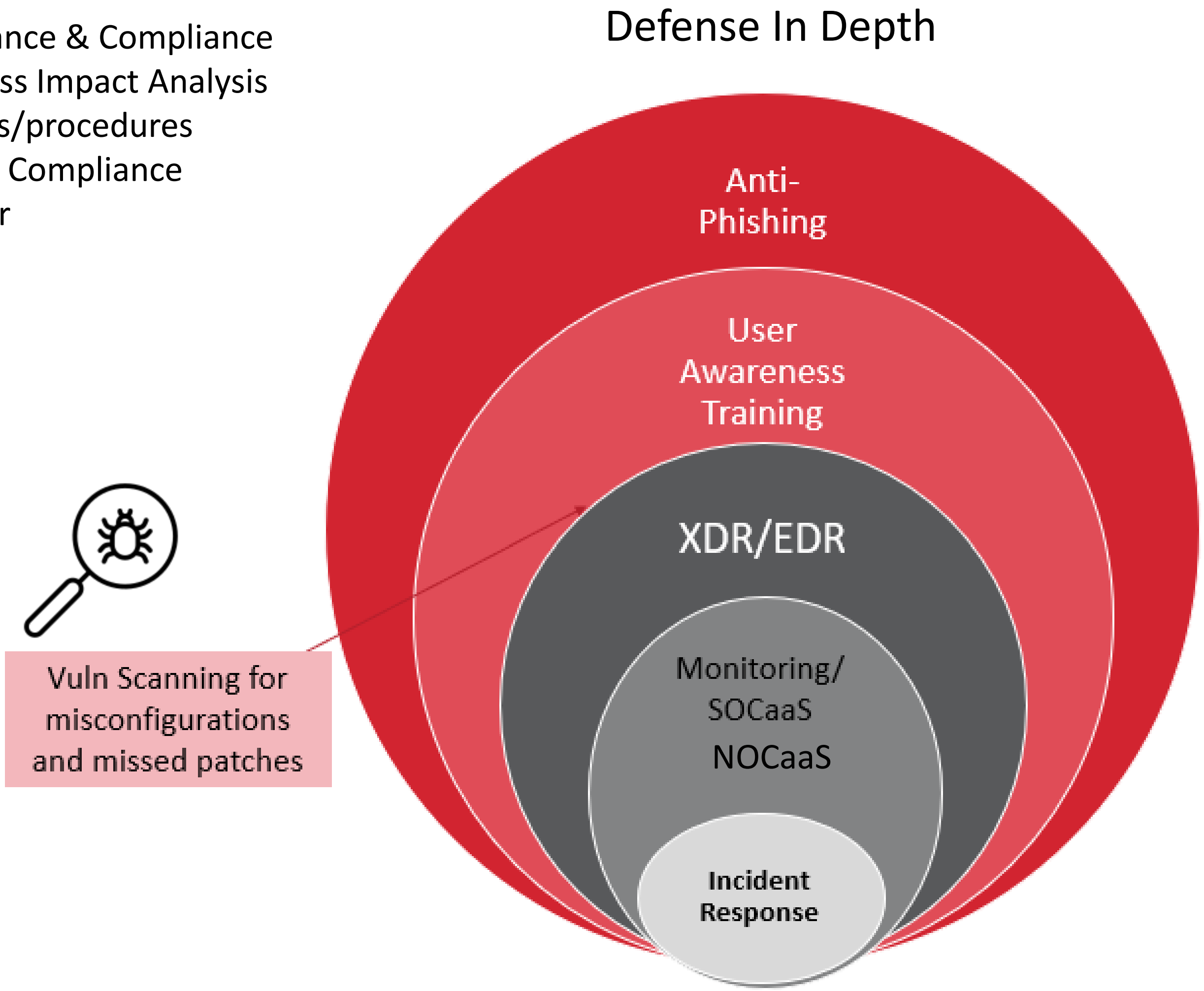
No connections or impacts of any type

Check and Check Again

Defense in Depth – Multi-Layered Security Strategy

Security AND Compliance with CMMC

Governance & Compliance
--Business Impact Analysis
--Policies/procedures
--Virtual Compliance Manager



Phishing Attacks

Most Ransomware is delivered via phishing attacks, tricking users to click and download. Step one is to prevent phishing attacks.

User Behavior

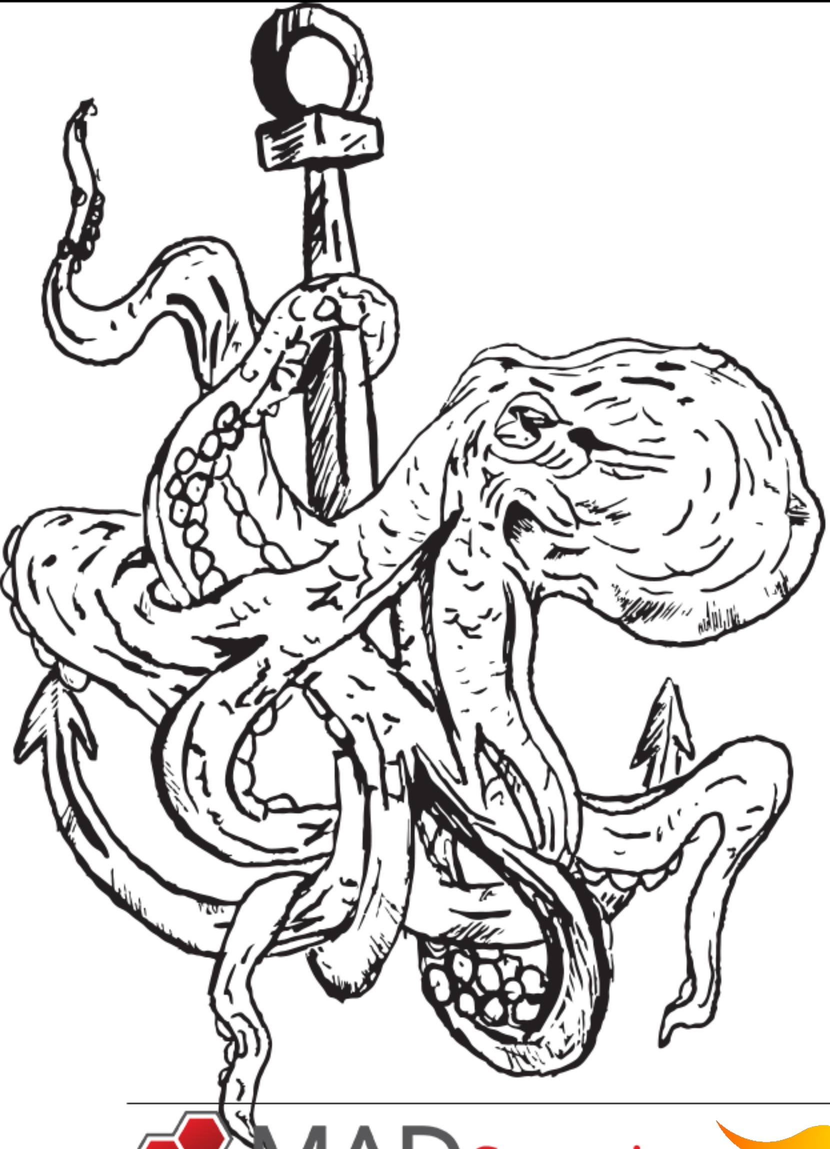
Should a phishing attack successfully penetrate your first layer of defenses, arm your users with training and testing to prevent clicking..

Endpoint Protection

In the event that a phishing attack is delivered to a user, and they do click on it, ensure that their machine can detect and quarantine the malware.

Monitoring / Incident Response

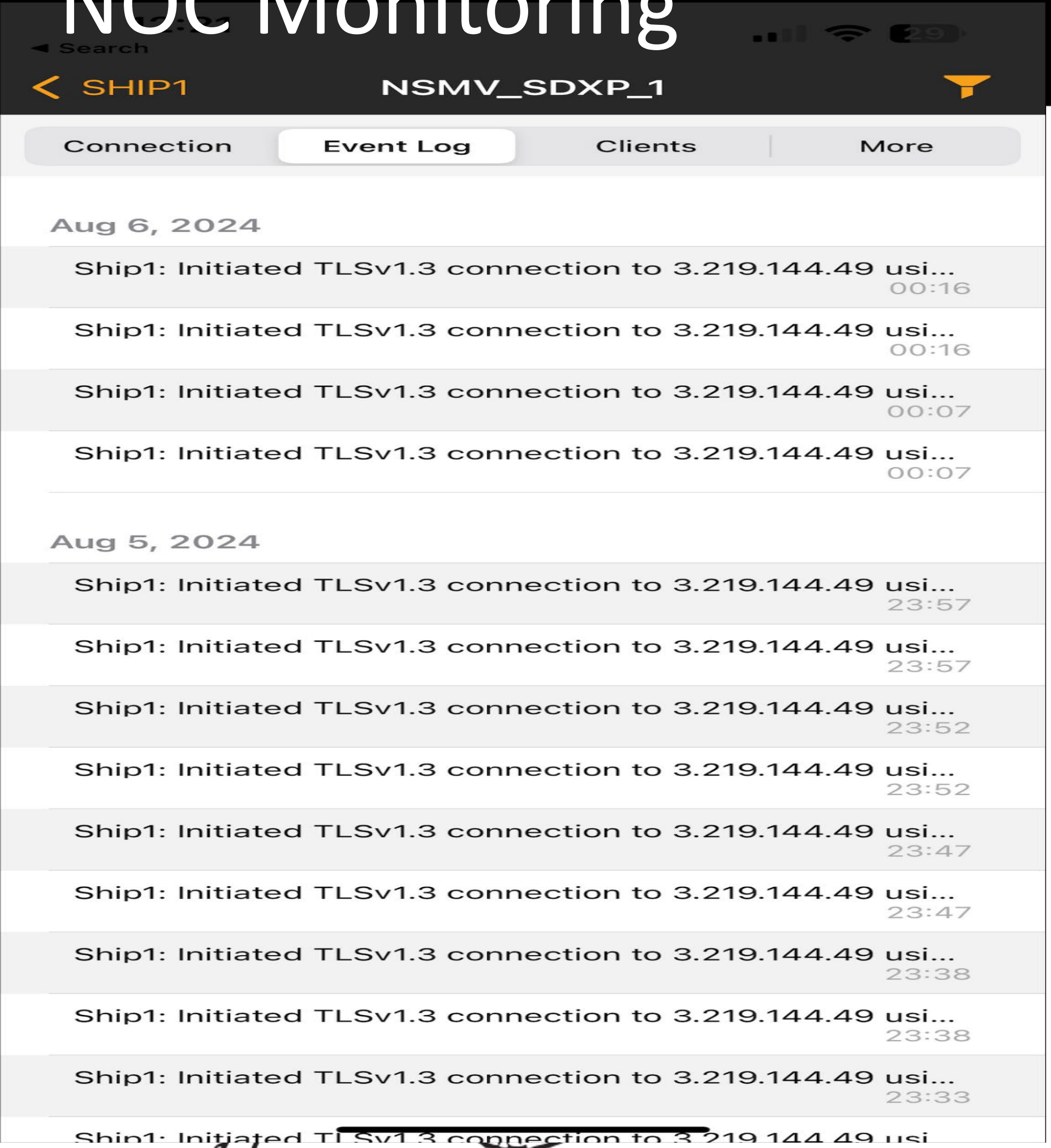
24/7 monitoring of logs and events for anything that happens out of the ordinary. Logs stored for analysis, and a response can be launched immediately.



