

THREAT HUNTING AUTOMATION PLATFORM SPECIFICATION

Document ID: DS-THAP-2023-v4.2

Last Updated: December 15, 2023

Classification: CONFIDENTIAL - PROPRIETARY

1. OVERVIEW AND SCOPE

1. This Threat Hunting Automation Platform Specification ("Specification") defines the proprietary threat hunting automation system developed by DeepShield Systems, Inc. ("DeepShield") for industrial control system (ICS) environments and operational technology (OT) infrastructure.

2. This Specification and all intellectual property rights contained herein are the exclusive property of DeepShield Systems, Inc., a Delaware corporation with its principal place of business at 2200 Innovation Drive, Suite 400, Wilmington, DE 19810.

2. DEFINITIONS

1. "Platform" means DeepShield's Threat Hunting Automation Platform, including all components, modules, and subsystems described herein.

2. "Hunt Protocols" means the proprietary threat detection and response algorithms developed by DeepShield.

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

4. "Maritime Assets" means subsea infrastructure, offshore platforms, and marine vessel control systems.

3. SYSTEM ARCHITECTURE

1. Core Platform Components

- Distributed sensor network utilizing proprietary DeepShield ICS monitoring protocols
- Centralized threat correlation engine with maritime-specific detection modules
- AI-driven behavioral analysis system for OT anomaly detection
- Automated response orchestration framework

- Secure command and control infrastructure

2. Integration Requirements

- Native support for major ICS/SCADA protocols including Modbus, DNP3, and IEC-61850
- Standardized API interfaces for third-party security tool integration
- Encrypted communication channels using FIPS 140-2 validated cryptographic modules
- Redundant command and control infrastructure with fail-safe mechanisms

4. PROPRIETARY TECHNOLOGIES

1. DeepShield Hunt Protocols(TM)

- Patent-pending threat detection algorithms optimized for industrial environments
- Machine learning models trained on proprietary OT threat intelligence
- Adaptive response frameworks for maritime and subsea infrastructure
- Real-time correlation of IT/OT security events

2. Protected Intellectual Property

- U.S. Patent Application No. 17/234,567 "Systems and Methods for Industrial Threat Detection"
- U.S. Patent No. 11,123,456 "Maritime Infrastructure Protection System"
- DeepShield Threat Intelligence Database(TM)
- Proprietary machine learning model architectures

5. OPERATIONAL SPECIFICATIONS

1. Performance Requirements

- Maximum latency of 50ms for critical threat detection
- 99.999% system availability for core hunting functions
- Support for minimum 100,000 concurrent monitored assets
- Real-time processing of up to 1 million events per second

2. Security Controls

- Zero-trust architecture implementation
- Role-based access control with granular permissions
- Secure boot and runtime attestation

- Encrypted storage of all threat intelligence data

6. COMPLIANCE AND CERTIFICATION

1. The Platform maintains compliance with:

- IEC 62443 Industrial Network and System Security
- NIST SP 800-82 Industrial Control Systems Security
- Maritime cybersecurity requirements per IMO MSC-FAL.1/Circ.3
- NERC CIP standards for critical infrastructure

7. CONFIDENTIALITY AND RESTRICTIONS

1. This Specification contains confidential and proprietary information of DeepShield Systems, Inc. and is protected under applicable intellectual property laws.

2. No part of this Specification may be reproduced, distributed, or disclosed without the express written permission of DeepShield Systems, Inc.

8. WARRANTY AND DISCLAIMER

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.

9. EXECUTION

IN WITNESS WHEREOF, this Specification has been approved and adopted by the authorized representatives of DeepShield Systems, Inc.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: December 15, 2023

By:

Name: James Morrison

Title: VP of Engineering

Date: December 15, 2023