Network Segmentation Implementation Guide

DeepShield Systems, Inc.

Document Version: 2.0

Effective Date: January 15, 2024

Classification: Confidential & Proprietary

1. Purpose and Scope

1. This Network Segmentation Implementation Guide ("Guide") establishes the mandatory requirements and procedures for implementing network segmentation across DeepShield Systems, Inc.'s ("Company") industrial control system (ICS) environments and client deployments.

2. This Guide applies to all Company employees, contractors, and authorized third parties involved in the implementation, maintenance, or modification of network segmentation controls within operational technology (OT) environments.

2. Definitions

1. "DMZ" means demilitarized zone, a physical or logical subnetwork that contains and exposes external-facing services to untrusted networks.

2. "ICS" means Industrial Control Systems, including SCADA systems, distributed control systems (DCS), and other control system configurations.

3. "Network Zones" means logical groupings of network assets with similar security requirements and trust levels.

4. "Security Perimeter" means the boundary between network zones with different security levels.

3. Network Zone Classification

1. Level 0 - Field Devices

- Direct process control
- Physical input/output devices
- No remote access permitted

2. Level 1 - Control Systems

- PLCs, RTUs, IEDs
- Basic control logic
- Restricted protocol usage

3. Level 2 - Supervisory Control
- HMI systems
- SCADA servers
- Engineering workstations

4. Level 3 - Operations Management
- Manufacturing execution systems
- Historian servers
- Production scheduling

5. Level 4 - Enterprise Network
- Business logistics systems
- Corporate IT infrastructure
- External connectivity

4. Segmentation Requirements

1. Physical Separation
- Dedicated hardware infrastructure for each network zone
- Physical air gaps where mandated by security policy
- Redundant communication paths for critical systems

2. Logical Separation
- VLAN implementation requirements
- Subnet allocation guidelines
- Protocol-specific filtering rules

3. Access Control
- Zone-specific authentication mechanisms
- Multi-factor authentication requirements
- Role-based access control implementation

5. Communication Controls

1. Inter-zone Communication

- Strictly controlled through security gateways
- Whitelist-based protocol filtering
- Detailed traffic logging requirements

2. Remote Access

- Dedicated jump servers for remote maintenance
- Encrypted VPN connections mandatory
- Time-limited access authorization

3. Data Flow Controls

- One-way data diodes where applicable
- Protocol break mechanisms
- Application-layer filtering requirements

6. Implementation Procedures

1. Network Assessment

- Documentation of existing network topology
- Identification of critical assets and data flows
- Risk assessment requirements

2. Design Phase

- Zone boundary definition
- Security control selection
- Performance impact analysis

3. Deployment

- Phased implementation approach
- Testing requirements
- Rollback procedures

7. Monitoring and Maintenance

1. Continuous Monitoring

- Network traffic analysis
- Security event logging
- Performance metrics collection

2. Periodic Review

- Quarterly security assessments
- Configuration validation
- Policy compliance verification

8. Compliance and Documentation

1. Required Documentation

- Network architecture diagrams
- Zone definitions and classifications
- Security control configurations
- Change management records

2. Audit Requirements

- Annual third-party security audits
- Quarterly internal reviews
- Compliance validation procedures

9. Legal Disclaimers

1. This Guide contains confidential and proprietary information of DeepShield Systems, Inc. and may not be disclosed without written authorization.

2. Implementation of this Guide must comply with all applicable laws, regulations, and industry standards, including but not limited to NERC CIP, IEC 62443, and NIST SP 800-82.

3. DeepShield Systems, Inc. reserves the right to modify this Guide at any time to maintain alignment with evolving security requirements and industry best practices.

10. Document Control

Document Owner: Chief Security Architect

Last Review Date: January 15, 2024

Next Review Date: July 15, 2024

Document ID: DSS-SEC-2024-001

APPROVED BY:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: _