SOC/NOC Requirements

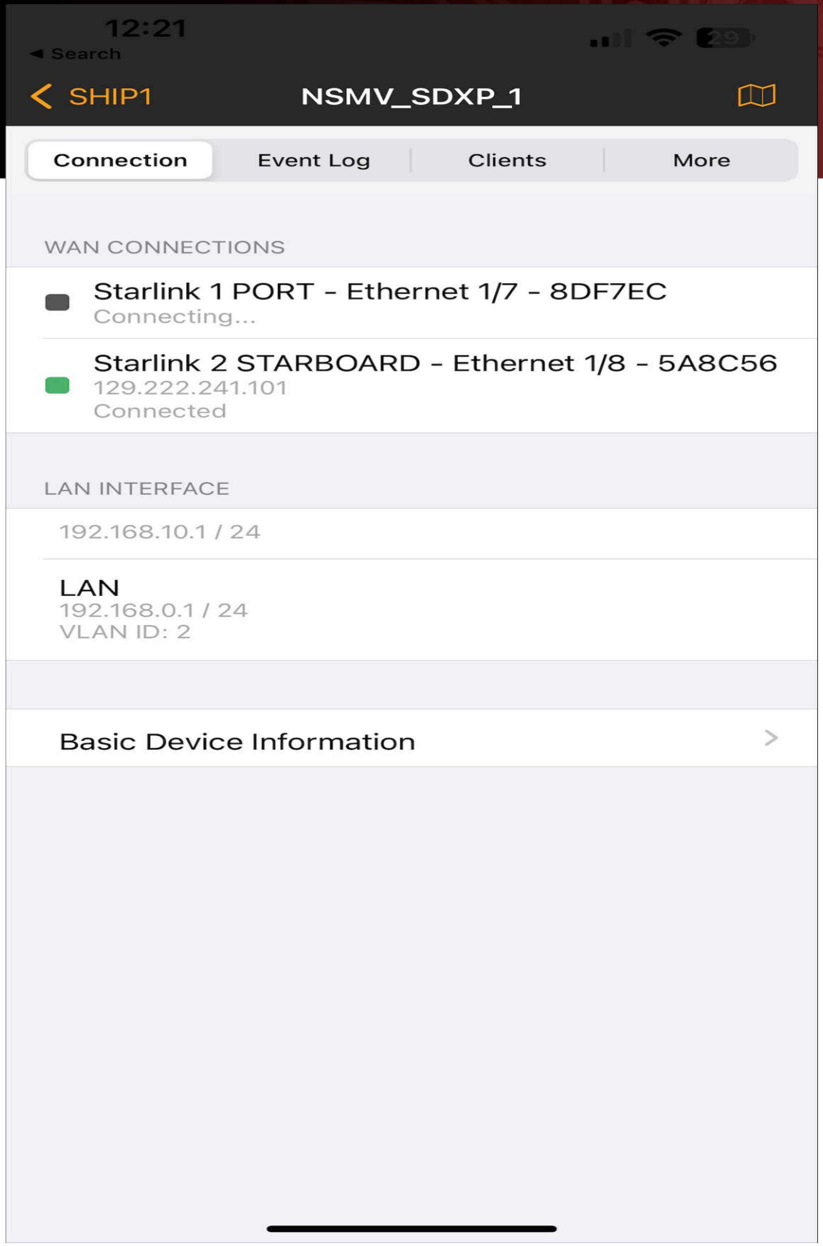
No NOC
No SOC
No Service

NOC Monitoring



```
Aug 6, 2024
Ship1: Initiated TLSv1.3 connection to 3.219.144.49 usi...
                                                   00:16
Ship1: Initiated TLSv1.3 connection to 3.219.144.49 usi...
                                                   00:16
Ship1: Initiated TLSv1.3 connection to 3.219.144.49 usi...
                                                   00:07
Ship1: Initiated TLSv1.3 connection to 3.219.144.49 usi...
                                                   00:07

Aug 5, 2024
Ship1: Initiated TLSv1.3 connection to 3.219.144.49 usi...
                                                   23:57
Ship1: Initiated TLSv1.3 connection to 3.219.144.49 usi...
                                                   23:57
Ship1: Initiated TLSv1.3 connection to 3.219.144.49 usi...
                                                   23:52
Ship1: Initiated TLSv1.3 connection to 3.219.144.49 usi...
                                                   23:52
Ship1: Initiated TLSv1.3 connection to 3.219.144.49 usi...
                                                   23:47
Ship1: Initiated TLSv1.3 connection to 3.219.144.49 usi...
                                                   23:47
Ship1: Initiated TLSv1.3 connection to 3.219.144.49 usi...
                                                   23:38
Ship1: Initiated TLSv1.3 connection to 3.219.144.49 usi...
                                                   23:38
Ship1: Initiated TLSv1.3 connection to 3.219.144.49 usi...
                                                   23:33
Ship1: Initiated TLSv1.3 connection to 3.219.144.49 usi
```



WAN CONNECTIONS

■ Starlink 1 PORT – Ethernet 1/7 – 8DF7EC
Connecting...

🟩 Starlink 2 STARBOARD – Ethernet 1/8 – 5A8C56
129.222.241.101
Connected

LAN INTERFACE

192.168.10.1 / 24

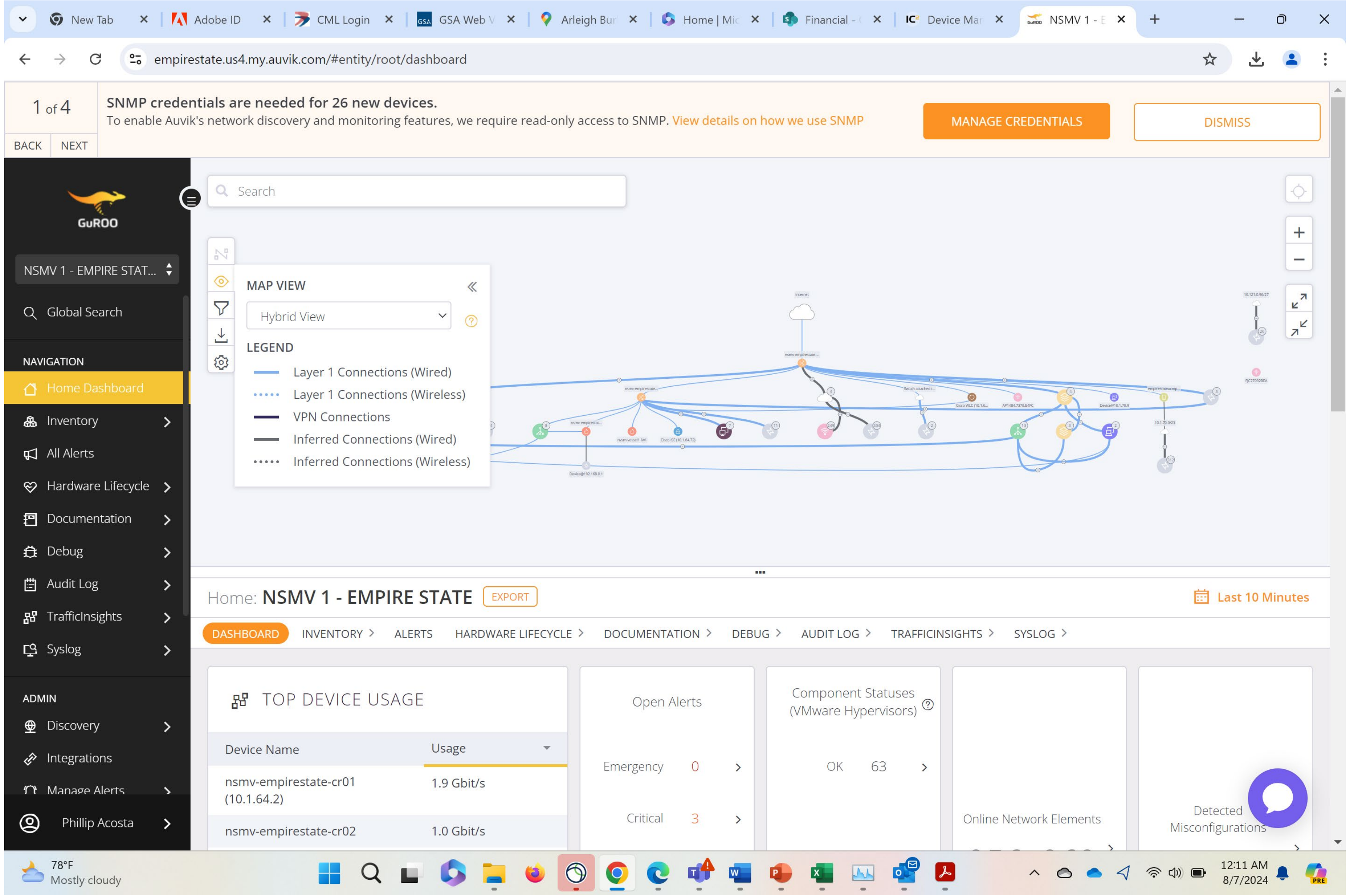
LAN
192.168.0.1 / 24
VLAN ID: 2

Basic Device Information >

MADSecurity Maritime Division

GuROO

NOC Monitoring



empirestate.us4.my.auvik.com/#entity/root/dashboard

SNMP credentials are needed for 26 new devices.
To enable Auvik's network discovery and monitoring features, we require read-only access to SNMP. View details on how we use SNMP

MAP VIEW

Hybrid View

LEGEND

- Layer 1 Connections (Wired)
- Layer 1 Connections (Wireless)
- VPN Connections
- Inferred Connections (Wired)
- Inferred Connections (Wireless)

Home: **NSMV 1 - EMPIRE STATE**

Last 10 Minutes

TOP DEVICE USAGE

Device Name	Usage
nsmv-empirestate-cr01 (10.1.64.2)	1.9 Gbit/s
nsmv-empirestate-cr02	1.0 Gbit/s

Open Alerts

Emergency	0
Critical	3

Component Statuses (VMware Hypervisors)

