Network Segmentation Engine Technical Specification

DeepShield Systems, Inc.

Document No.: TS-NSE-2023-001

Version: 3.2

Last Updated: December 15, 2023

1. Overview and Scope

1. This Technical Specification ("Specification") describes the proprietary Network Segmentation Engine ("NSE") developed by DeepShield Systems, Inc. ("DeepShield") for use within its Industrial Control System (ICS) security platform.

2. The NSE represents core intellectual property of DeepShield and incorporates patented technologies covered under U.S. Patent Nos. 11,234,567 and 11,345,678.

2. Technical Architecture

1. Core Components

- Adaptive Segmentation Controller (ASC)
- Dynamic Policy Engine (DPE)
- OT Protocol Analysis Module (OTPAM)
- Real-time Traffic Classification System (RTCS)
- Segmentation Rule Enforcement Module (SREM)

2. System Requirements

- Processing: Intel Xeon E5-2680 v4 or equivalent
- Memory: Minimum 64GB ECC RAM
- Storage: 500GB NVMe SSD
- Network: Dual 10Gbps interfaces
- Operating System: Hardened Linux kernel 5.15 or higher

3. Functional Specifications

1. Network Analysis Capabilities

- Deep packet inspection of industrial protocols

- Real-time traffic pattern analysis
- Behavioral baseline establishment
- Anomaly detection with <0.001% false positive rate
- Support for 47 industrial protocols including Modbus, DNP3, EtherNet/IP

2. Segmentation Rules Engine

- Dynamic rule generation based on learned behavior
- Policy enforcement at Layer 2-7
- Microsegmentation capability at individual device level
- Integration with existing firewall infrastructure
- Support for up to 100,000 concurrent rules

4. Performance Parameters

1. Processing Capacity

- Maximum throughput: 20Gbps per instance
- Latency overhead: <50 microseconds
- Maximum concurrent connections: 1,000,000
- Rule processing time: <100 microseconds

2. Scalability

- Horizontal scaling up to 64 nodes
- Active-active clustering support
- Automatic load balancing
- State synchronization across cluster

5. Security Features

1. Encryption and Authentication

- TLS 1.3 for all management communications
- Hardware-based encryption acceleration
- Integration with enterprise PKI systems
- Support for HSM key storage
- FIPS 140-2 Level 3 compliance

2. Access Control

- Role-based access control (RBAC)
- Multi-factor authentication support
- Audit logging of all administrative actions
- Integration with enterprise directory services

6. Integration Capabilities

1. Supported Systems

- Major SCADA platforms
- Industrial firewall systems
- Security information and event management (SIEM) systems
- Asset management databases
- Configuration management databases

2. APIs and Protocols

- RESTful API for management functions
- MQTT support for real-time data
- Syslog output for event logging
- SNMP v3 for monitoring
- Custom API endpoints for specialized integrations

7. Compliance and Standards

1. Industrial Standards Compliance

- IEC 62443-4-2 Level 2
- NIST SP 800-82r2
- ISA-99
- NERC CIP

2. Certification Status

- Common Criteria EAL4+
- UL 2900-2-2
- IEC 62443 Security Level 2

8. Proprietary Rights and Confidentiality

1. All aspects of this Specification, including but not limited to algorithms, architectures, and implementations described herein, constitute confidential and proprietary information of DeepShield Systems, Inc.

2. This Specification is protected under applicable trade secret and intellectual property laws. No part may be reproduced, distributed, or disclosed without prior written authorization from DeepShield Systems, Inc.

9. Version Control

Version 3.2 approved by:

/s/ Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: December 15, 2023

/s/ James Morrison

VP of Engineering

DeepShield Systems, Inc.

Date: December 15, 2023

CONFIDENTIAL AND PROPRIETARY