DeepShield Dashboard Technical Specification

Document Version: 3.2.1

Last Updated: January 11, 2024

Classification: CONFIDENTIAL - Internal Use Only

1. Overview

This Technical Specification ("Specification") defines the architectural framework, functional requirements, and technical parameters for the DeepShield Dashboard ("Dashboard"), the primary user interface component of the DeepShield Industrial Control System Security Platform ("Platform").

2. System Architecture

2.1 Core Components

- Presentation Layer: React.js-based frontend with Material-UI components
- Application Layer: Node.js backend with Express.js framework
- Data Processing Layer: Apache Kafka for real-time event streaming
- Storage Layer: PostgreSQL for relational data, MongoDB for event logs
- Security Layer: Zero-trust architecture with JWT-based authentication

2.2 Integration Points

- OT Network Interface: Proprietary DeepShield Protocol (DSP) v2.5
- SCADA Systems: Modbus TCP/IP, DNP3, IEC 61850
- External APIs: REST/HTTPS with TLS 1.3
- Authentication: SAML 2.0, OAuth 2.0 with OIDC

3. Functional Specifications

3.1 Real-time Monitoring

- Continuous monitoring of up to 50,000 ICS endpoints
- Latency requirements: <100ms for critical alerts
- Refresh rate: 1-second intervals for primary metrics
- Support for concurrent monitoring of 1,000 active users

3.2 Threat Detection

- AI-powered anomaly detection using DeepShield's proprietary algorithms
- Pattern recognition based on ML models trained on 10+ million events
- False positive rate: <0.1% for critical alerts
- Threat classification accuracy: >99.9% for known attack vectors

3.3 Visualization Components

- Interactive topology maps with drill-down capability
- Real-time asset health indicators
- Customizable dashboard widgets
- Support for 3D rendering of industrial environments

4. Security Requirements

4.1 Access Control

- Role-based access control (RBAC) with minimum 6 privilege levels
- Multi-factor authentication (MFA) mandatory for administrative access
- Session timeout: 15 minutes of inactivity
- IP-based access restrictions with configurable allowlists

4.2 Data Protection

- AES-256 encryption for data at rest
- TLS 1.3 for data in transit
- Secure key management using HSM integration
- Automated data retention policies compliant with NERC CIP

5. Performance Requirements

5.1 Scalability

- Horizontal scaling up to 1,000 nodes
- Vertical scaling support for up to 64 CPU cores per node
- Memory utilization: Maximum 85% under peak load
- Storage scaling: Support for 10PB+ of historical data

5.2 Availability

- 99.999% uptime requirement
- Automatic failover within 30 seconds
- Geographic redundancy across minimum 3 regions
- Recovery Time Objective (RTO): <5 minutes

6. Compliance & Standards

6.1 Industrial Standards

- IEC 62443 compliance
- NIST SP 800-82 alignment
- ISA-99 security standards
- NERC CIP v5/v6 requirements

6.2 Certification Requirements

- ISO 27001 certification
- SOC 2 Type II compliance
- Maritime certification (where applicable)
- Critical infrastructure protection standards

7. Proprietary Notice

8. Version Control

This specification is maintained under strict version control. All modifications must be approved by the Chief Security Architect and documented in the change log maintained in the DeepShield document management system.

9. Approval

APPROVED AND ADOPTED by DeepShield Systems, Inc.

By:

Dr. Elena Rodriguez

Chief Security Architect

Date: _

By:

James Morrison

VP of Engineering

Date: _