VULNERABILITY ASSESSMENT FRAMEWORK - MARITIME

DeepShield Systems, Inc.

Document Version: 2.4

Effective Date: January 15, 2024

Classification: Confidential

1. PURPOSE AND SCOPE

1. This Vulnerability Assessment Framework ("Framework") establishes the standardized methodology and procedures for conducting security vulnerability assessments of maritime facilities, vessels, and associated operational technology (OT) infrastructure protected by DeepShield Systems, Inc. ("DeepShield") solutions.

2. This Framework applies to all vulnerability assessments conducted by DeepShield personnel or authorized contractors on maritime assets including, but not limited to:

a) Port facilities and terminals

b) Commercial vessels and shipping operations

c) Offshore platforms and installations

d) Maritime control systems and SCADA networks

e) Subsea infrastructure and communications systems

2. DEFINITIONS

1. "Assessment Team" means the designated DeepShield personnel responsible for executing the vulnerability assessment.

2. "Critical Maritime Assets" means any operational technology, control systems, or physical infrastructure essential to maritime operations.

3. "Maritime Facility" means any port, terminal, vessel, or offshore installation subject to assessment under this Framework.

4. "Security Controls" means the collective safeguards and countermeasures implemented to protect maritime assets.

3. ASSESSMENT METHODOLOGY

1. Pre-Assessment Phase

a) Document review of facility security plans and procedures

b) Analysis of historical incident data and threat intelligence

c) Identification of critical systems and assets

d) Development of assessment scope and objectives

e) Coordination with facility operators and stakeholders

2. Technical Assessment Components

a) Network architecture review and analysis

b) Control system configuration assessment

c) Communications protocol security evaluation

d) Physical security control verification

e) Access control system testing

f) Emergency response capability assessment

3. Vulnerability Classification

a) Critical (Score 9-10): Immediate remediation required

b) High (Score 7-8): Remediation within 30 days

c) Medium (Score 4-6): Remediation within 90 days

d) Low (Score 1-3): Remediation at next maintenance interval

4. ASSESSMENT PROCEDURES

1. The Assessment Team shall:

a) Conduct initial briefing with facility management

b) Execute technical testing according to approved scope

c) Document all findings in the prescribed format

d) Maintain chain of custody for all assessment data

e) Prepare detailed assessment reports

2. Required Assessment Areas

a) Physical security controls and barriers

b) Access control systems and procedures

c) Network segmentation and security

d) Industrial control system security

e) Communications security

f) Emergency response capabilities

g) Security awareness and training

5. REPORTING AND DOCUMENTATION

1. Assessment Reports shall include:

a) Executive summary

b) Detailed findings and vulnerability scores

c) Supporting evidence and technical data

d) Recommended remediation measures

e) Implementation priorities and timelines

2. All assessment documentation must be:

a) Marked as Confidential

b) Stored in DeepShield's secure document repository

c) Accessible only to authorized personnel

d) Retained for a minimum of seven (7) years

6. CONFIDENTIALITY AND SECURITY

1. All information obtained during assessments shall be treated as confidential and protected according to DeepShield's Information Security Policy.

2. Assessment Team members must:

a) Sign non-disclosure agreements

b) Maintain current security clearances

c) Complete required training certifications

d) Follow all facility security protocols

7. COMPLIANCE AND REVIEW

1. This Framework shall be reviewed annually and updated as necessary to maintain alignment with:

a) Industry standards and best practices

b) Regulatory requirements

c) Emerging threats and vulnerabilities

d) Technology advances

2. Compliance with this Framework is mandatory for all vulnerability assessments conducted by DeepShield.

8. AUTHORIZATION

This Framework is authorized and approved by:

Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: January 15, 2024