OK	63

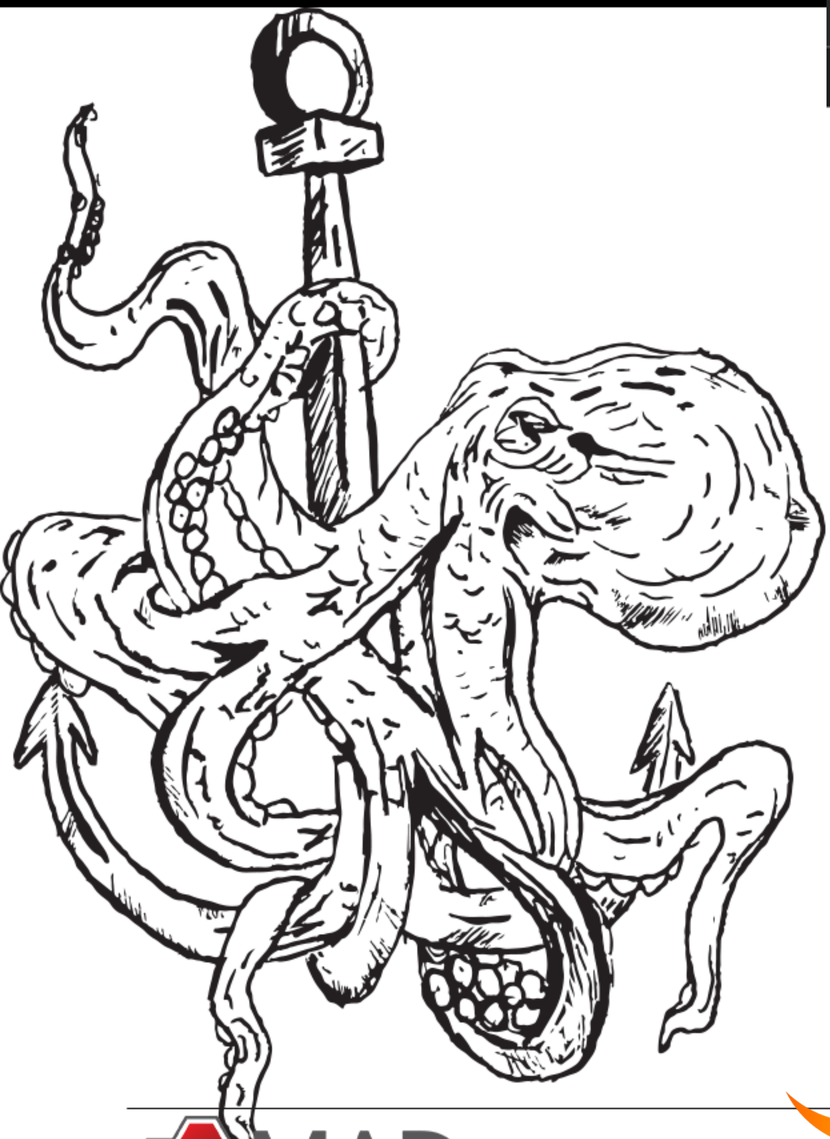
Online Network Elements

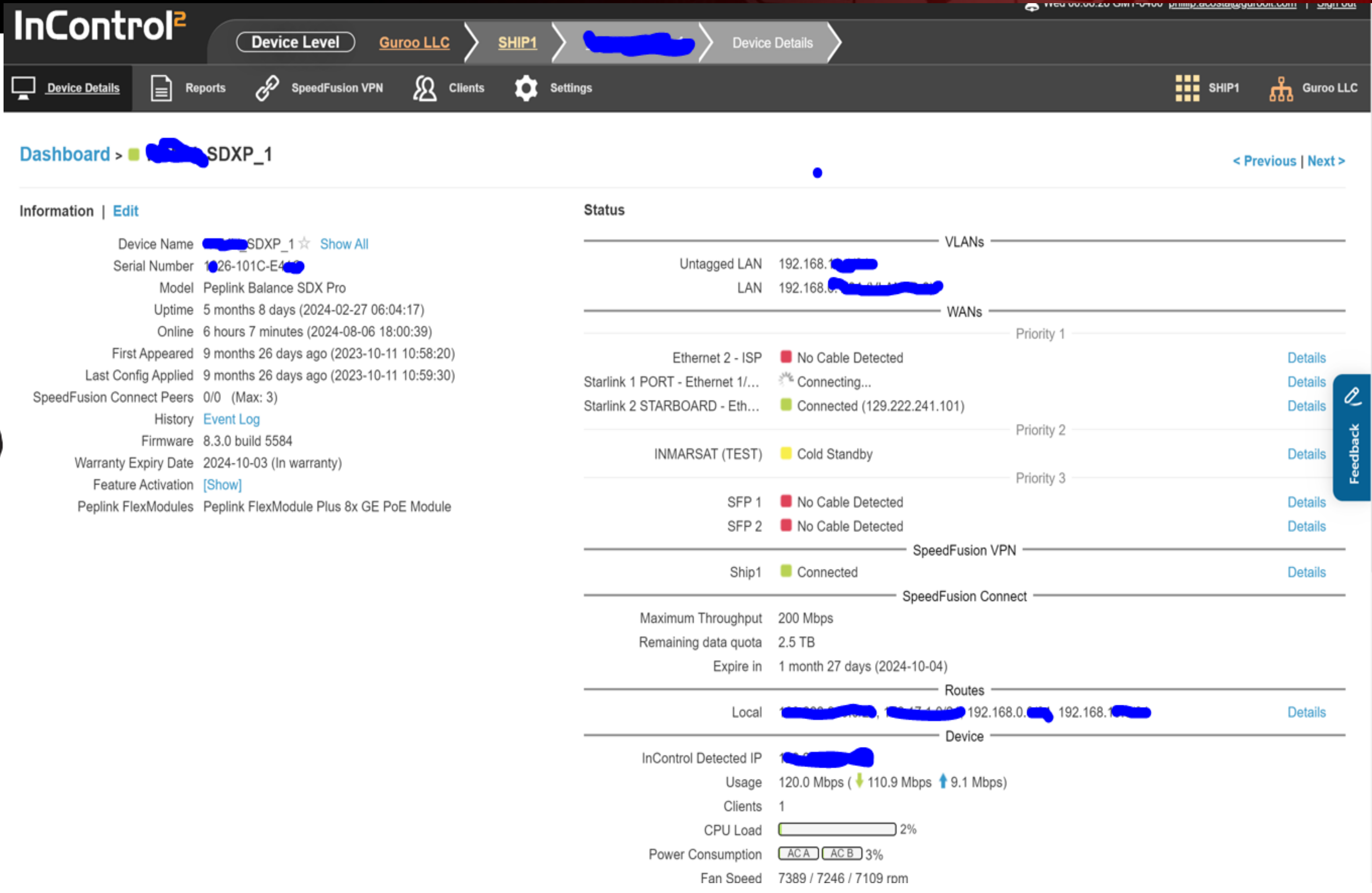
Detected Misconfigurations

MADSecurity
Maritime Division

GuROO

NOC Monitoring





Dashboard > 🟩 [redacted]SDXP_1

< Previous | Next >

Information | Edit

Device Name	[redacted]SDXP_1 ☆ Show All
Serial Number	1[redacted]26-101C-E4[redacted]
Model	Peplink Balance SDX Pro
Uptime	5 months 8 days (2024-02-27 06:04:17)
Online	6 hours 7 minutes (2024-08-06 18:00:39)
First Appeared	9 months 26 days ago (2023-10-11 10:58:20)
Last Config Applied	9 months 26 days ago (2023-10-11 10:59:30)
SpeedFusion Connect Peers	0/0 (Max: 3)
History	Event Log
Firmware	8.3.0 build 5584
Warranty Expiry Date	2024-10-03 (In warranty)
Feature Activation	[Show]
Peplink FlexModules	Peplink FlexModule Plus 8x GE PoE Module

Status

VLANs

Untagged LAN	192.168.[redacted]
LAN	192.168.[redacted]

WANs

Priority 1

Ethernet 2 - ISP	🟥 No Cable Detected	Details
Starlink 1 PORT - Ethernet 1/...	Connecting...	Details
Starlink 2 STARBOARD - Eth...	🟩 Connected (129.222.241.101)	Details

Priority 2

INMARSAT (TEST)	🟨 Cold Standby	Details

Priority 3

SFP 1	🟥 No Cable Detected	Details
SFP 2	🟥 No Cable Detected	Details

SpeedFusion VPN

Ship1	🟩 Connected	Details

SpeedFusion Connect

Maximum Throughput	200 Mbps
Remaining data quota	2.5 TB
Expire in	1 month 27 days (2024-10-04)

Routes

Local	[redacted], [redacted] 192.168.0.[redacted] 192.168.1[redacted]	Details

Device

InControl Detected IP	1[redacted]
Usage	120.0 Mbps (↓ 110.9 Mbps ↑ 9.1 Mbps)
Clients	1
CPU Load	2%
Power Consumption	AC A AC B 3%
Fan Speed	7389 / 7246 / 7109 rpm

