GREEK SHIPPING TERMINAL ASSESSMENT REPORT

DeepShield Systems, Inc.

CONFIDENTIAL AND PRIVILEGED

Date: January 11, 2024

1. EXECUTIVE SUMMARY

This report presents findings from the technical assessment of cybersecurity vulnerabilities and operational technology (OT) infrastructure at the Piraeus Container Terminal (PCT) conducted by DeepShield Systems, Inc. ("DeepShield") between November 15-30, 2023. The assessment was performed pursuant to Service Order #GR-2023-456 under Master Services Agreement dated September 1, 2023.

2. SCOPE OF ASSESSMENT

1. **Physical Infrastructure Evaluated**

- Main terminal control center
- Four container berths (Berths 12-15)
- Automated crane systems (8 units)
- Terminal operating system (TOS) infrastructure
- SCADA control networks
- Vessel traffic management system
- Gate automation systems

2. **Systems Analysis Coverage**

- Industrial control system (ICS) architecture
- OT network segmentation
- SCADA system vulnerabilities
- Maritime automation protocols
- Legacy system interfaces
- Emergency shutdown systems
- Remote access points

3. METHODOLOGY

1. **Assessment Protocols**

- DeepShield Maritime Infrastructure Security Framework v4.2
- IEC 62443 Industrial Network Security Standards
- NIST SP 800-82 Guide to ICS Security
- ENISA Port Cybersecurity Guidelines

2. **Testing Procedures**

- Passive network monitoring
- Control system architecture review
- Protocol analysis
- Vulnerability scanning (authorized)
- Configuration assessment
- Access control evaluation
- Incident response capability testing

4. KEY FINDINGS

1. **Critical Vulnerabilities**

- Unpatched legacy SCADA systems (3 instances)
- Insufficient network segmentation between IT/OT
- Outdated firmware in crane automation controllers
- Unsecured remote access pathways
- Non-compliant password policies
- Absence of encrypted protocols for critical commands

2. **Operational Risks**

- Single point of failure in terminal operating system
- Limited redundancy in control network
- Inadequate backup power systems
- Incomplete disaster recovery procedures
- Insufficient change management controls
- Vulnerable vendor remote access

5. TECHNICAL ANALYSIS

1. **Network Architecture**

The terminal's OT infrastructure operates on a partially segmented network with insufficient isolation between critical control systems and administrative networks. Legacy protocols (Modbus TCP, EtherNet/IP) lack proper encryption and authentication mechanisms.

2. **Control Systems**

Crane automation systems utilize outdated firmware versions (v3.2.14) with known vulnerabilities (CVE-2023-XXXX). Terminal Operating System runs on unsupported database version with limited security patches.

3. **Security Controls**

Current implementation lacks:

- Multi-factor authentication for critical systems
- Real-time threat monitoring
- Automated incident response
- Comprehensive audit logging
- Network traffic analysis
- Asset inventory management

6. RECOMMENDATIONS

1. **Immediate Actions Required**

Implement network segmentation using industrial firewalls

Update crane automation firmware to version 4.1.8

Deploy multi-factor authentication

Establish encrypted communication protocols

Install DeepShield OT monitoring solution

2. **Short-term Improvements (90 days)**

Upgrade SCADA system software

Implement comprehensive backup solutions

Deploy industrial DMZ architecture

Enhance access control systems

Establish security incident response procedures

3. **Long-term Strategy**

Modernize control system architecture

Implement redundant control networks

Deploy advanced threat detection

Establish security operations center

Develop comprehensive disaster recovery plan

7. IMPLEMENTATION TIMELINE

1. **Phase 1: Critical Remediation** (30 days)

- Network segmentation
- Firmware updates
- Authentication enhancement
- Protocol encryption

2. **Phase 2: System Hardening** (90 days)

- SCADA upgrades
- Backup implementation
- DMZ deployment
- Access control enhancement

3. **Phase 3: Advanced Security** (180 days)

- Architecture modernization
- Redundancy implementation
- SOC establishment
- DR planning

8. LEGAL DISCLAIMERS

This assessment report is provided pursuant to the terms and conditions of the Master Services Agreement. The information contained herein is confidential and proprietary to DeepShield Systems, Inc. This report represents findings as of the assessment date and does not guarantee future security performance. DeepShield makes no warranties, express or implied, regarding the completeness or accuracy of this assessment.

9. CERTIFICATION

This report has been prepared and reviewed by qualified DeepShield security professionals in accordance with industry standards and best practices.

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]