MEDITERRANEAN SHIPPING COMPANY SECURITY REVIEW

DeepShield Systems, Inc.

Security Assessment Report

Date: January 11, 2024

Document Reference: DSS-SEC-2024-MSC-001

1. EXECUTIVE SUMMARY

This security review document presents the findings and recommendations from DeepShield Systems, Inc.'s ("DeepShield") comprehensive assessment of Mediterranean Shipping Company's ("MSC") operational technology (OT) infrastructure and maritime control systems. The review was conducted between November 15, 2023, and December 31, 2023, pursuant to Master Services Agreement DSS-MSC-2023-456.

2. SCOPE OF REVIEW

1. Systems Evaluated

- Vessel Control Systems (VCS-2000 Series)
- Terminal Operating Systems (TOS)
- Container Tracking Infrastructure
- Port Facility Access Control Systems
- Maritime SCADA Networks
- Automated Cargo Handling Systems

2. Assessment Methodology

- Deep-layer architecture analysis
- Network penetration testing
- Control system vulnerability assessment
- Protocol security evaluation
- Threat modeling and risk assessment
- Compliance verification against ISPS Code requirements

3. KEY FINDINGS

1. Critical Vulnerabilities

- Three (3) Level 1 vulnerabilities in legacy SCADA systems
- Two (2) Level 2 vulnerabilities in terminal access control
- One (1) Level 1 vulnerability in container tracking protocols

2. System Architecture Concerns

- Outdated firmware in 23% of control systems
- Non-segmented networks in 3 terminal locations
- Insufficient encryption protocols for vessel-to-shore communications
- Legacy authentication mechanisms in cargo handling systems

3. Compliance Status

- 87% alignment with ISPS Code requirements
- 92% compliance with IMO cybersecurity guidelines
- 76% adherence to IEC 62443 standards

4. REMEDIATION RECOMMENDATIONS

1. Immediate Actions Required

a) Implementation of deep-layer security architecture

b) Network segmentation deployment

c) Control system firmware updates

d) Enhanced encryption protocol deployment

2. Short-Term Priorities (90 Days)

a) Authentication system modernization

b) SCADA network hardening

c) Access control system upgrades

d) Security monitoring enhancement

3. Long-Term Initiatives (12 Months)

a) Full OT infrastructure modernization

b) Integrated security operations center deployment

c) Advanced threat detection implementation

d) Automated incident response capabilities

5. IMPLEMENTATION PLAN

1. Phase I - Critical Security Enhancement

- Timeline: February 1, 2024 - April 30, 2024
- Budget Estimate: $2,750,000
- Resource Requirements: 3 Security Engineers, 2 OT Specialists

2. Phase II - System Modernization

- Timeline: May 1, 2024 - October 31, 2024
- Budget Estimate: $4,200,000
- Resource Requirements: 4 Integration Specialists, 3 Security Architects

6. RISK ASSESSMENT

1. Current Risk Profile

- High-risk areas: 3
- Medium-risk areas: 7
- Low-risk areas: 12

2. Post-Implementation Risk Profile

- High-risk areas: 0
- Medium-risk areas: 3
- Low-risk areas: 19

7. LEGAL DISCLAIMERS

This security review document is confidential and proprietary to DeepShield Systems, Inc. The information contained herein is provided pursuant to the confidentiality provisions of the Master Services Agreement between DeepShield and Mediterranean Shipping Company dated October 1, 2023.

This assessment represents findings as of the review period and does not guarantee future security status. DeepShield makes no warranties, express or implied, regarding the security of systems following implementation of recommended measures.

8. AUTHORIZATION

REVIEWED AND APPROVED BY:

_

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: January 11, 2024

_

James Morrison

VP of Engineering

DeepShield Systems, Inc.

Date: January 11, 2024

9. DISTRIBUTION RESTRICTIONS

This document is classified as CONFIDENTIAL and shall be distributed only to authorized personnel on a need-to-know basis. Any unauthorized disclosure, copying, or distribution is strictly prohibited and may result in civil and criminal penalties.

[END OF DOCUMENT]