Zero Trust Architecture Implementation Guide

DeepShield Systems, Inc.

Document Version: 1.2

Effective Date: January 15, 2024

Classification: Confidential - Internal Use Only

1. Purpose and Scope

1. This Zero Trust Architecture Implementation Guide ("Guide") establishes the mandatory framework and procedures for implementing DeepShield Systems, Inc.'s ("Company") Zero Trust security model across all industrial control system (ICS) environments, operational technology (OT) networks, and related infrastructure.

2. This Guide applies to all Company employees, contractors, systems integrators, and authorized third parties who access, maintain, or interface with the Company's protected industrial control systems and networks.

2. Definitions

1. "Zero Trust Architecture" (ZTA): A security framework requiring all users and devices, whether internal or external, to be authenticated, authorized, and continuously validated before being granted access to applications and data.

2. "Micro-segmentation": The practice of dividing industrial control networks into isolated security segments, each requiring separate authentication and authorization.

3. "Least Privilege Access": The practice of limiting access rights to the minimum permissions necessary to perform required job functions.

3. Core Principles

1. Never Trust, Always Verify

a) All network traffic must be treated as untrusted by default

b) Authentication required regardless of network location

c) Continuous validation of security posture and compliance

2. Least Privilege Access Control

a) Access rights strictly limited to required functions

b) Time-bound access permissions

c) Regular access review and revocation procedures

3. Micro-segmentation Requirements

a) Isolation of critical OT systems

b) Separate security domains for SCADA networks

c) Independent authentication zones for maritime systems

4. Implementation Requirements

1. Network Architecture

a) Segmented industrial control networks

b) Encrypted communication channels

c) Multi-factor authentication (MFA) at all access points

d) Real-time monitoring and logging infrastructure

2. Access Control Implementation

a) Role-based access control (RBAC) framework

b) Just-in-time access provisioning

c) Automated access revocation

d) Privileged access management (PAM) systems

3. Security Monitoring

a) Continuous security posture assessment

b) Real-time threat detection and response

c) Automated compliance monitoring

d) Security event logging and analysis

5. Compliance and Audit

1. Regular compliance assessments against:

a) NIST SP 800-207 Zero Trust Architecture

b) IEC 62443 Industrial Network Security Standards

c) Company's internal security policies

d) Relevant regulatory requirements

2. Audit Requirements

a) Quarterly internal security audits

b) Annual third-party security assessments

c) Continuous compliance monitoring

d) Regular penetration testing

6. Incident Response and Recovery

1. Security Incident Management

a) Automated incident detection

b) Rapid response procedures

c) Incident containment protocols

d) Recovery and restoration processes

2. Business Continuity

a) Failover procedures

b) Disaster recovery protocols

c) System restoration priorities

d) Communication procedures

7. Training and Awareness

1. Required Training Programs

a) Initial Zero Trust security training

b) Annual security awareness updates

c) Role-specific security training

d) Incident response drills

8. Document Control

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

a) Technology infrastructure

b) Security requirements

c) Regulatory obligations

d) Threat landscape

9. Legal Disclaimer

This document contains confidential and proprietary information of DeepShield Systems, Inc. Any unauthorized use, disclosure, or distribution is strictly prohibited. The procedures and requirements outlined in this Guide are subject to change without notice and should be implemented in conjunction with all applicable laws, regulations, and company policies.

10. Approval and Authorization

This Zero Trust Architecture Implementation Guide has been reviewed and approved by:

_

Dr. Elena Rodriguez

Chief Security Architect

Date: January 15, 2024

_

Sarah Blackwood

Chief Technology Officer

Date: January 15, 2024

Document Control Number: ZTA-IG-2024-001

Last Updated: January 15, 2024

Next Review Date: January 15, 2025