SECURITY RISK ASSESSMENT METHODOLOGY

DeepShield Systems, Inc.

Effective Date: January 1, 2024

Document Version: 2.4

Classification: Confidential

1. PURPOSE AND SCOPE

1. This Security Risk Assessment Methodology ("Methodology") establishes the standardized framework and procedures for conducting security risk assessments of industrial control systems (ICS), operational technology (OT) environments, and critical infrastructure protected by DeepShield Systems, Inc. ("DeepShield" or the "Company").

2. This Methodology applies to all security assessments conducted by DeepShield personnel, contractors, and authorized third-party assessors evaluating client infrastructure security posture.

2. DEFINITIONS

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

2. "Critical Assets" means the essential systems, networks, and infrastructure components necessary for maintaining operational continuity.

3. "Risk Rating" means the calculated severity level assigned to identified vulnerabilities based on the Company's proprietary scoring matrix.

4. "Target Environment" means the client's industrial control systems, OT networks, and associated infrastructure subject to assessment.

3. ASSESSMENT METHODOLOGY

1. **Pre-Assessment Phase**

a) Documentation Review

- Collect and analyze system architecture diagrams
- Review existing security policies and procedures

- Evaluate incident response protocols
- Examine maintenance and change management records

b) Scope Definition

- Identify critical assets and systems for evaluation
- Define assessment boundaries and exclusions
- Document regulatory compliance requirements
- Establish assessment timeline and milestones

2. **Technical Assessment Phase**

a) Network Security Analysis

- Conduct passive network monitoring
- Perform authorized vulnerability scanning
- Evaluate network segmentation effectiveness
- Assess remote access controls

b) Control System Security

- Review ICS configuration standards
- Evaluate automation system security
- Assess SCADA network protection
- Validate safety system isolation

3. **Risk Analysis Phase**

a) Vulnerability Classification

- Categorize identified vulnerabilities
- Apply DeepShield Risk Rating Matrix
- Determine exploitation potential
- Assess business impact scenarios

b) Threat Modeling

- Identify relevant threat actors
- Evaluate attack vectors
- Assess threat capability requirements

- Document attack path analysis

4. REPORTING AND DOCUMENTATION

1. The Assessment Team shall prepare the following deliverables:

a) Executive Summary Report

b) Detailed Technical Findings

c) Risk Rating Matrix Results

d) Remediation Recommendations

e) Implementation Roadmap

2. All assessment documentation must be maintained in accordance with DeepShield's Information Classification Policy.

5. QUALITY ASSURANCE

1. All security assessments must be reviewed and validated by a DeepShield Senior Security Architect prior to client delivery.

2. Assessment methodologies shall be updated annually to incorporate emerging threats and industry best practices.

6. CONFIDENTIALITY

1. All information obtained during security assessments shall be treated as strictly confidential and subject to applicable non-disclosure agreements.

2. Assessment results shall only be shared with authorized client personnel designated in the engagement scope.

7. COMPLIANCE AND STANDARDS

1. This Methodology adheres to:

a) NIST SP 800-82r3 Guidelines

b) ISA/IEC 62443 Standards

c) Maritime cybersecurity requirements (BIMCO)

d) Relevant regulatory frameworks

8. LIMITATIONS AND DISCLAIMERS

1. This Methodology provides a framework for security assessment but does not guarantee the identification of all possible vulnerabilities or security risks.

2. Assessment results represent a point-in-time evaluation and should be regularly updated.

9. REVISION HISTORY

Version 2.4 - January 1, 2024

- Updated risk rating matrix
- Added maritime-specific controls
- Enhanced OT network assessment procedures

Version 2.3 - June 15, 2023

- Incorporated AI-driven threat detection protocols
- Updated compliance requirements

10. APPROVAL AND AUTHORIZATION

This Methodology is approved and authorized by:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: _