Zero Trust Architecture Implementation Guide

DeepShield Systems, Inc.

Document Version: 1.2

Effective Date: January 15, 2024

Classification: Confidential & Proprietary

1. Purpose and Scope

1. This Zero Trust Architecture Implementation Guide ("Guide") establishes the mandatory security framework and implementation requirements for DeepShield Systems, Inc.'s ("DeepShield") industrial control system (ICS) security solutions and operational technology (OT) environments.

2. This Guide applies to all DeepShield products, services, and internal systems, including but not limited to the DeepShield Platform(TM), Maritime Defense Module(TM), and SubSea Protect(TM) offerings.

2. Definitions

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

2. "Trust Zones" means logically isolated network segments with defined security policies and access controls.

3. "Micro-segmentation" means the practice of dividing networks into isolated segments down to the individual workload level.

3. Core Principles

1. Never Trust, Always Verify

- All network traffic must be treated as untrusted
- Authentication required regardless of source location
- Continuous validation of security posture

2. Least Privilege Access

- Access rights limited to minimum necessary
- Time-bound access permissions
- Regular access review and revocation

3. Assume Breach
- All environments considered potentially compromised
- Continuous monitoring and threat detection
- Automated incident response capabilities

4. Implementation Requirements

1. Identity and Access Management
- Multi-factor authentication mandatory for all access
- Role-based access control (RBAC) implementation
- Regular credential rotation and audit
- Integration with industrial identity management systems

2. Network Segmentation
- Implementation of trust zones for OT networks
- Micro-segmentation of critical assets
- East-west traffic control and monitoring
- Air-gapped environments where required

3. Monitoring and Analytics
- Real-time traffic analysis
- Behavioral baseline establishment
- Anomaly detection and alerting
- AI-driven threat detection

5. Technical Controls

1. Network Security
- Layer 7 inspection of all traffic
- Encrypted communication channels

- Network access control (NAC)
- Software-defined perimeter implementation

2. Endpoint Security

- Host-based firewalls
- Endpoint detection and response (EDR)
- Application whitelisting
- Secure configuration baseline

3. Data Security

- Data classification and handling
- Encryption at rest and in transit
- Data loss prevention controls
- Secure backup and recovery

6. Compliance and Audit

1. Documentation Requirements

- Architecture diagrams
- Access policies and procedures
- Security incident response plans
- Change management records

2. Audit Schedule

- Quarterly internal security assessments
- Annual third-party security audit
- Continuous compliance monitoring
- Regular penetration testing

7. Incident Response

1. Detection and Analysis

- Automated threat detection
- Security event correlation

- Incident classification
- Impact assessment

2. Containment and Recovery

- Automated response procedures
- System isolation protocols
- Business continuity measures
- Recovery time objectives

8. Proprietary Rights

1. This Guide and all implementation methodologies described herein are the confidential and proprietary information of DeepShield Systems, Inc.

2. No part of this Guide may be reproduced, distributed, or transmitted without the express written permission of DeepShield Systems, Inc.

9. Amendments and Updates

1. DeepShield reserves the right to modify this Guide at any time.

2. Material changes will be communicated to affected parties with reasonable notice.

10. Approval and Authorization

APPROVED AND ADOPTED by DeepShield Systems, Inc.

By:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: January 15, 2024

By:

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: January 15, 2024