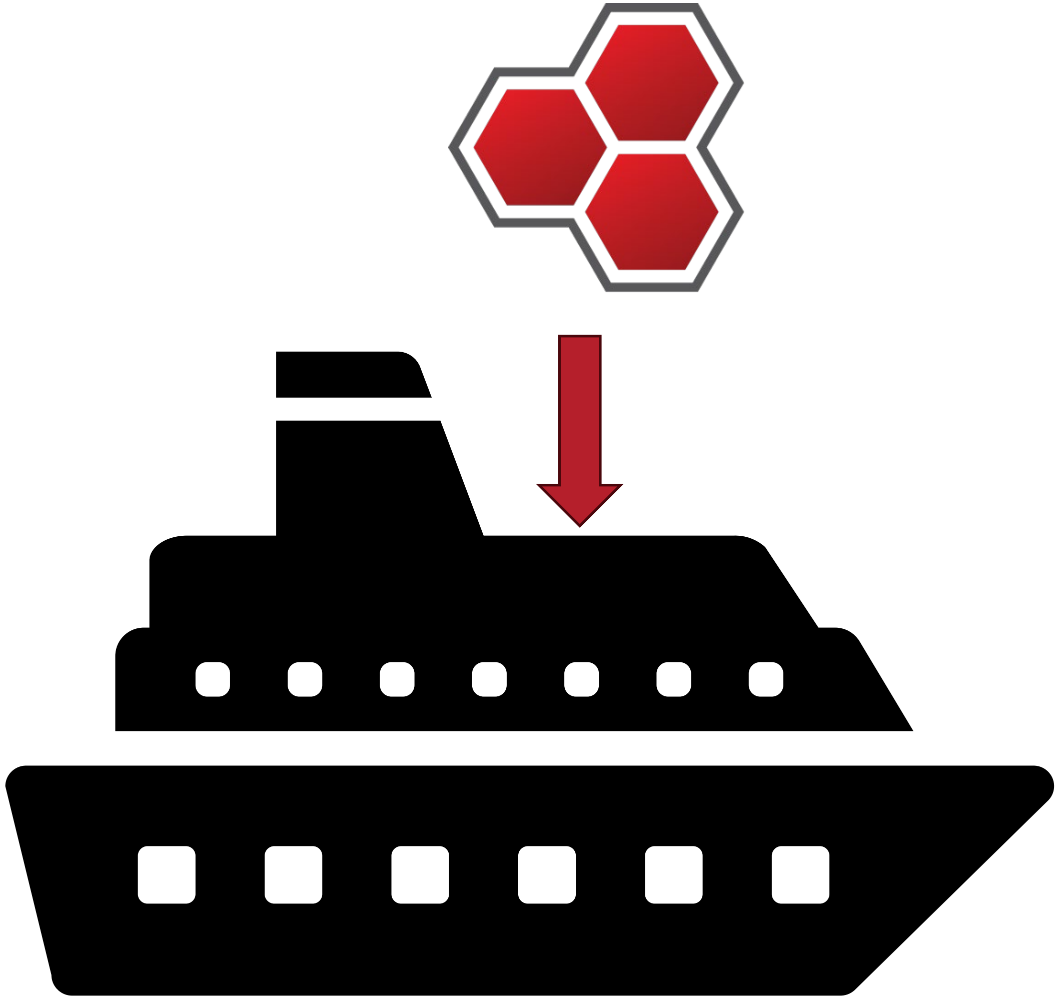
MADSecurity
Maritime Division

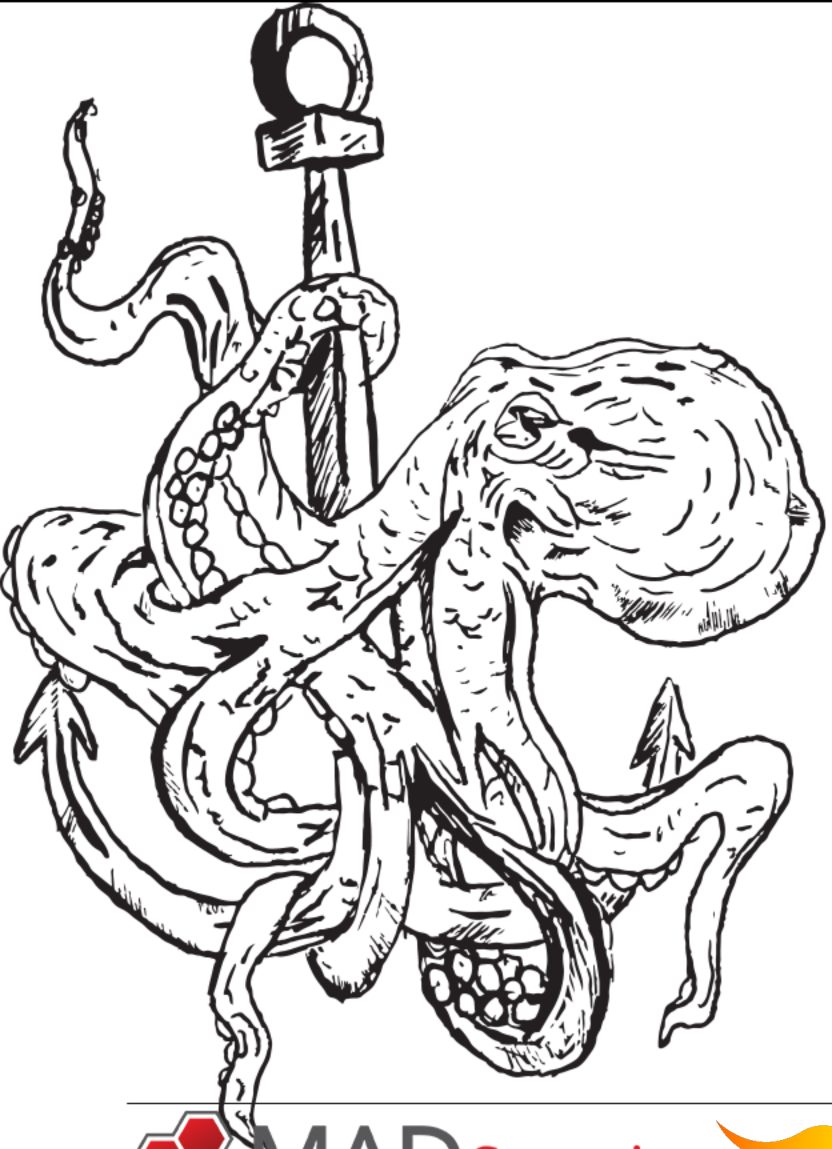
GuROO

888-623-7324 | madmaritime.com

Just Put a 24/7 SOC and NOC on the ship???

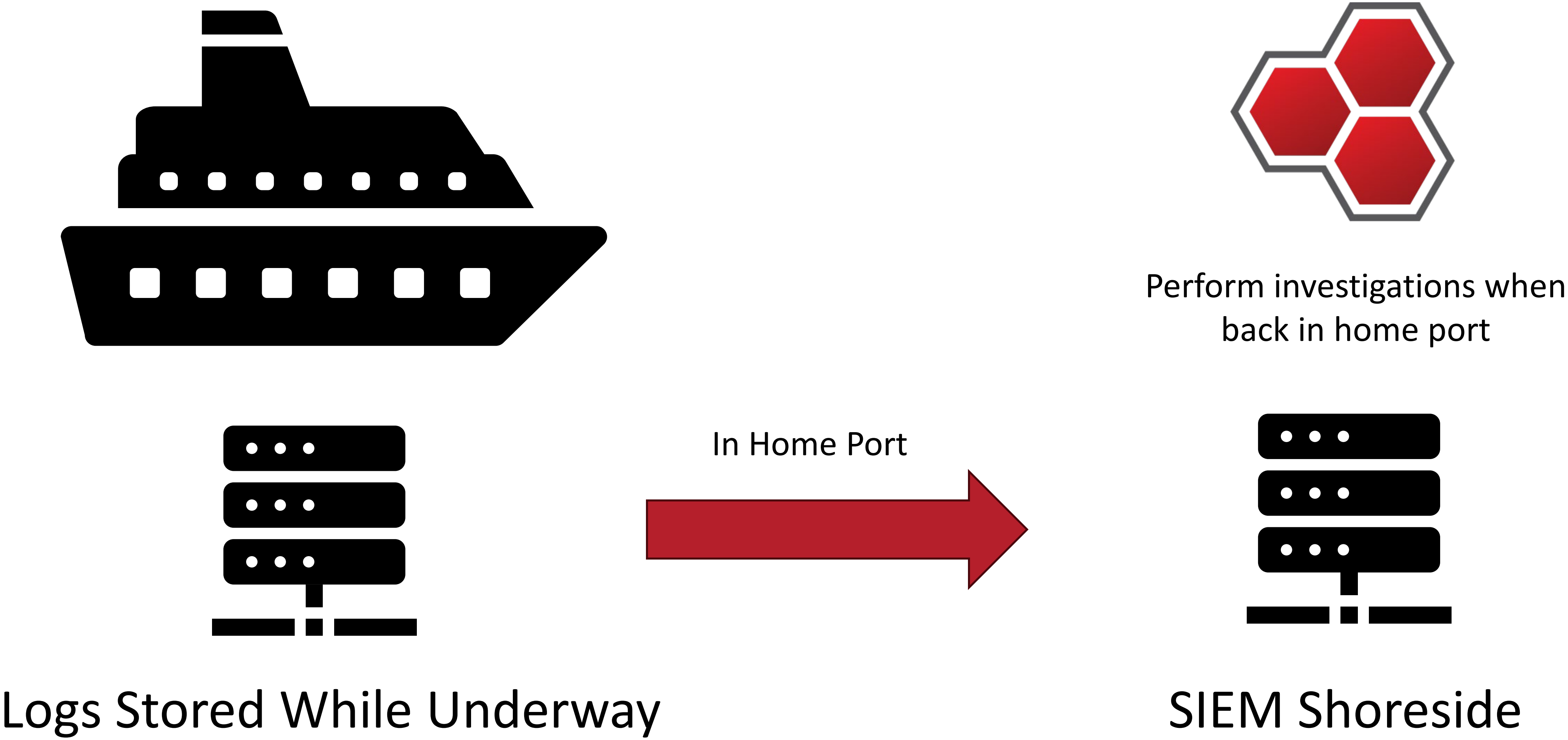
Logs + SATCOM = $$$$$





SOC Solutions

Option 1



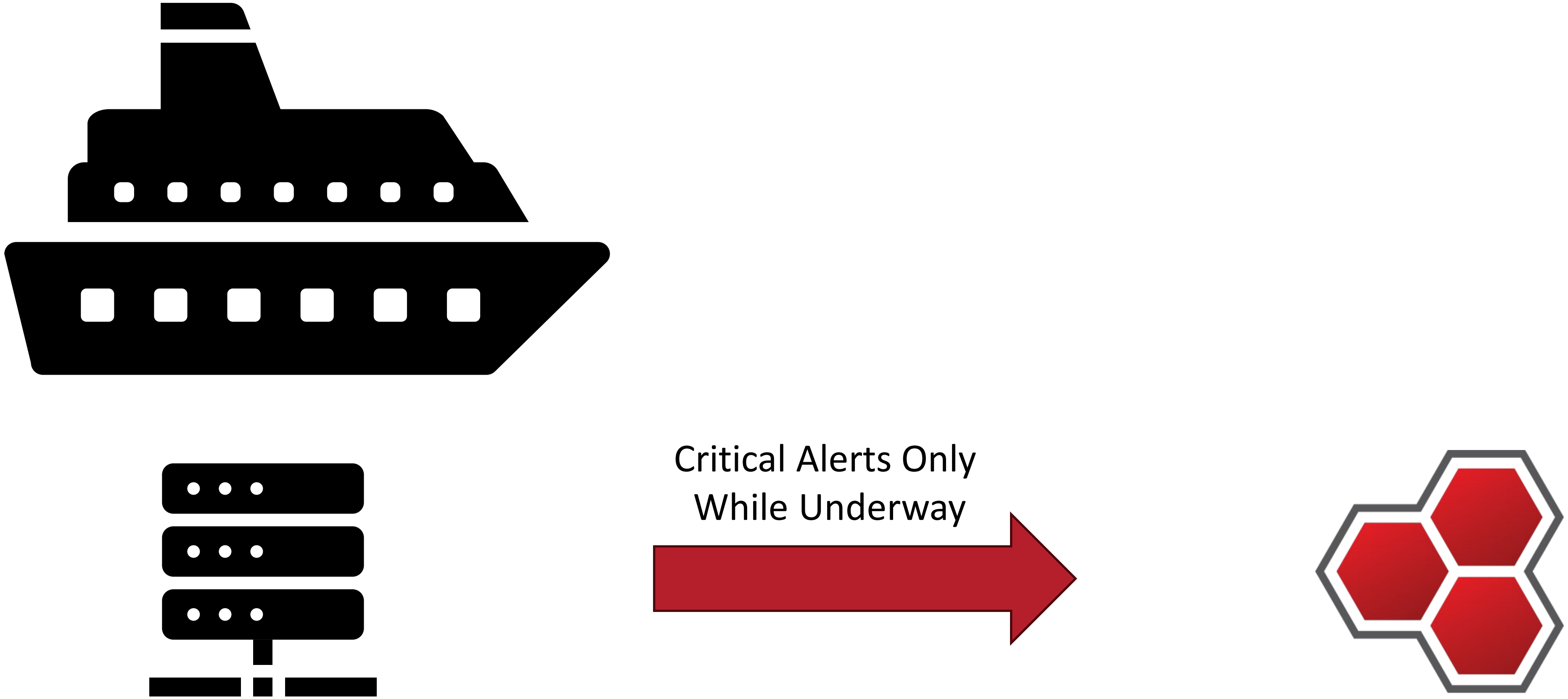
Perform investigations when back in home port

