PORT FACILITY SECURITY ASSESSMENT METHODOLOGY

DeepShield Systems, Inc.

Document No. SEC-PRT-2023-014

Version 2.1 - January 2024

1. PURPOSE AND SCOPE

1. This methodology document establishes the standardized procedures and protocols for conducting comprehensive security assessments of maritime port facilities utilizing DeepShield Systems' integrated industrial cybersecurity platform and associated technologies.

2. This methodology applies to all security assessments conducted by DeepShield Systems personnel or authorized partners at maritime port facilities, including container terminals, bulk cargo facilities, passenger terminals, and associated operational technology (OT) infrastructure.

2. DEFINITIONS

1. "Critical Assets" means vital operational systems, including but not limited to:

a) Terminal Operating Systems (TOS)

b) Vessel Traffic Management Systems (VTMS)

c) Automated Gate Systems

d) Crane Control Systems

e) SCADA Networks

f) Physical Access Control Systems

2. "Security Zone" means a defined area within the port facility requiring specific security controls and monitoring protocols.

3. "Threat Vector" means any potential path or means by which an unauthorized entity could compromise facility security.

3. ASSESSMENT METHODOLOGY

1. Pre-Assessment Phase

a) Document review of existing security protocols

b) Stakeholder interviews and operational workflow analysis

c) Network architecture review and system inventory

d) Regulatory compliance status evaluation

2. Technical Assessment Phase

a) OT Network Vulnerability Scanning using DeepShield's proprietary tools

b) Control System Security Analysis

c) Communications Infrastructure Assessment

d) Physical Security Control Evaluation

e) Human Factors and Access Control Review

3. Risk Analysis Phase

a) Threat Modeling and Impact Analysis

b) Vulnerability Scoring and Prioritization

c) Control Gap Analysis

d) Risk Matrix Development

4. ASSESSMENT PROCEDURES

1. Network Security Assessment

a) Passive network monitoring using DeepShield's Deep-Layer Protocol Analysis

b) Industrial protocol security verification

c) Network segmentation validation

d) Wireless security assessment

e) Remote access control evaluation

2. Physical Security Integration

a) Access control system testing

b) Video surveillance system assessment

c) Perimeter security evaluation

d) Integration with cybersecurity controls

3. Operational Technology Assessment

a) SCADA system security analysis

b) PLC/RTU security evaluation

c) Industrial network protocol analysis

d) Control system vulnerability assessment

5. REPORTING AND DOCUMENTATION

1. Assessment Documentation Requirements

a) Detailed findings report

b) Risk assessment matrix

c) Remediation recommendations

d) Technical appendices

e) Executive summary

2. Confidentiality Requirements

a) All assessment findings shall be treated as Confidential Information

b) Distribution limited to authorized personnel only

c) Secure storage and transmission protocols

6. QUALITY ASSURANCE

1. Assessment Team Requirements

a) Minimum certification requirements

b) Experience qualifications

c) Ongoing training requirements

2. Quality Control Procedures

a) Peer review requirements

b) Technical validation protocols

c) Documentation standards

7. COMPLIANCE AND STANDARDS

1. Regulatory Compliance

a) MTSA requirements

b) ISPS Code compliance

c) Local port authority regulations

d) Industry best practices

2. Technical Standards

a) IEC 62443

b) NIST Cybersecurity Framework

c) ISO 27001

d) ANSI/ISA 99

8. PROPRIETARY RIGHTS AND CONFIDENTIALITY

1. All assessment methodologies, tools, and procedures described herein are the exclusive property of DeepShield Systems, Inc. and are protected by applicable intellectual property laws.

2. This document contains confidential and proprietary information and shall not be disclosed to third parties without written authorization from DeepShield Systems, Inc.

9. REVISION AND CONTROL

1. This methodology shall be reviewed annually and updated as necessary to reflect evolving security threats and technological capabilities.

2. All revisions must be approved by DeepShield's Chief Security Architect and documented in the version control system.

APPROVAL AND EXECUTION

APPROVED AND ADOPTED this 11th day of January, 2024.

DEEPSHIELD SYSTEMS, INC.

By:

Dr. Elena Rodriguez

Chief Security Architect

By:

James Morrison

VP of Engineering