Cloud Security Integration Architecture v2.1

DeepShield Systems, Inc.

Confidential & Proprietary

Effective Date: January 11, 2024

1. Introduction and Scope

1. This Cloud Security Integration Architecture document ("Architecture") defines the authorized technical and security specifications for DeepShield Systems, Inc.'s ("Company") cloud-based security integration framework as implemented within the DeepShield Industrial Control System Protection Platform(TM) ("Platform").

2. This Architecture is designated as Level 1 Confidential information under the Company's Information Classification Policy and contains trade secrets protected under applicable law.

2. Definitions

1. "Cloud Security Stack" means the Company's proprietary multi-layered security architecture comprising the following components:

a) Deep Learning Analytics Engine (DLAE)

b) OT Network Monitoring System (ONMS)

c) Maritime Asset Protection Framework (MAPF)

d) Subsea Infrastructure Defense Module (SIDM)

2. "Integration Points" means the authorized connection interfaces between Platform components and third-party industrial control systems.

3. "Security Zones" means the hierarchical trust boundaries established within the Platform architecture.

3. Architecture Components

1. Core Security Services

a) Identity and Access Management (IAM)

b) Encryption Management System

c) Key Management Service

d) Certificate Authority

e) Security Information and Event Management (SIEM)

2. Data Processing Pipeline

a) OT Protocol Analysis Engine

b) Anomaly Detection System

c) Threat Intelligence Integration

d) Machine Learning Classification Service

3. Integration Framework

a) API Gateway

b) Message Queue System

c) Service Mesh

d) Container Orchestration Platform

4. Security Controls

1. Authentication Requirements

a) Multi-factor authentication mandatory for all administrative access

b) Hardware security module (HSM) integration for key storage

c) Role-based access control (RBAC) enforcement

d) Just-in-time access provisioning

2. Encryption Standards

a) AES-256 for data at rest

b) TLS 1.3 for data in transit

c) Format-preserving encryption for OT protocols

d) Quantum-resistant algorithms for critical subsystems

3. Network Security

a) Microsegmentation

b) Zero trust architecture

c) East-west traffic encryption

d) OT protocol-aware firewall rules

5. Compliance Framework

1. The Architecture implements controls satisfying:

a) IEC 62443 (Industrial Network and System Security)

b) NIST SP 800-82 (Industrial Control Systems Security)

c) Maritime Transportation Security Act requirements

d) API Security Framework requirements

2. Audit Requirements

a) Quarterly architecture review

b) Annual penetration testing

c) Continuous compliance monitoring

d) Third-party security assessments

6. Integration Requirements

1. API Security

a) OAuth 2.0 with PKCE

b) API key rotation

c) Rate limiting

d) Request validation

2. Third-Party Integration

a) Vendor security assessment

b) Data processing agreement

c) Security controls verification

d) Integration testing requirements

7. Incident Response

1. Security Incident Classification

a) Severity levels

b) Response timeframes

c) Escalation procedures

d) Communication protocols

2. Recovery Procedures

a) Failover mechanisms

b) Data backup requirements

c) Service restoration priorities

d) Post-incident analysis

8. Maintenance and Updates

1. The Architecture shall be reviewed and updated:

a) Quarterly for technical specifications

b) Monthly for security controls

c) As needed for emergency patches

d) Annually for compliance requirements

9. Proprietary Rights

1. This Architecture and all components described herein are proprietary to DeepShield Systems, Inc. and protected under applicable intellectual property laws.

10. Version Control

Version 2.1

Approved by: Security Architecture Review Board

Date: January 11, 2024

Previous Version: 2.0 (October 15, 2023)

11. Authorization

APPROVED AND ADOPTED by the undersigned authorized representatives of DeepShield Systems, Inc.

Dr. Elena Rodriguez

Chief Security Architect

James Morrison

VP of Engineering

Sarah Blackwood

Chief Technology Officer