In Home Port

Logs Stored While Underway

SIEM Shoreside

Option 2

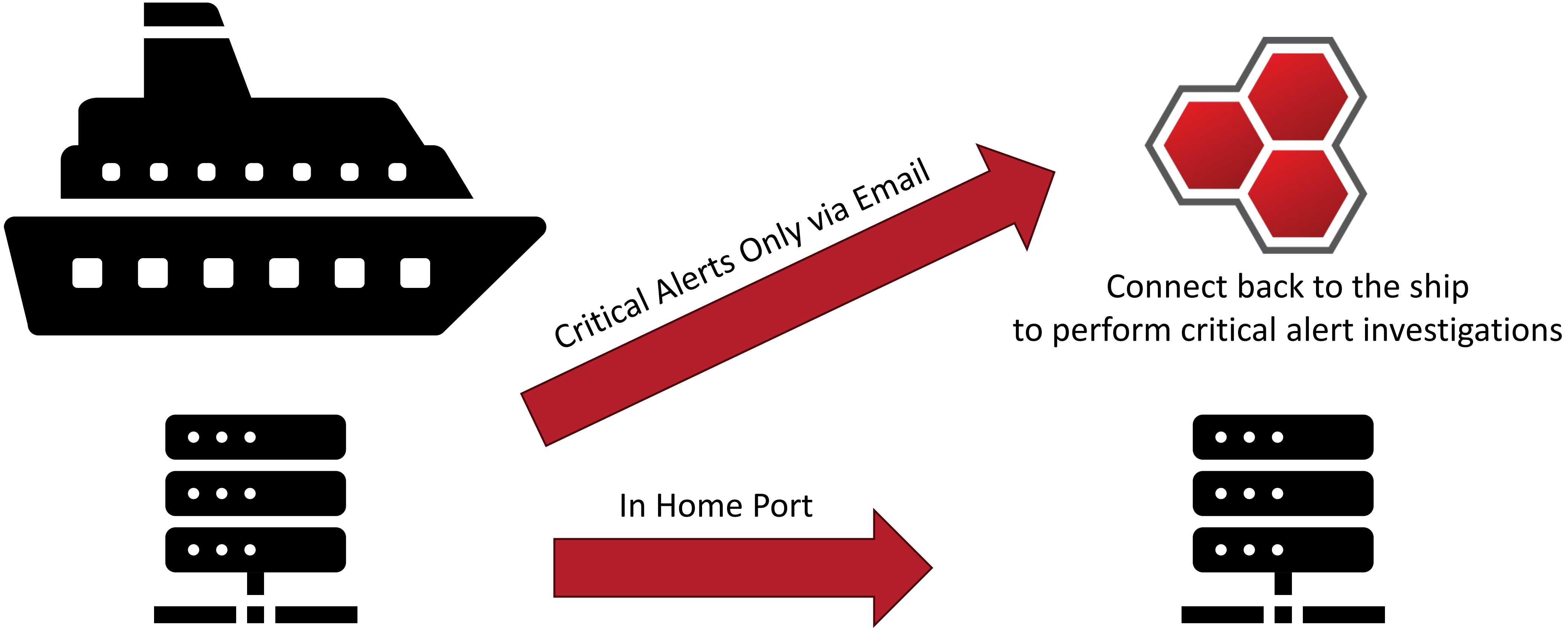


Critical Alerts Only
While Underway

Full SIEM Onboard

Connect back to the ship
to perform investigations

Option 3

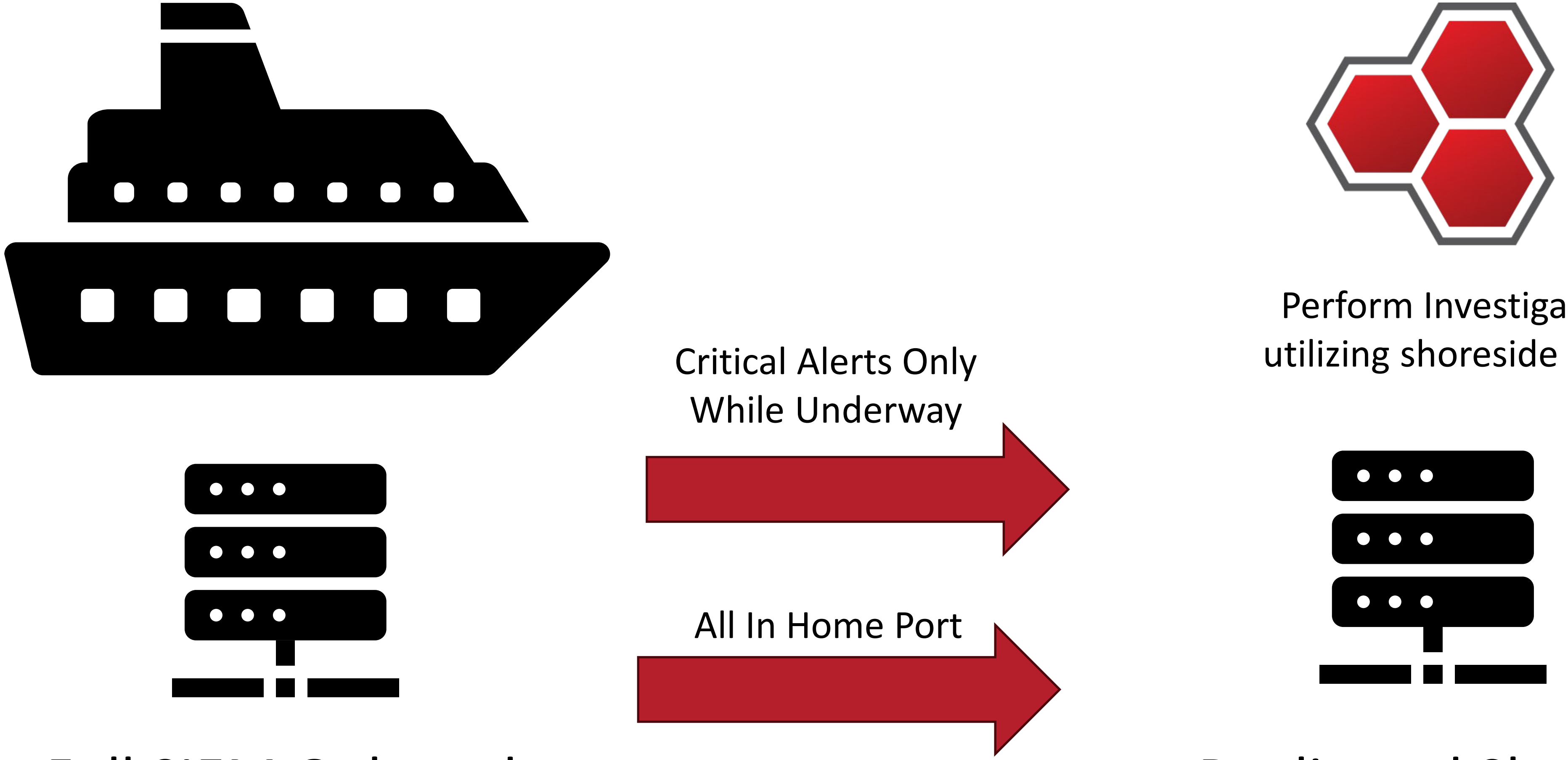


Connect back to the ship
to perform critical alert investigations

Full SIEM Onboard

Replicated Shoreside

Our Solution



Critical Alerts Only
While Underway

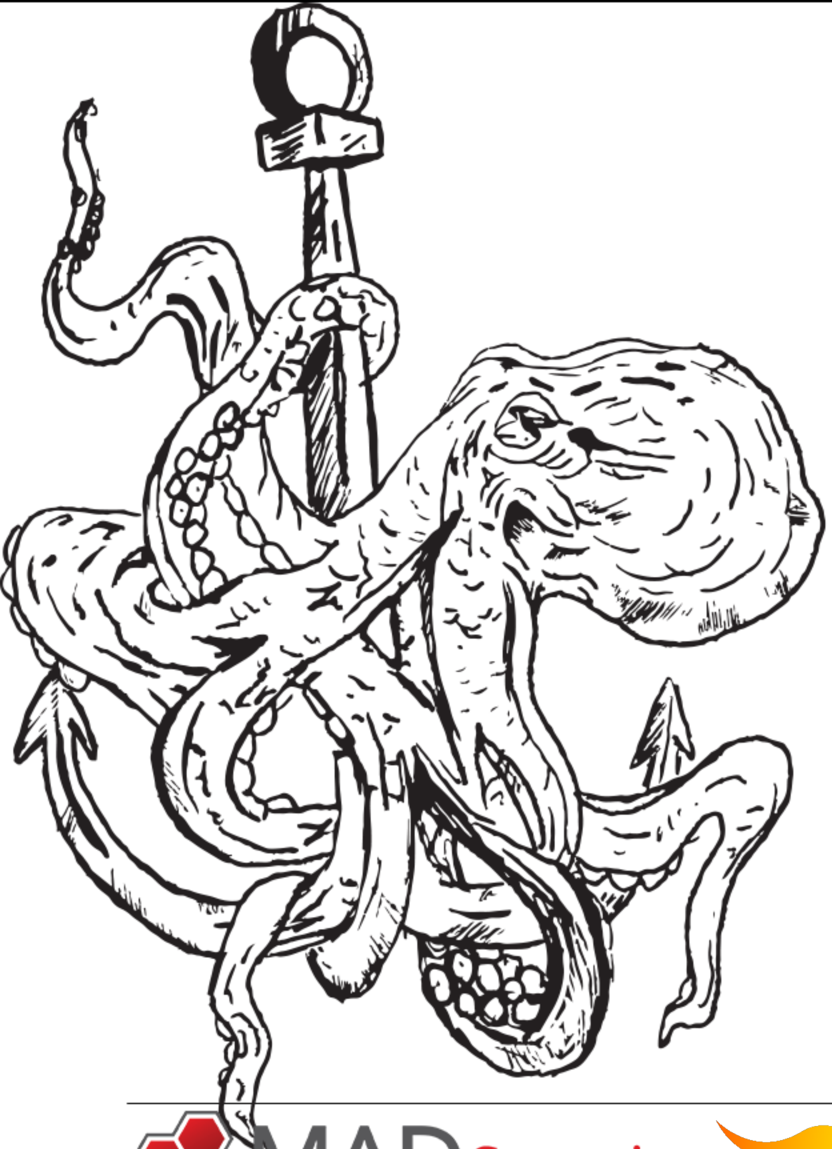
All In Home Port

Perform Investigation
utilizing shoreside SIEM

Full SIEM Onboard

