THREAT HUNTING ALGORITHM DOCUMENTATION

DeepShield Systems, Inc.

Document Version: 3.2

Last Updated: January 11, 2024

Classification: CONFIDENTIAL

1. OVERVIEW AND SCOPE

1. This documentation ("Documentation") describes the proprietary threat hunting algorithms ("Algorithms") developed by DeepShield Systems, Inc. ("Company") for use in its Industrial Control System (ICS) security solutions and operational technology (OT) protection systems.

2. The Algorithms constitute protected intellectual property and trade secrets of the Company under 18 U.S.C.   1839 and applicable state laws.

2. DEFINITIONS

1. "Algorithm Components" means the collection of mathematical models, decision trees, neural network architectures, and processing workflows that comprise the Algorithms.

2. "Threat Hunting Engine" means the software implementation of the Algorithms within the Company's DeepShield(TM) Platform.

3. "Detection Parameters" means the configurable variables, thresholds, and operating conditions that govern Algorithm behavior.

3. ALGORITHM ARCHITECTURE

1. Core Components

- Multi-layer neural network for behavioral analysis
- Recursive pattern matching engine
- Anomaly detection framework
- Threat correlation matrix
- Response prioritization system

2. Input Processing

The Algorithms process the following data streams:

- Network traffic patterns
- Control system commands
- Device state changes
- Process variables
- Authentication events
- System logs

3. Output Generation

The Algorithms produce:

- Threat classification scores
- Attack vector identification
- Impact assessments
- Remediation recommendations
- Confidence ratings

4. PROPRIETARY METHODS

1. Pattern Recognition

The Algorithms employ proprietary methods for:

- Baseline behavior modeling
- Deviation detection
- Signature-less threat identification
- Zero-day attack recognition

2. Machine Learning Implementation

Protected elements include:

- Training methodologies
- Feature extraction techniques
- Model optimization procedures
- Accuracy improvement protocols

5. PERFORMANCE SPECIFICATIONS

1. Processing Requirements

- Minimum sampling rate: 1000 events/second
- Maximum latency: 50 milliseconds
- Accuracy threshold: 99.99%
- False positive rate: <0.01%

2. Operating Parameters

- Temperature range: 0 C to 45 C
- Memory utilization: 8GB-64GB
- Network bandwidth: 100Mbps-10Gbps
- Storage requirements: 500GB-4TB

6. IMPLEMENTATION REQUIREMENTS

1. The Algorithms shall be implemented only on Company-approved hardware configurations.

2. All Algorithm Components must maintain specified performance metrics under load.

3. Implementation must include:

- Redundancy mechanisms
- Failover capabilities
- Data integrity verification
- Access control enforcement

7. SECURITY CONTROLS

1. Algorithm Protection

- Encryption of all Algorithm Components
- Secure storage of detection parameters
- Access logging and auditing
- Version control requirements

2. Operational Security

- Runtime integrity checking
- Memory protection

- Component authentication
- Secure communication channels

8. INTELLECTUAL PROPERTY PROTECTION

1. All Algorithm Components are protected under U.S. Patent Applications:

- 17/234,567 (filed April 15, 2023)
- 17/456,789 (filed June 30, 2023)

2. Additional protection through:

- Copyright registration TX 8-925-461
- Trade secret protocols per Company Policy DS-IP-2023-01

9. CONFIDENTIALITY

1. This Documentation contains confidential and proprietary information of the Company.

2. Disclosure, reproduction, or distribution without express written authorization is strictly prohibited.

3. Authorized recipients shall:

- Maintain strict confidentiality
- Implement specified security controls
- Report unauthorized access attempts
- Return or destroy copies upon request

10. CERTIFICATION

The undersigned certifies this Documentation as complete and accurate as of the date below.

DEEPSHIELD SYSTEMS, INC.

By:

Dr. Elena Rodriguez

Chief Security Architect

Date: January 11, 2024

11. DOCUMENT CONTROL

Document ID: DS-ALG-2024-011

Version: 3.2

Classification: CONFIDENTIAL

Distribution: Authorized Personnel Only

Review Cycle: Annual