

SECURITY AUDIT REPORT

Mediterranean Shipping Company Network Security Assessment

Prepared by: DeepShield Systems, Inc.

Report Date: January 11, 2024

Reference: DSS-MSC-2024-001

1. EXECUTIVE SUMMARY

This report presents the findings and recommendations from the comprehensive security audit conducted by DeepShield Systems, Inc. ("DeepShield") for Mediterranean Shipping Company's ("MSC") operational technology (OT) infrastructure and maritime control systems between November 15, 2023, and December 31, 2023. The audit scope encompassed 47 vessels, 3 major port facilities, and associated SCADA networks.

1.1 Key Findings

- Critical vulnerability identified in legacy ECDIS systems (CVE-2023-7851)
- Non-compliant network segmentation in 28% of assessed vessels
- Outdated firmware in 65% of automated cargo handling systems
- Insufficient endpoint protection on bridge navigation systems

1.2 Risk Assessment Summary

Risk Category	Severity Level	Remediation Priority
OT Network Security	High	Immediate
Access Control Systems	Medium	60 Days
SCADA Infrastructure	High	Immediate
Maritime IoT Devices	Medium	90 Days

2. AUDIT METHODOLOGY

2.1 Assessment Framework

The security audit was conducted using DeepShield's proprietary Maritime Security Assessment Framework (MSAF) v4.2, incorporating:

- IMO Cybersecurity Guidelines (MSC-FAL.1/Circ.3)
- NIST Special Publication 800-82r3
- IEC 62443 Standards
- BIMCO Guidelines on Cyber Security Onboard Ships

2.2 Testing Procedures

- Network architecture review
- Vulnerability scanning using DeepShield MarineGuard(TM) platform
- Penetration testing of critical systems
- Configuration assessment of OT components
- Security policy review and compliance verification

3. DETAILED FINDINGS

3.1 Network Infrastructure

3.1.1 Segmentation Issues

- Insufficient isolation between IT and OT networks
- Non-compliant VLAN configurations
- Inadequate firewall rule sets

3.1.2 Communication Protocols

- Unsecured Modbus TCP traffic
- Legacy serial protocols without encryption
- Unauthorized remote access paths

3.2 Control Systems

3.2.1 ECDIS Vulnerabilities

- CVE-2023-7851: Remote Code Execution vulnerability
- Outdated chart systems lacking security patches
- Unsecured USB ports enabling unauthorized access

3.2.2 Cargo Handling Systems

- Firmware versions 3.2.1 susceptible to buffer overflow

- Unencrypted PLC communications
- Default credentials in use on multiple controllers

4. COMPLIANCE ASSESSMENT

4.1 Regulatory Requirements

Requirement	Status	Gap Analysis
----- ----- -----		
IMO Resolution MSC.428(98)	Partial	Section 5.2
ISPS Code Part A	Compliant	None
EU NIS Directive	Non-Compliant	Section 3.4
TMSA3 Element 13	Partial	Section 2.1

4.2 Industry Standards

Assessment against maritime cybersecurity standards revealed:

- 76% compliance with BIMCO guidelines
- 82% alignment with IACS recommendations
- 64% conformity with OCIMF cybersecurity elements

5. RISK MITIGATION RECOMMENDATIONS

5.1 Immediate Actions (0-30 Days)

Deploy security patches for ECDIS systems (CVE-2023-7851)

Implement network segmentation controls

Update cargo handling system firmware

Enable encrypted communications for all OT protocols

5.2 Short-Term Actions (31-90 Days)

Enhance access control systems

Deploy endpoint protection solutions

Implement secure remote access protocols

Update security policies and procedures

5.3 Long-Term Actions (91-180 Days)

- Establish continuous monitoring program
- Implement automated patch management
- Develop incident response capabilities
- Conduct crew cybersecurity training

6. IMPLEMENTATION PLAN

6.1 Resource Requirements

Component	Estimated Cost	Timeline
-----	-----	-----
Network Security	\$875,000	60 days
System Updates	\$425,000	45 days
Training Program	\$150,000	90 days
Monitoring Solutions	\$650,000	120 days

6.2 Phasing Strategy

- Phase 1: Critical Vulnerabilities
- Phase 2: System Hardening
- Phase 3: Process Implementation
- Phase 4: Training and Awareness

7. DISCLAIMERS AND LIMITATIONS

This report is provided pursuant to the Master Services Agreement dated October 1, 2023, between DeepShield Systems, Inc. and Mediterranean Shipping Company. The findings and recommendations contained herein are based on conditions observed during the audit period and information provided by MSC personnel.

7.1 Confidentiality Notice

This document contains confidential and proprietary information of both DeepShield Systems, Inc. and Mediterranean Shipping Company. Distribution is restricted to authorized personnel only.

7.2 Liability Limitations

DeepShield Systems, Inc. makes no warranties, express or implied, regarding the completeness or accuracy of this assessment. This report represents a point-in-time evaluation and does not guarantee future security performance.

8. CERTIFICATION

This security audit report has been prepared and reviewed by qualified security professionals at DeepShield Systems, Inc.

Prepared by:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Reviewed by:

James Morrison

VP of Engineering

DeepShield Systems, Inc.

Date: January 11, 2024

[END OF REPORT]