Replicated Shoreside

Tech Stack



Container: Docker

Orchestration: Ansible

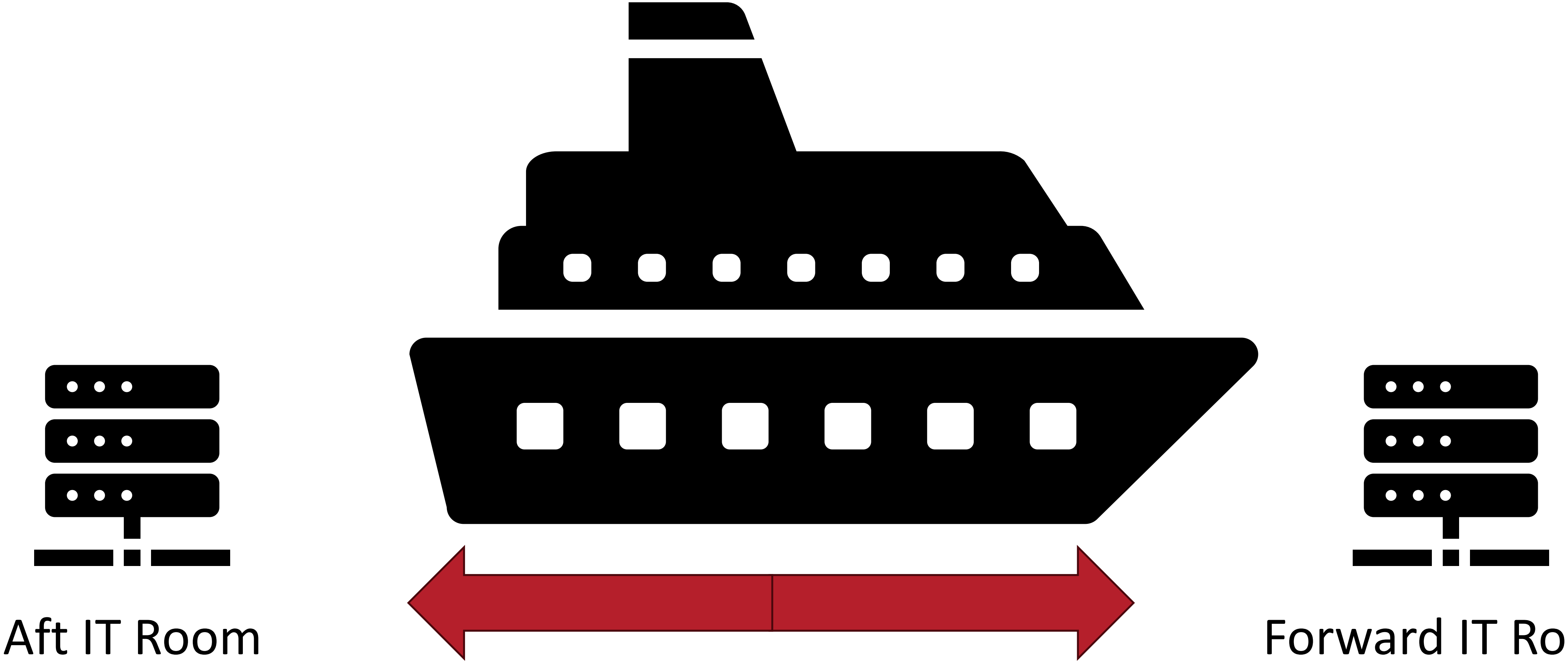
OS: Debian

VPN: OpenVPN

SIEM: Elastic

EDR: Elastic EDR

High Availability

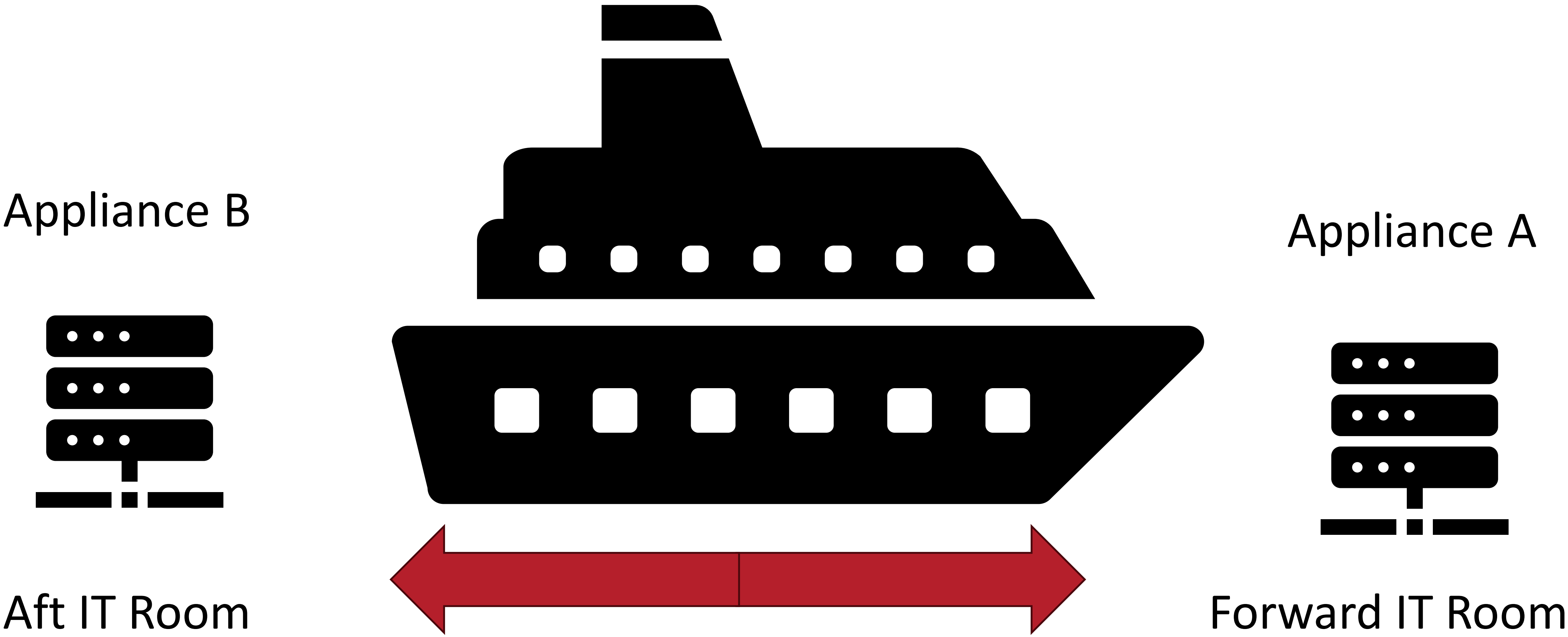


Aft IT Room

Forward IT Room

HA Pairs

High Availability



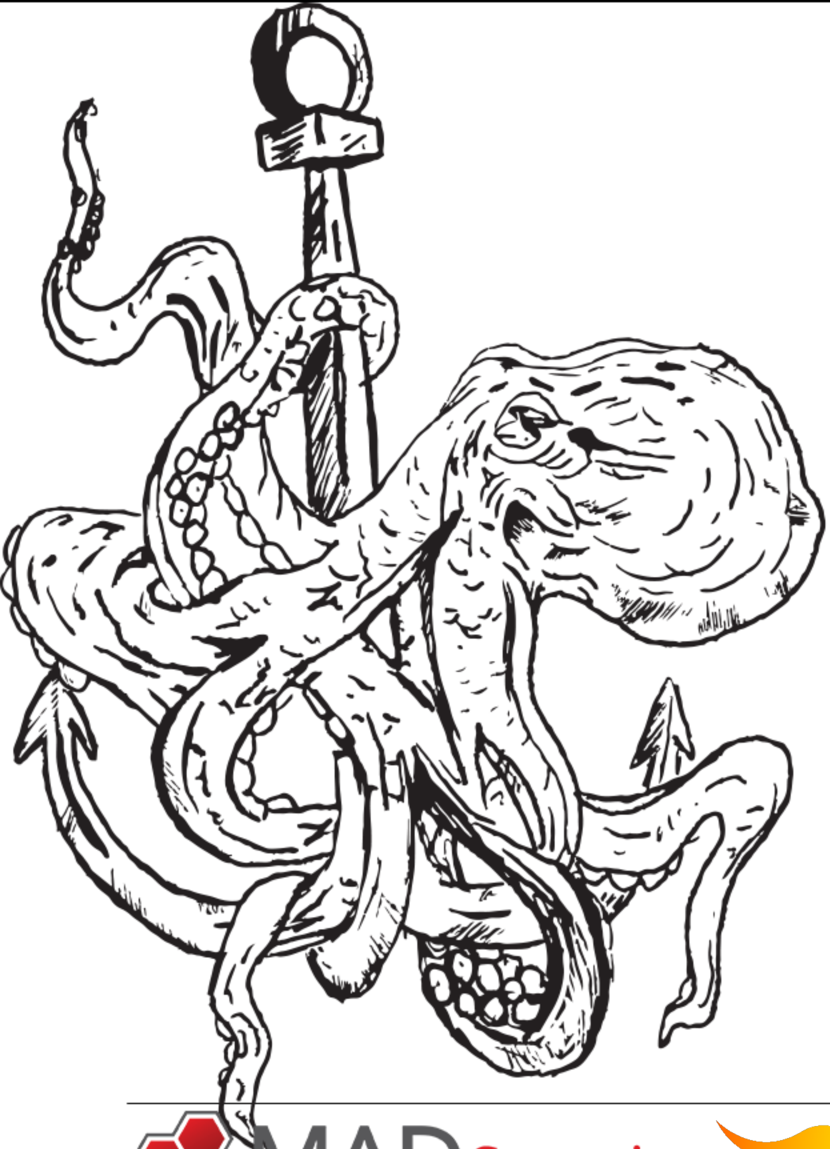
Appliance B

Aft IT Room

Appliance A

Forward IT Room

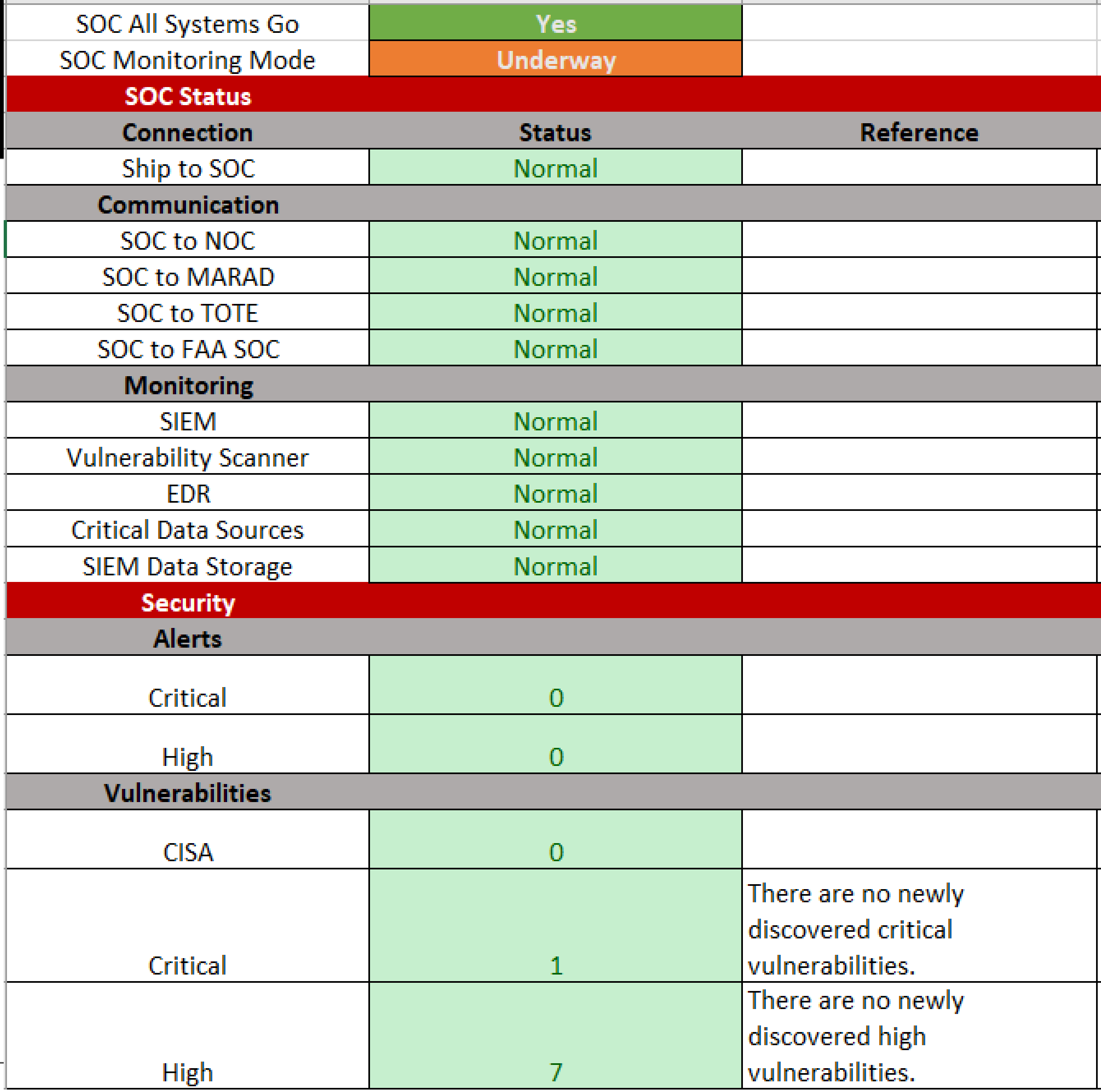
HA Pairs



Test Environment

Dashboards

Customized for client needs

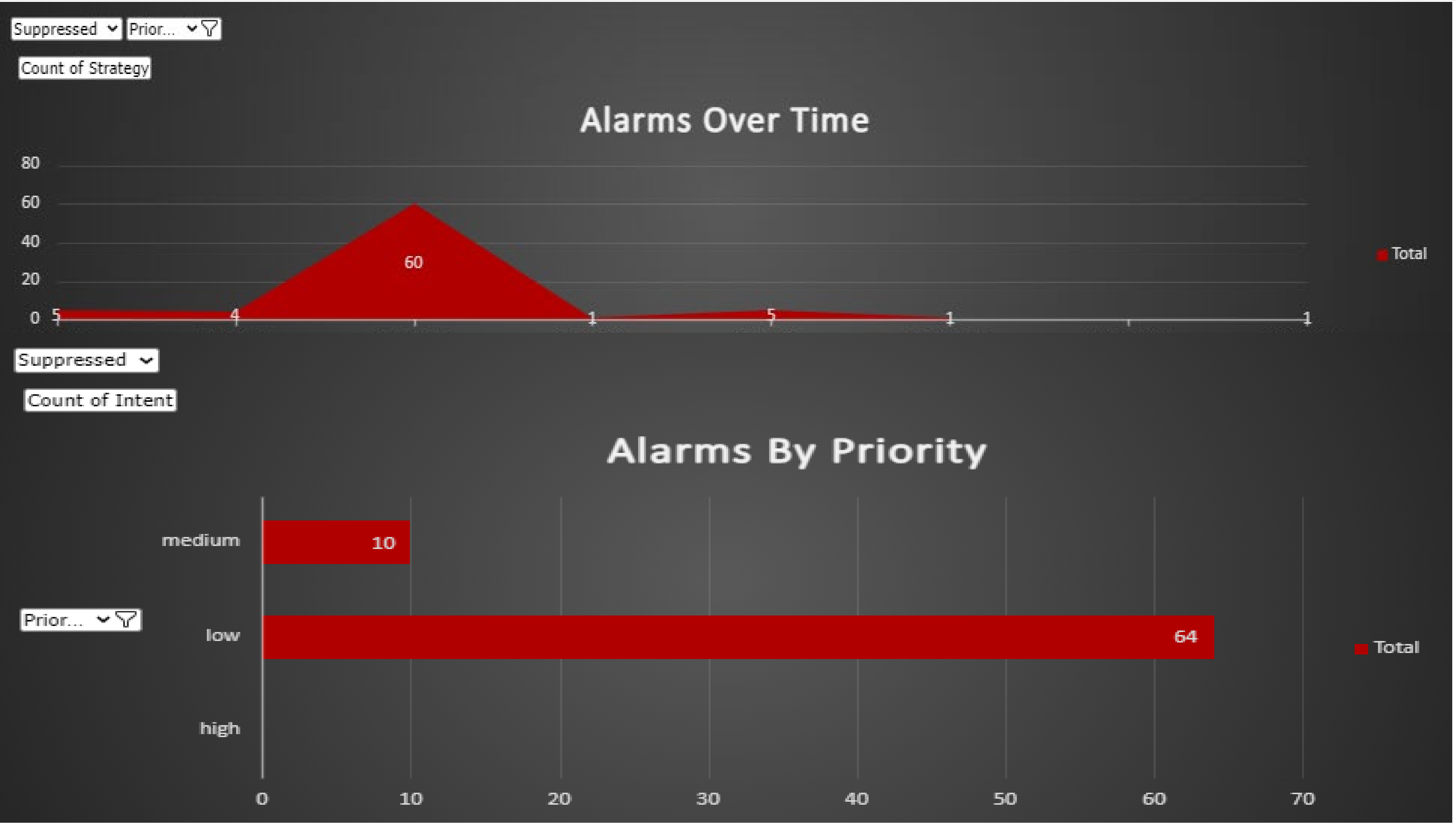


