Security Event Correlation Engine Documentation

DeepShield Systems, Inc.

Version 3.2.1

Last Updated: December 15, 2023

Classification: CONFIDENTIAL

1. Overview and Proprietary Notice

This document describes the proprietary Security Event Correlation Engine ("SECE") developed by DeepShield Systems, Inc. ("DeepShield"). This documentation and all information contained herein is confidential and proprietary to DeepShield Systems, Inc. All rights reserved.

2. Technical Architecture

2.1 Core Components

The SECE comprises the following proprietary components:

- Neural Event Processing Core (NEPC)
- Distributed Sensor Integration Framework (DSIF)
- Maritime-Optimized Detection Algorithm Suite (MODAS)
- Industrial Control System Pattern Recognition Module (ICSPRM)

2.2 Processing Architecture

The SECE utilizes a multi-layered processing architecture incorporating:

- Layer 1: Raw event ingestion and normalization
- Layer 2: Context-aware pattern matching
- Layer 3: Machine learning correlation analysis
- Layer 4: Threat determination and response orchestration

3. Proprietary Algorithms

3.1 Pattern Recognition

The SECE implements DeepShield's patented Deep-Layer Industrial Pattern Recognition(TM) technology (U.S. Patent No. 11,XXX,XXX) for identifying anomalous behavior in industrial control systems.

3.2 Maritime Subsystems

Specialized correlation algorithms optimized for maritime and subsea infrastructure, including:

- Subsea sensor data normalization
- Maritime traffic pattern analysis
- Offshore platform behavioral modeling
- Port facility access correlation

4. Integration Specifications

4.1 Data Ingestion

The SECE accepts the following data formats:

- Standard SIEM outputs (CEF, LEEF)
- Industrial protocol traffic (Modbus, DNP3, OPC-UA)
- Custom sensor feeds via REST API
- Maritime AIS data streams

4.2 Output Interfaces

Standardized output mechanisms including:

- STIX/TAXII threat intelligence feeds
- REST API endpoints
- SIEM integration connectors
- Custom webhook notifications

5. Performance Parameters

5.1 Processing Capacity

- Maximum events per second: 500,000
- Correlation window: Configurable 1-180 days
- Maximum sensor connections: 10,000
- Storage capacity: 24 months online, unlimited archived

5.2 Accuracy Metrics

Based on controlled testing environments:

- False positive rate: <0.001%

- Detection accuracy: >99.99%
- Response latency: <50ms
- Pattern matching precision: >99.95%

6. Intellectual Property Protection

6.1 Ownership

All intellectual property rights, including but not limited to patents, copyrights, trade secrets, and know-how related to the SECE are exclusively owned by DeepShield Systems, Inc.

6.2 Confidentiality

This documentation contains trade secrets and confidential information of DeepShield Systems, Inc. Any unauthorized access, use, or disclosure is strictly prohibited and may result in civil and criminal penalties.

7. Compliance and Certification

7.1 Standards Compliance

The SECE has been certified compliant with:

- IEC 62443 Industrial Network Security
- NIST SP 800-82 Industrial Control Systems Security
- ISO 27001:2013 Information Security Management
- Maritime cybersecurity requirements (BIMCO, TMSA3)

7.2 Validation

Independent security validation performed by:

- Maritime Classification Societies
- Industrial Control System Testing Labs
- Third-party penetration testing firms

8. Version Control

8.1 Documentation History

- Version 3.2.1 (Current) - December 15, 2023
- Version 3.2.0 - September 30, 2023

- Version 3.1.2 - June 15, 2023
- Version 3.1.1 - March 1, 2023

8.2 Change Management

All modifications to the SECE documentation are subject to DeepShield's formal change control process and require approval from the Chief Security Architect.

9. Legal Notice

This document is protected by copyright and trade secret laws. No part of this documentation may be reproduced, transmitted, or distributed in any form or by any means without the prior written permission of DeepShield Systems, Inc. All violations will be prosecuted to the fullest extent of the law.

APPROVED BY:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: December 15, 2023

James Morrison

VP of Engineering

DeepShield Systems, Inc.

Date: December 15, 2023