Maritime Cybersecurity Assessment Report

Maersk Line Q4 2022

Prepared by DeepShield Systems, Inc.

Report Date: December 15, 2022

Reference: DSS-MA-2022-Q4-001

1. Executive Summary

This Maritime Cybersecurity Assessment Report ("Assessment") has been prepared by DeepShield Systems, Inc. ("DeepShield") for A.P. Moller-Maersk ("Maersk Line") pursuant to Service Agreement DSS-2022-103 dated January 15, 2022. The Assessment evaluates cybersecurity controls and vulnerabilities across Maersk Line's maritime operations infrastructure for Q4 2022.

2. Assessment Scope

1. Systems Evaluated

- Vessel Operations Technology (OT) Networks
- Bridge Navigation Systems
- Cargo Management Systems
- Engine Control and Monitoring Systems
- Satellite Communications Infrastructure
- Shore-based Support Systems

2. Assessment Period

October 1, 2022 through December 31, 2022

3. Geographic Coverage

Global fleet operations across 12 major maritime routes

3. Methodology

1. Assessment Framework

This evaluation follows the NIST Cybersecurity Framework (CSF) and incorporates maritime-specific controls from:

- IEC 61162-460:2018 Maritime Navigation Standards
- BIMCO Guidelines on Cyber Security Onboard Ships v4.0
- IMO Resolution MSC.428(98) Maritime Cyber Risk Management

2. Testing Protocols

- Network Architecture Review
- Control System Configuration Analysis
- Vulnerability Scanning
- Penetration Testing
- Security Control Validation
- Incident Response Capability Assessment

4. Key Findings

1. Critical Vulnerabilities

Three (3) critical vulnerabilities were identified:

- CVE-2022-28456: Remote Code Execution in Bridge Navigation System
- CVE-2022-30121: Authentication Bypass in Cargo Management Interface
- CVE-2022-35789: Buffer Overflow in Engine Monitoring System

2. High-Risk Areas

- Outdated firmware versions on 23% of networked navigation equipment
- Insufficient network segmentation between OT and IT systems
- Legacy authentication protocols in use on satellite communication systems
- Inadequate backup systems for critical navigation data

3. Compliance Status

- IMO Cyber Risk Management: 87% compliant
- BIMCO Guidelines: 92% compliant
- IEC Standards: 85% compliant

5. Recommendations

1. Immediate Actions Required

- Patch critical vulnerabilities within 30 days
- Implement network segmentation controls
- Update authentication protocols
- Deploy automated backup systems

2. Short-Term Improvements (90 Days)

- Upgrade firmware on navigation equipment
- Enhance monitoring capabilities
- Implement additional access controls
- Strengthen incident response procedures

3. Long-Term Strategy

- Develop comprehensive OT security architecture
- Establish continuous monitoring program
- Implement AI-driven threat detection
- Deploy automated incident response capabilities

6. Risk Matrix

1. Current Risk Profile

- Critical: 3 findings
- High: 7 findings
- Medium: 12 findings
- Low: 8 findings

2. Projected Risk Profile (Post-Remediation)

- Critical: 0 findings
- High: 2 findings
- Medium: 8 findings
- Low: 20 findings

7. Limitations and Disclaimers

This Assessment represents DeepShield's professional opinion based on information available during the assessment period. DeepShield makes no warranties, express or implied, regarding the security of assessed systems. This report is provided for informational purposes only and should not be considered a guarantee of security.

8. Confidentiality

This document contains confidential and proprietary information belonging to both DeepShield Systems, Inc. and A.P. Moller-Maersk. Distribution is restricted to authorized personnel only.

9. Authentication

PREPARED BY:

DeepShield Systems, Inc.

By: _

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: December 15, 2022

REVIEWED BY:

DeepShield Systems, Inc.

By: _

Name: James Morrison

Title: VP of Engineering

Date: December 15, 2022

10. Document Control

Document ID: DSS-MA-2022-Q4-001

Version: 1.0

Classification: Confidential

Distribution: Restricted