OT/IT CONVERGENCE SECURITY FRAMEWORK DOCUMENTATION

DeepShield Systems, Inc.

Document Version: 2.4

Last Updated: January 11, 2024

Classification: CONFIDENTIAL

1. FRAMEWORK OVERVIEW AND SCOPE

1. This OT/IT Convergence Security Framework Documentation ("Framework") establishes the governing principles, architectural requirements, and implementation standards for DeepShield Systems, Inc.'s ("Company") integrated operational technology (OT) and information technology (IT) security infrastructure.

2. This Framework applies to all Company products, services, and internal systems that facilitate the convergence of OT and IT environments, including but not limited to:

a) DeepShield Maritime Protection Platform(TM)

b) Industrial Control System (ICS) Security Suite

c) SCADA Network Defense Architecture

d) Subsea Infrastructure Protection Modules

2. DEFINITIONS

1. "OT Systems" refers to hardware and software that monitors or controls physical devices, processes, and events in industrial environments.

2. "IT Systems" refers to traditional information processing systems, networks, and applications used for data-centric computing.

3. "Convergence Points" refers to technological intersections where OT and IT systems interface, communicate, or share data.

4. "Security Controls" refers to safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

3. ARCHITECTURAL REQUIREMENTS

1. Segmentation and Isolation

a) Physical and logical separation of OT and IT networks

b) Dedicated security zones for critical control systems

c) Air-gapped environments for highest-risk operations

d) Monitored and controlled interconnection points

2. Authentication and Access Control

a) Role-based access control (RBAC) implementation

b) Multi-factor authentication for all privileged access

c) Separate authentication domains for OT and IT systems

d) Privileged Access Management (PAM) integration

3. Communication Security

a) Encrypted protocols for all cross-domain communication

b) Dedicated VPN infrastructure for remote access

c) Protocol-specific security controls for industrial protocols

d) Real-time traffic monitoring and analysis

4. SECURITY CONTROLS AND MONITORING

1. The Company shall maintain the following minimum security controls:

a) Network-level intrusion detection and prevention

b) Asset inventory and configuration management

c) Vulnerability assessment and management

d) Security information and event management (SIEM)

e) Automated incident response capabilities

f) Continuous security monitoring

2. All security controls shall be tested quarterly and validated annually by independent third-party assessors.

5. COMPLIANCE AND STANDARDS

1. This Framework adheres to and incorporates requirements from:

a) IEC 62443 Industrial Automation and Control Systems Security

b) NIST SP 800-82 Guide to Industrial Control Systems Security

c) ISO/IEC 27001:2013 Information Security Management

d) Maritime cybersecurity guidelines (BIMCO, IMO)

2. Annual compliance assessments shall be conducted and documented.

6. INCIDENT RESPONSE AND RECOVERY

1. The Company shall maintain documented procedures for:

a) Security incident detection and classification

b) Incident response and containment

c) System recovery and business continuity

d) Post-incident analysis and reporting

2. Incident response procedures shall be tested semi-annually through tabletop exercises and technical simulations.

7. PROPRIETARY RIGHTS AND CONFIDENTIALITY

1. This Framework and all associated documentation constitute confidential and proprietary information of the Company.

2. No part of this Framework may be disclosed, copied, or distributed without prior written authorization from the Company's Chief Security Architect or General Counsel.

8. AMENDMENTS AND UPDATES

1. This Framework shall be reviewed and updated annually or upon significant changes to:

a) Regulatory requirements

b) Threat landscape

c) Technology infrastructure

d) Business operations

2. All updates shall be approved by the Security Architecture Review Board.

9. EXECUTION AND APPROVAL

IN WITNESS WHEREOF, this Framework has been reviewed and approved by the undersigned authorized representatives of the Company.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: January 11, 2024

By:

Name: Sarah Blackwood

Title: Chief Technology Officer

Date: January 11, 2024