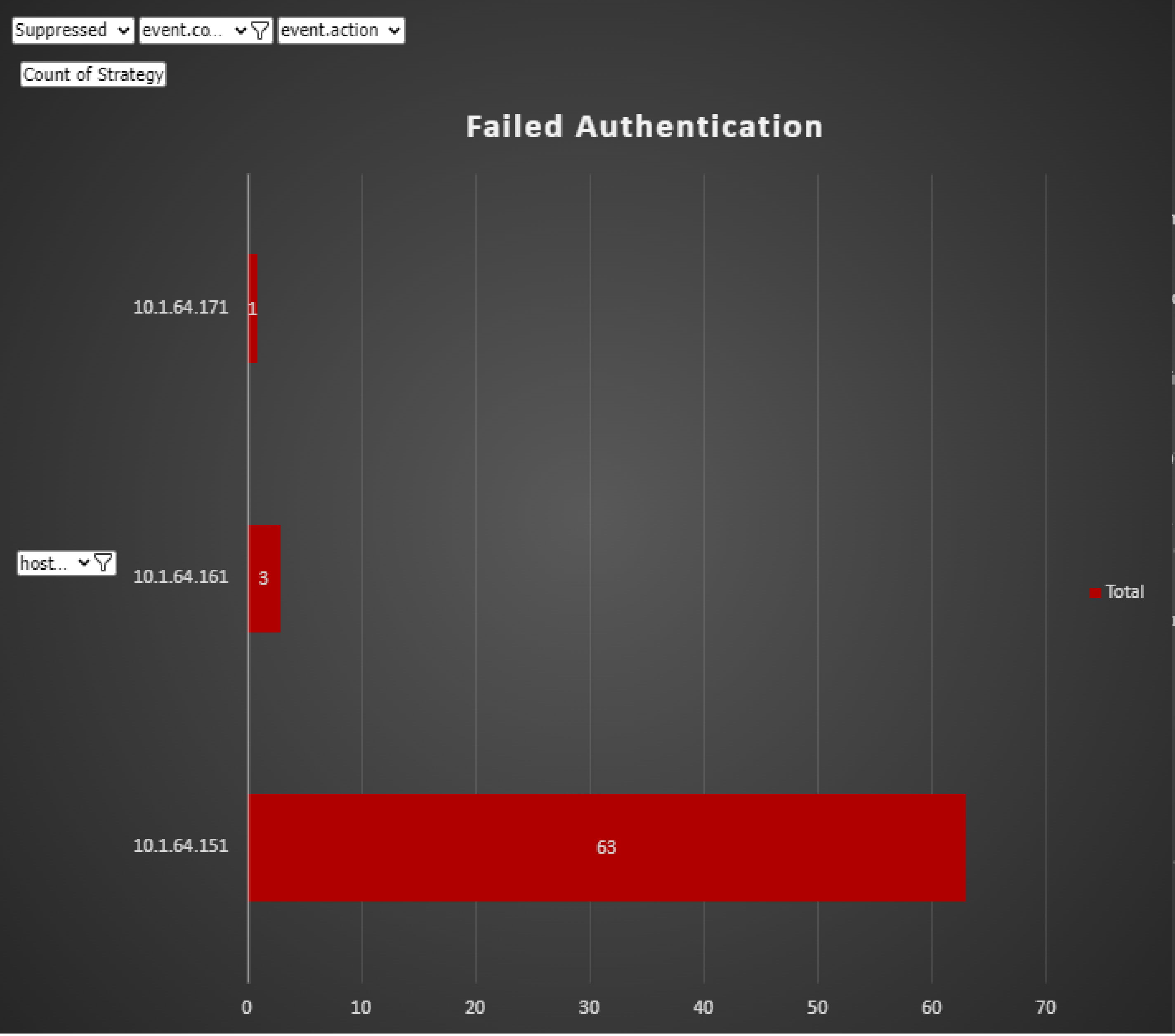
SOC All Systems Go	Yes	
SOC Monitoring Mode	Underway	
SOC Status		
Connection	**Status**	**Reference**
Ship to SOC	Normal	
Communication		
SOC to NOC	Normal	
SOC to MARAD	Normal	
SOC to TOTE	Normal	
SOC to FAA SOC	Normal	
Monitoring		
SIEM	Normal	
Vulnerability Scanner	Normal	
EDR	Normal	
Critical Data Sources	Normal	
SIEM Data Storage	Normal	
Security		
Alerts		
Critical	0	
High	0	
Vulnerabilities		
CISA	0	
Critical	1	There are no newly discovered critical vulnerabilities.
High	7	There are no newly discovered high vulnerabilities.

