OT/IT CONVERGENCE SECURITY STANDARDS

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 3.2

Classification: Confidential

1. PURPOSE AND SCOPE

1. This document establishes mandatory security standards governing the convergence of Operational Technology (OT) and Information Technology (IT) systems within DeepShield Systems, Inc. ("Company") and its client implementations.

2. These standards apply to all Company employees, contractors, and third-party integrators involved in the design, implementation, maintenance, or operation of integrated OT/IT environments.

2. DEFINITIONS

1. "Operational Technology (OT)" refers to hardware and software systems that monitor and control physical devices, processes, and events within industrial environments.

2. "Information Technology (IT)" encompasses systems for storing, retrieving, and sending information, including enterprise networks, databases, and business applications.

3. "Convergence Zone" defines any area where OT and IT systems interface, integrate, or share data.

4. "Deep-Layer Architecture" refers to Company's proprietary multi-tiered security framework for protecting industrial control systems.

3. ARCHITECTURAL REQUIREMENTS

1. Segmentation and Isolation

1.1. Physical and logical separation must be maintained between OT and IT networks using Company's Deep-Layer Architecture.

1.2. Data exchange between OT and IT systems shall occur only through approved secure gateways implementing protocol-specific security controls.

2. Access Control

2.1. Implementation of role-based access control (RBAC) with principle of least privilege.

2.2. Multi-factor authentication required for all administrative access to convergence zones.

2.3. Separate authentication domains for OT and IT systems with controlled trust relationships.

4. SECURITY CONTROLS

1. Network Security

1.1. Industrial firewalls must be deployed at all OT/IT boundaries.

1.2. Network traffic monitoring using Company's AI-driven anomaly detection.

1.3. Encrypted communications for all cross-domain data transfers.

2. System Hardening

2.1. Regular vulnerability assessments of both OT and IT components.

2.2. Security patch management coordinated between OT and IT systems.

2.3. Removal or secure configuration of unnecessary services and ports.

5. MONITORING AND INCIDENT RESPONSE

1. Continuous Monitoring

1.1. Real-time monitoring of all convergence points using Company's proprietary sensors.

1.2. Automated asset discovery and inventory maintenance.

1.3. Performance impact monitoring of security controls.

2. Incident Response

2.1. Dedicated OT/IT incident response team and procedures.

2.2. Automated containment measures for detected threats.

2.3. Regular testing of recovery procedures.

6. COMPLIANCE AND AUDIT

1. Documentation Requirements

1.1. Maintenance of current network architecture diagrams.

1.2. Regular review and updates of security policies.

1.3. Change management documentation for all modifications.

2. Audit Procedures

2.1. Quarterly internal security audits of convergence zones.

2.2. Annual third-party assessment of OT/IT security controls.

2.3. Continuous compliance monitoring with applicable standards.

7. TRAINING AND AWARENESS

1. All personnel with access to convergence zones must complete Company's OT/IT security training program annually.

2. Role-specific training required for administrators and security personnel.

3. Regular security awareness updates regarding emerging threats.

8. EXCEPTIONS AND DEVIATIONS

1. Exceptions to these standards must be documented and approved by the Chief Security Architect.

2. Temporary deviations require compensating controls and time-limited approvals.

9. REVIEW AND UPDATES

1. These standards shall be reviewed and updated annually or upon significant changes to the threat landscape.

2. Updates require approval from the Security Standards Committee.

AUTHORIZATION

These standards are hereby authorized and enacted by:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: _

DOCUMENT CONTROL

Version: 3.2

Last Review: January 15, 2024

Next Review: January 15, 2025

Document Owner: Security Standards Committee

Classification: Confidential