CONTROL SYSTEMS SECURITY PROGRAM DOCUMENTATION

DeepShield Systems, Inc.

Last Updated: January 11, 2024

Document Version: 3.2

Classification: CONFIDENTIAL

1. PROGRAM OVERVIEW

1. This Control Systems Security Program Documentation ("Program Documentation") establishes the comprehensive framework for protecting industrial control systems (ICS), operational technology (OT), and critical infrastructure assets under DeepShield Systems, Inc.'s ("Company") security architecture.

2. This Program Documentation is maintained pursuant to NIST SP 800-82, IEC 62443, and relevant industry standards for industrial cybersecurity controls.

2. DEFINITIONS

1. "Control Systems" means all industrial automation systems, SCADA networks, programmable logic controllers (PLCs), and associated operational technology managed or protected by the Company.

2. "Deep-Layer Architecture" means the Company's proprietary multi-tiered security framework incorporating AI-driven threat detection, behavioral analysis, and automated response capabilities.

3. "Security Events" means any detected or suspected security incidents, anomalies, or unauthorized access attempts affecting protected Control Systems.

3. SECURITY ARCHITECTURE

1. **Core Components**

- Deep-Layer Network Monitoring System v4.2
- Adaptive Defense Engine v3.7
- Maritime Operations Security Module v2.1
- Subsea Infrastructure Protection Framework v1.8
- Real-Time Analytics Platform v3.5

2. **Security Zones**

The Program implements ISO/IEC 62443-3-2 security zones including:

- Level 0: Field Devices
- Level 1: Control Systems
- Level 2: Supervisory Systems
- Level 3: Operations Management
- Level 4: Enterprise Systems

4. SECURITY CONTROLS

1. **Access Control**

- Multi-factor authentication for all control system access
- Role-based access control (RBAC) with principle of least privilege
- Secure remote access protocols with session monitoring
- Automated access revocation procedures

2. **Network Security**

- Segmented OT networks with managed interfaces
- Deep packet inspection for industrial protocols
- Encrypted communications for remote operations
- Real-time traffic analysis and anomaly detection

3. **System Hardening**

- Baseline security configurations for all control system components
- Regular vulnerability assessments and penetration testing
- Patch management procedures for OT environments
- Secure system backup and recovery protocols

5. INCIDENT RESPONSE

1. **Detection & Analysis**

- Continuous monitoring of control system operations
- AI-driven anomaly detection and threat classification
- Automated correlation of security events

- Real-time alert generation and escalation

2. **Response Procedures**

- Defined incident classification matrix
- Automated containment procedures
- Manual override capabilities for critical systems
- Incident documentation and forensics protocols

3. **Recovery Operations**

- System restoration procedures
- Business continuity integration
- Post-incident analysis requirements
- Lessons learned documentation

6. COMPLIANCE & AUDIT

1. The Program shall be reviewed annually by the Chief Security Architect and updated as necessary to maintain alignment with:

- NIST Cybersecurity Framework
- IEC 62443 Standards
- Maritime cybersecurity regulations
- Industry-specific compliance requirements

2. Internal audits shall be conducted quarterly with results reported to the Security Operations Committee.

7. TRAINING & AWARENESS

1. All personnel with access to Control Systems shall complete:

- Initial security awareness training
- Annual refresher courses
- Role-specific technical training
- Incident response drills

8. PROGRAM MAINTENANCE

1. This Program Documentation shall be maintained by the Security Operations team under supervision of the Chief Security Architect.

2. Updates require approval from:

- Chief Technology Officer
- VP of Engineering
- Chief Security Architect
- Compliance Officer

9. CONFIDENTIALITY

1. This Program Documentation contains confidential and proprietary information of DeepShield Systems, Inc. Unauthorized disclosure is strictly prohibited.

APPROVALS

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

DEEPSHIELD SYSTEMS, INC.

By:

Dr. Elena Rodriguez

Chief Security Architect

By:

Sarah Blackwood

Chief Technology Officer

By:

James Morrison

VP of Engineering