DevSecOps Integration Architecture Guide

DeepShield Systems, Inc.

Document Version: 1.2.4

Last Updated: January 11, 2024

Classification: CONFIDENTIAL - Legal & Technical

1. Purpose and Scope

1. This DevSecOps Integration Architecture Guide ("Guide") establishes the mandatory security architecture requirements and integration protocols for DeepShield Systems, Inc.'s ("Company") industrial control system (ICS) security platform and related components.

2. This Guide governs all development, deployment, and maintenance activities related to the Company's proprietary deep-layer security architecture and shall be binding upon all engineering teams, security architects, and development personnel.

2. Definitions

1. "Deep-Layer Architecture" means the Company's proprietary multi-tiered security framework incorporating AI-driven threat detection, real-time monitoring, and adaptive defense mechanisms.

2. "Critical Infrastructure Components" means any software, hardware, or integrated systems designed to protect SCADA networks, industrial automation systems, or operational technology (OT) environments.

3. "Maritime Security Modules" means specialized components designed for maritime and subsea infrastructure protection, including all associated proprietary algorithms and detection mechanisms.

3. Security Architecture Requirements

1. Core Architecture Components

a) All system components must implement the Company's Triple-Shield Protocol(TM)

b) Minimum encryption requirements: AES-256 for data at rest, TLS 1.3 for data in transit

c) Mandatory implementation of zero-trust architecture principles

d) Real-time threat intelligence integration with the DeepShield Threat Matrix(TM)

2. Integration Requirements

a) API security controls must conform to NIST 800-53 Rev. 5

b) Mandatory implementation of secure service mesh architecture

c) Container security protocols as specified in DS-SEC-2024-01

d) Automated security testing integration at all CI/CD pipeline stages

4. Development Security Controls

1. Code Security

a) Mandatory static code analysis using Company-approved tools

b) Dynamic security testing requirements per Schedule A

c) Secure code review procedures as outlined in DS-DEV-2024-02

d) Implementation of least-privilege access controls

2. Build and Deployment Security

a) Automated vulnerability scanning requirements

b) Secure artifact management protocols

c) Infrastructure-as-Code security validation

d) Deployment verification procedures

5. Operational Technology Integration

1. OT Security Requirements

a) Specialized protocols for industrial control system protection

b) SCADA network security integration requirements

c) Real-time monitoring and response mechanisms

d) OT-specific threat detection algorithms

2. Maritime Module Requirements

a) Subsea infrastructure protection protocols

b) Maritime-specific threat detection requirements

c) Offshore platform security integration procedures

d) Specialized maritime encryption requirements

6. Compliance and Audit

1. All implementations must maintain auditable compliance with:

a) ISO 27001:2022 requirements

b) IEC 62443 industrial security standards

c) Maritime cybersecurity regulations

d) Critical infrastructure protection requirements

2. Audit Requirements

a) Quarterly security architecture reviews

b) Annual penetration testing

c) Continuous compliance monitoring

d) Documentation maintenance requirements

7. Intellectual Property Protection

1. All architectural components, designs, and implementations developed under this Guide are the exclusive property of DeepShield Systems, Inc.

2. Confidentiality requirements and trade secret protections as specified in Schedule B shall apply to all architectural documentation and implementations.

8. Modification and Updates

1. This Guide may be updated or modified only by authorized Company personnel following the change control procedures specified in DS-CTRL-2024-01.

2. All modifications must be documented and communicated to affected personnel within 48 hours of approval.

9. Legal Disclaimer

This document contains confidential and proprietary information of DeepShield Systems, Inc. Unauthorized use, reproduction, or distribution is strictly prohibited. All rights reserved. Patents pending.

Execution

APPROVED AND ADOPTED this 11th day of January, 2024.

DEEPSHIELD SYSTEMS, INC.

By:

Dr. Elena Rodriguez

Chief Security Architect

By:

James Morrison

VP of Engineering