DeepShield OT Network Segmentation Protocol v2.1

Effective Date: January 15, 2024

Document Control Number: DS-SEC-2024-011

Classification: CONFIDENTIAL

Version: 2.1

1. PURPOSE AND SCOPE

1. This Network Segmentation Protocol ("Protocol") establishes mandatory requirements and procedures for the logical and physical separation of operational technology (OT) networks within industrial control system (ICS) environments protected by DeepShield Systems, Inc. ("DeepShield") solutions.

2. This Protocol applies to all DeepShield products, services, and implementations involving OT network security, including but not limited to SCADA systems, industrial automation networks, and maritime control systems.

2. DEFINITIONS

1. "OT Network" means any network containing industrial control systems, programmable logic controllers (PLCs), remote terminal units (RTUs), or other operational technology components.

2. "Security Zone" means a grouped set of systems with common security requirements and trust levels.

3. "Demilitarized Zone" or "DMZ" means a perimeter network that contains and exposes external-facing services while protecting the internal OT network.

4. "Deep Packet Inspection" or "DPI" means DeepShield's proprietary protocol-aware inspection technology for industrial protocols.

3. NETWORK SEGMENTATION REQUIREMENTS

1. Mandatory Zone Separation

1.1. All protected OT networks must maintain a minimum of five (5) distinct security zones:

a) Level 0: Field Devices

b) Level 1: Control Systems

c) Level 2: Supervisory Control

d) Level 3: Operations Management

e) Level 4: Enterprise Network

1.2. Each security zone shall be separated by DeepShield-approved firewalls implementing stateful inspection and Deep Packet Inspection capabilities.

2. DMZ Implementation

2.1. A DMZ must be established between any OT network and external networks, including corporate IT networks.

2.2. All data exchange between OT and external networks must traverse the DMZ using DeepShield's secure proxy services.

4. ACCESS CONTROL AND AUTHENTICATION

1. Zone Access Requirements

1.1. Access between zones shall be restricted to explicitly permitted communications using DeepShield's Zero Trust Architecture.

1.2. All inter-zone communications must be authenticated using:

a) PKI certificates for machine-to-machine communications

b) Multi-factor authentication for human users

c) Biometric verification for privileged access

2. Protocol Restrictions

2.1. Only approved industrial protocols shall be permitted within OT networks, including:

a) Modbus TCP

b) EtherNet/IP

c) ProfiNet

d) OPC UA

e) Additional protocols as specified in Appendix A

5. MONITORING AND ENFORCEMENT

1. Continuous Monitoring

1.1. DeepShield's AI-driven monitoring system shall maintain real-time visibility of:

a) Network traffic patterns

b) Protocol behaviors

c) Asset communications

d) Security zone integrity

2. Automated Response

2.1. The system shall automatically enforce segmentation through:

a) Dynamic access control updates

b) Threat-based isolation

c) Protocol validation

d) Traffic filtering

6. COMPLIANCE AND AUDIT

1. Regular audits of network segmentation shall be conducted quarterly using DeepShield's Compliance Verification Module.

2. Audit reports shall document:

a) Zone integrity status

b) Policy compliance

c) Segmentation violations

d) Remediation actions

7. MAINTENANCE AND UPDATES

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

a) Threat landscape

b) Industry standards

c) Regulatory requirements

d) Technology capabilities

2. All updates must be approved by DeepShield's Chief Security Architect and documented in the

version control system.

8. LEGAL COMPLIANCE

1. This Protocol is designed to support compliance with:

a) NIST SP 800-82

b) IEC 62443

c) NERC CIP

d) Maritime cybersecurity regulations

9. DISCLAIMER AND PROPRIETARY RIGHTS

1. This Protocol contains confidential and proprietary information of DeepShield Systems, Inc. and is protected under applicable intellectual property laws.

2. No part of this Protocol may be reproduced, modified, or distributed without express written permission from DeepShield Systems, Inc.

AUTHORIZATION

APPROVED AND ADOPTED by DeepShield Systems, Inc.

By:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: January 15, 2024

Document Control: DS-SEC-2024-011-v2.1