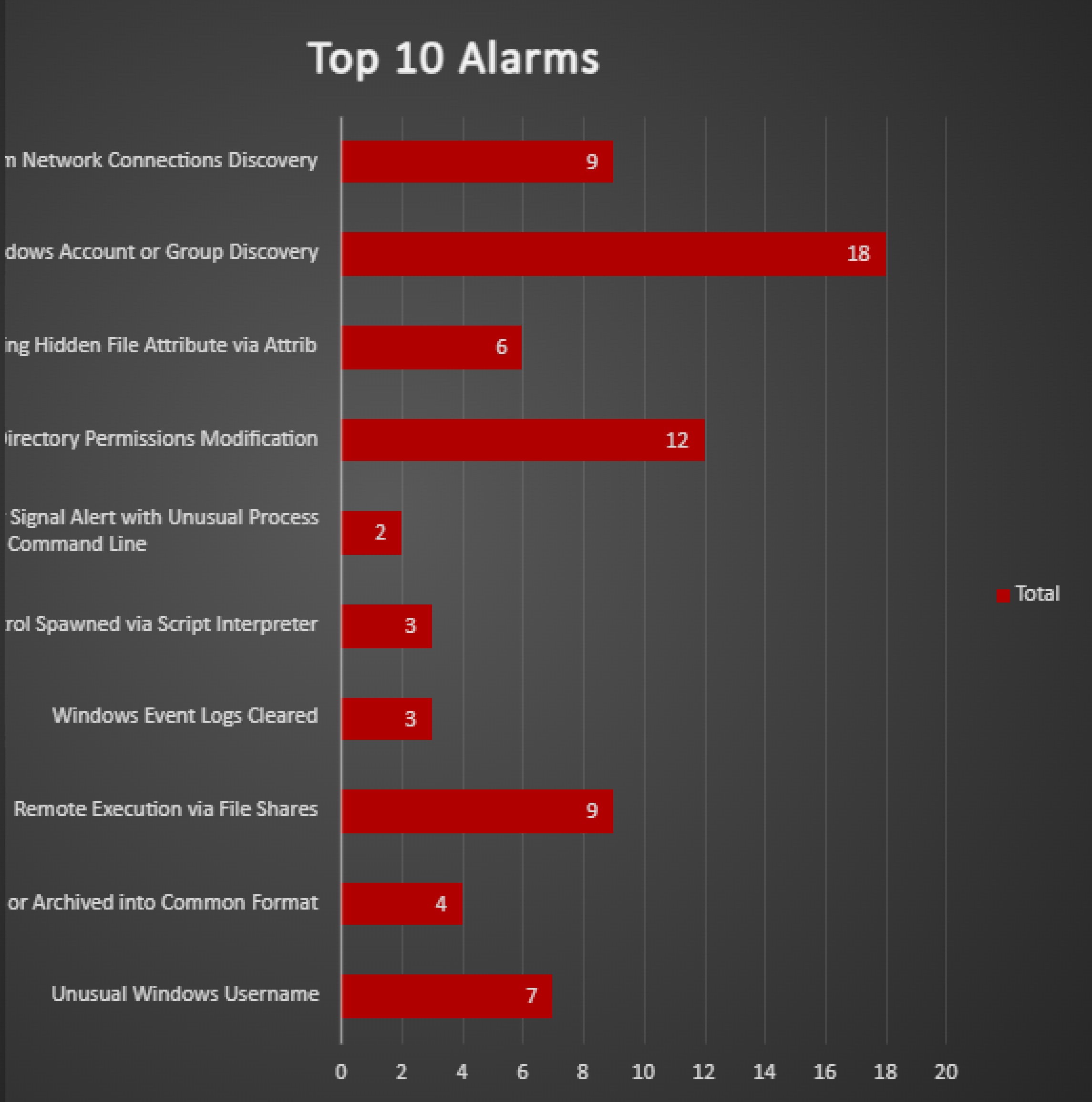
MADSecurity Maritime Division

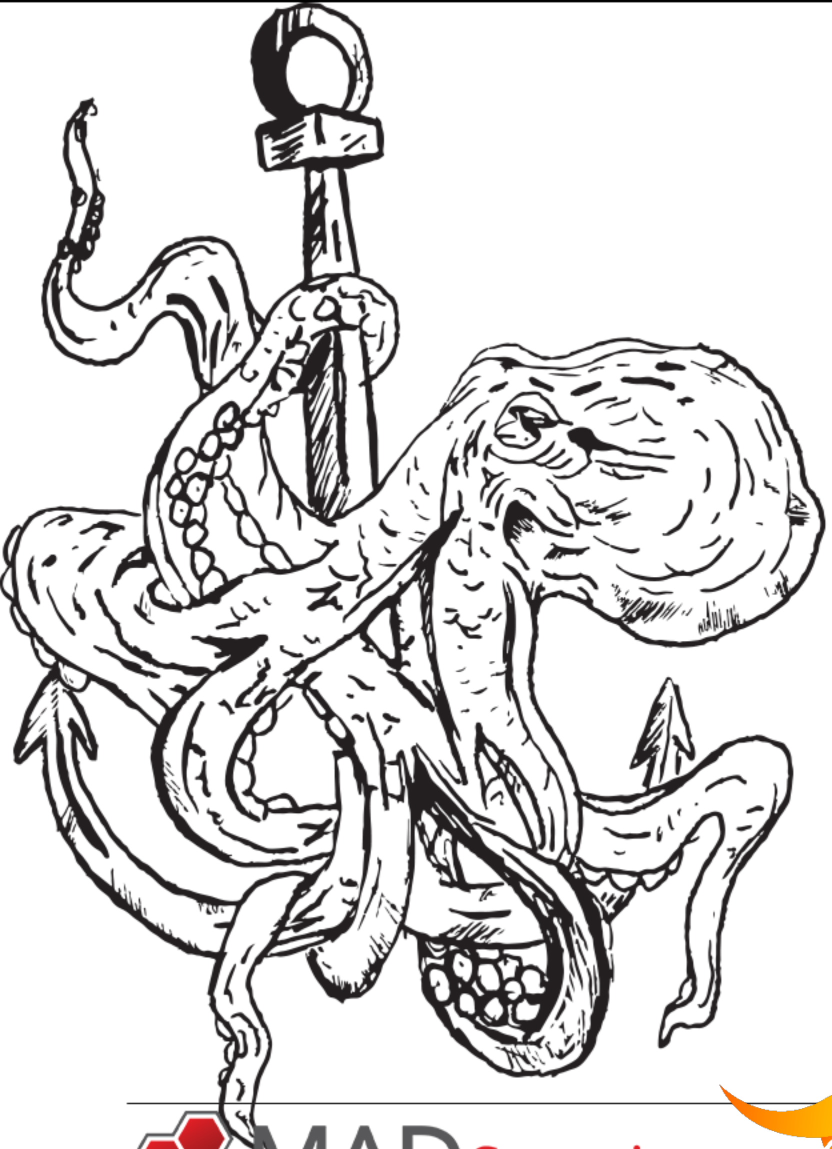
GuROO

888-623-7324 I madmaritime.com

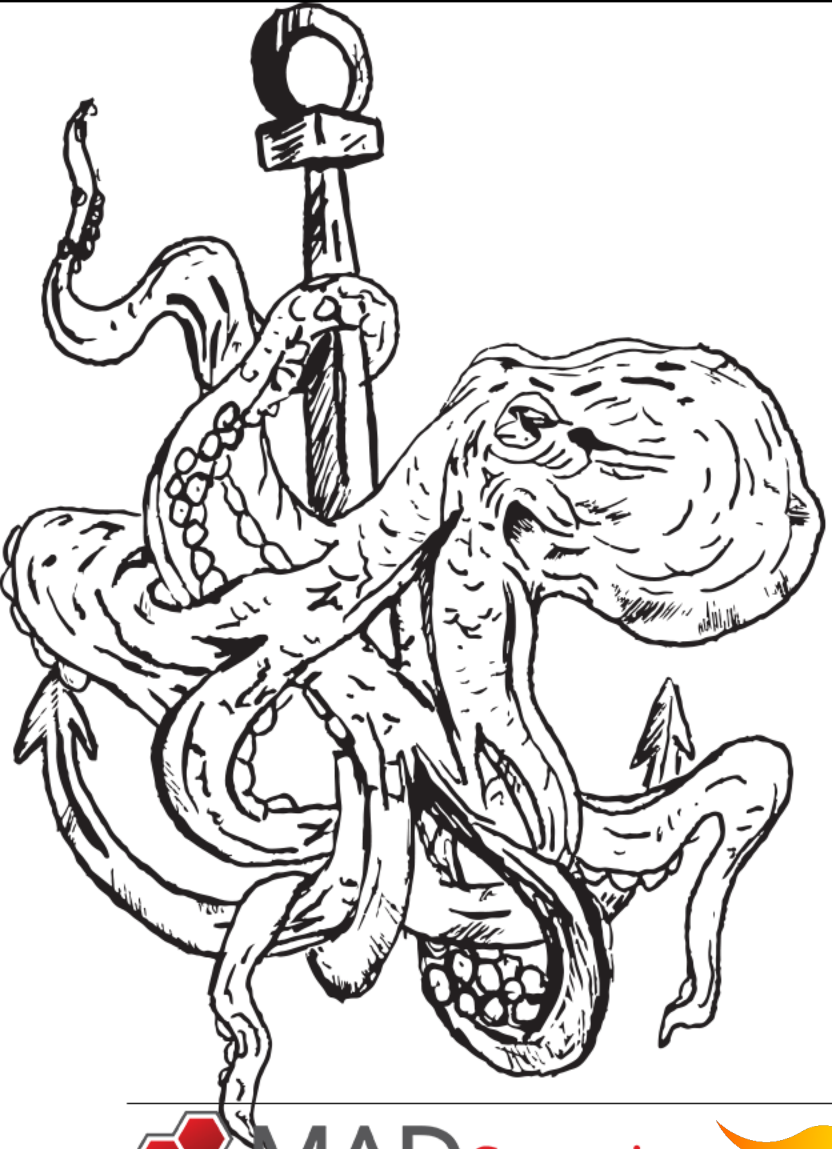

Suppressed
Prior...
Count of Strategy
Alarms Over Time
80
60
40
20
0
5
4
60
1
5
1
1
Total
Suppressed
Count of Intent
Alarms By Priority
Prior...
medium
10
low
64
high
0
10
20
30
40
50
60
70
Total


Suppressed
event.co...
event.action
Count of Strategy
Failed Authentication
host...
10.1.64.171
10.1.64.161
10.1.64.151
1
3
63
0
10
20
30
40
50
60
70
Total

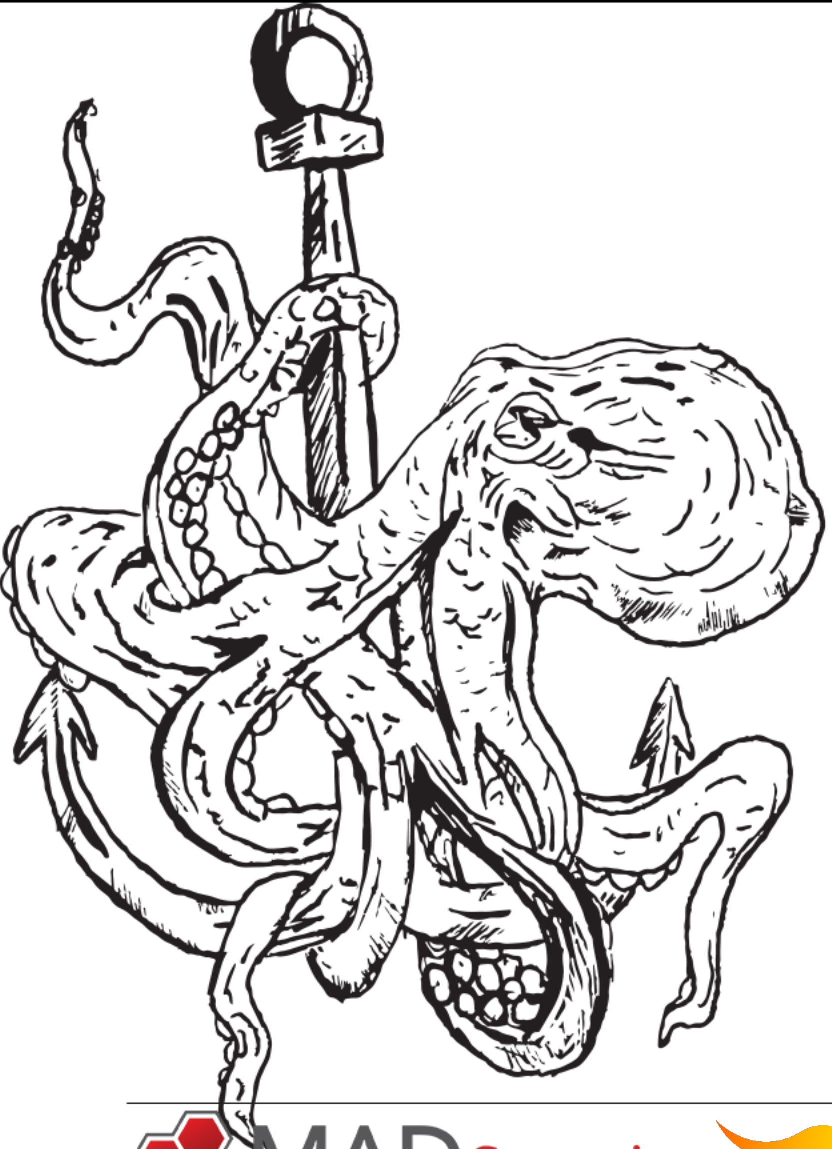

Top 10 Alarms
n Network Connections Discovery
dows Account or Group Discovery
ing Hidden File Attribute via Attrib
irectory Permissions Modification
Signal Alert with Unusual Process Command Line
rol Spawned via Script Interpreter
Windows Event Logs Cleared
Remote Execution via File Shares
or Archived into Common Format
Unusual Windows Username
9
18
6
12
2
3
3
9
4
7
0
2
4
6
8
10
12
14
16
18
20
Total



- **Physical Testing**
- **Config Reviews**
- **Wireless Testing**
- **Pentest**



Changing Requirements



Q and A