Adaptive Security Response Framework Technical Specification

Document ID: ASRF-TS-2023-001

Version: 3.2

Effective Date: January 15, 2024

Classification: CONFIDENTIAL - PROPRIETARY

1. Overview and Scope

1. This Technical Specification ("Specification") defines the architectural framework, operational parameters, and implementation requirements for DeepShield Systems, Inc.'s ("DeepShield") Adaptive Security Response Framework ("ASRF"), a core component of the DeepShield Industrial Control System Security Platform.

2. The ASRF provides real-time threat detection, analysis, and automated response capabilities specifically engineered for operational technology (OT) environments, industrial control systems (ICS), and critical infrastructure protection.

2. Definitions

1. "Response Actions" means the predefined or dynamically generated security countermeasures implemented by the ASRF.

2. "Threat Vector Analysis" means the systematic evaluation of potential attack pathways within protected OT environments.

3. "Security Event" means any detected anomaly, unauthorized access attempt, or deviation from baseline operational parameters.

4. "Deep-Layer Architecture" means DeepShield's proprietary multi-tiered security implementation methodology.

3. Technical Architecture

1. Core Components

- Threat Detection Engine (TDE-7000)
- Neural Network Analysis Module (NNAM)
- Automated Response Coordinator (ARC)

- OT Protocol Integration Layer
- Secure Communications Backend

2. Implementation Requirements

- Minimum hardware specifications per Appendix A
- Network segmentation compliance with IEC 62443
- Redundant processing capabilities
- Fault-tolerant operational mode
- Secure boot verification

4. Operational Parameters

1. Response Time Requirements

- Critical Events: <50ms
- High Priority Events: <200ms
- Standard Events: <1000ms

2. System Availability

- 99.999% uptime requirement
- No single point of failure
- Automatic failover capabilities
- Geographic redundancy support

5. Security Controls

1. Authentication and Access Control

- Multi-factor authentication for administrative access
- Role-based access control (RBAC)
- Privileged Access Management (PAM) integration
- Session monitoring and logging

2. Encryption Requirements

- AES-256 for data at rest
- TLS 1.3 for data in transit

- Hardware Security Module (HSM) integration
- Perfect Forward Secrecy (PFS)

6. Integration Specifications

1. Supported Protocols

- Modbus TCP/IP
- EtherNet/IP
- Profinet
- OPC UA
- DNP3

2. API Requirements

- RESTful API endpoints
- GraphQL support
- WebSocket secure connections
- Rate limiting enforcement

7. Compliance and Certification

1. Regulatory Standards

- NIST SP 800-82r3
- IEC 62443
- NERC CIP
- ISO/IEC 27001:2022

2. Industry Certifications

- ISASecure EDSA
- Achilles Level 2
- Common Criteria EAL4+

8. Performance Metrics

1. Processing Capabilities

- Minimum 100,000 events per second

- Maximum latency of 5ms for critical events
- Concurrent session support: 10,000
- Real-time analysis capacity: 1TB/day

2. Scalability Requirements

- Horizontal scaling up to 1,000 nodes
- Vertical scaling support
- Dynamic resource allocation
- Load balancing capabilities

9. Intellectual Property Rights

1. All intellectual property rights, including patents, copyrights, trade secrets, and other proprietary information contained within or relating to the ASRF are the exclusive property of DeepShield Systems, Inc.

2. This Specification contains confidential and proprietary information and may not be disclosed, copied, or distributed without prior written authorization from DeepShield Systems, Inc.

10. Warranty and Liability

1. This Specification is provided "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

2. DeepShield Systems, Inc. shall not be liable for any damages arising from the use of or inability to use the ASRF or any associated documentation.

Execution

IN WITNESS WHEREOF, this Technical Specification has been executed by the duly authorized representatives of DeepShield Systems, Inc.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: January 15, 2024

By:

Name: James Morrison

Title: VP of Engineering

Date: January 15, 2024