Security Operations Center Integration Specification

DeepShield Systems, Inc.

Document Version: 1.2

Effective Date: January 11, 2024

1. Purpose and Scope

1. This Security Operations Center ("SOC") Integration Specification ("Specification") establishes the technical and operational requirements for integrating DeepShield Systems' Industrial Control System Security Platform ("ICS-SP") with client Security Operations Centers.

2. This Specification applies to all DeepShield Systems' SOC integration implementations and supersedes all previous versions of integration specifications.

2. Definitions

1. "Alert Data" means any security event, anomaly detection, or threat indicator data generated by the ICS-SP.

2. "Integration Components" means all software modules, APIs, and connectivity elements required to establish bi-directional communication between ICS-SP and client SOC infrastructure.

3. "OT Environment" means the operational technology environment containing industrial control systems, SCADA networks, and related infrastructure.

3. Technical Requirements

1. Communication Protocols

- 3.1.1. All integrations must utilize encrypted HTTPS (TLS 1.3 or higher) for REST API communications
- 3.1.2. MQTT protocol support with TLS encryption for real-time data streaming
- 3.1.3. Support for STIX/TAXII 2.1 or higher for threat intelligence sharing

2. Authentication

- 3.2.1. Mandatory implementation of OAuth 2.0 with JWT tokens
- 3.2.2. Multi-factor authentication for administrative access

- 3.2.3. Role-based access control (RBAC) with minimum privilege principle

3. Data Format

- 3.3.1. All Alert Data must conform to DeepShield's JSON schema version 3.0
- 3.3.2. Support for CEF and LEEF log formats
- 3.3.3. Syslog RFC 5424 compliance for log forwarding

4. Operational Requirements

1. Performance Standards

- 4.1.1. Maximum latency of 500ms for Alert Data transmission
- 4.1.2. Minimum 99.9% uptime for Integration Components
- 4.1.3. Automatic failover capability with redundant connectivity

2. Scalability Requirements

- 4.2.1. Support for minimum 10,000 events per second
- 4.2.2. Horizontal scaling capability for high-availability deployments
- 4.2.3. Dynamic resource allocation based on load

3. Monitoring and Maintenance

- 4.3.1. Real-time health monitoring of Integration Components
- 4.3.2. Automated alerting for integration failures
- 4.3.3. Monthly maintenance windows for updates

5. Security Controls

1. Data Protection

- 5.1.1. AES-256 encryption for data at rest
- 5.1.2. End-to-end encryption for data in transit
- 5.1.3. Secure key management system integration

2. Access Control

- 5.2.1. IP whitelisting for API endpoints
- 5.2.2. Certificate-based mutual authentication
- 5.2.3. Automated session termination after 15 minutes of inactivity

6. Compliance Requirements

1. All Integration Components must maintain compliance with:

- 6.1.1. IEC 62443 industrial security standards
- 6.1.2. NIST Cybersecurity Framework
- 6.1.3. Client-specific regulatory requirements

2. Documentation Requirements

- 6.2.1. Maintenance of integration architecture diagrams
- 6.2.2. Regular updates to security documentation
- 6.2.3. Incident response procedures

7. Liability and Warranties

1. DeepShield Systems warrants that the Integration Components will perform substantially in accordance with this Specification when properly implemented.

2. This Specification does not guarantee security against all possible threats or vulnerabilities.

3. DeepShield Systems' liability shall be limited to the remediation of integration-specific issues within commercially reasonable timeframes.

8. Modification and Updates

1. DeepShield Systems reserves the right to modify this Specification with 30 days' written notice to clients.

2. Emergency security updates may be implemented immediately when required.

9. Execution

IN WITNESS WHEREOF, this Specification is executed by the authorized representative of DeepShield Systems, Inc.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: January 11, 2024