Security Event Correlation Engine Design

CONFIDENTIAL AND PROPRIETARY

DeepShield Systems, Inc.

Document Version: 3.2

Last Updated: January 11, 2024

1. OVERVIEW AND SCOPE

1. This document describes the proprietary design specifications and architecture of DeepShield Systems, Inc.'s ("DeepShield") Security Event Correlation Engine ("SECE"), a core component of DeepShield's Industrial Control System Security Platform.

2. The SECE design detailed herein represents confidential intellectual property of DeepShield, protected under U.S. Patent No. 11,487,XXX and related pending applications.

2. DEFINITIONS

1. "Correlation Rules" means the proprietary algorithmic frameworks that define relationships between security events across OT network layers.

2. "Event Processing Pipeline" means the sequential stages of data ingestion, normalization, enrichment, and analysis within the SECE.

3. "Industrial Protocol Parsers" means software components that decode and normalize industrial control system protocols including but not limited to Modbus, DNP3, and proprietary SCADA protocols.

3. SYSTEM ARCHITECTURE

1. Core Components

a) Event Ingestion Layer

b) Protocol Normalization Engine

c) Context Enrichment Module

d) Correlation Analysis Engine

e) Alert Generation System

2. Data Flow Architecture

a) Raw event data is captured through distributed sensors

b) Events are normalized using Industrial Protocol Parsers

c) Contextual data is added through the Enrichment Module

d) Correlation Rules are applied in real-time

e) Actionable alerts are generated based on threat severity

4. CORRELATION METHODOLOGY

1. Pattern Recognition

The SECE employs proprietary machine learning models to identify complex attack patterns across multiple OT network segments, incorporating:

a) Temporal correlation algorithms

b) Spatial relationship mapping

c) Behavioral anomaly detection

d) Protocol-specific threat indicators

2. Risk Scoring

Events are scored using DeepShield's proprietary risk calculation framework that considers:

a) Asset criticality

b) Threat intelligence

c) Historical baseline deviation

d) Operational impact assessment

5. INTEGRATION SPECIFICATIONS

1. Input Interfaces

a) Native protocol support for industrial control systems

b) REST API for external data sources

c) MQTT broker integration

d) Custom connector framework

2. Output Interfaces

a) SIEM integration via syslog

b) REST API for alert consumption

c) Message queue interface

d) Custom webhook support

6. PERFORMANCE REQUIREMENTS

1. Processing Capacity

a) Minimum throughput: 50,000 events per second

b) Maximum latency: 100 milliseconds

c) Correlation window: configurable up to 30 days

2. Availability Requirements

a) System uptime: 99.999%

b) Failover time: < 5 seconds

c) Data retention: 365 days

7. SECURITY CONTROLS

1. Data Protection

a) AES-256 encryption for data at rest

b) TLS 1.3 for data in transit

c) Hardware Security Module integration

d) Secure key management system

2. Access Control

a) Role-based access control

b) Multi-factor authentication

c) Audit logging of all system access

d) Privileged access management

8. INTELLECTUAL PROPERTY NOTICE

written permission of DeepShield Systems, Inc.

9. REVISION HISTORY

Version 3.2 - January 11, 2024

- Updated correlation algorithms
- Enhanced protocol parser specifications
- Added maritime-specific correlation rules

Version 3.1 - October 15, 2023

- Added subsea infrastructure monitoring capabilities
- Updated performance requirements

Version 3.0 - July 1, 2023

- Initial release of maritime/subsea module
- Core architecture revision

10. APPROVAL AND VALIDATION

This design specification has been reviewed and approved by:

/s/ Dr. Elena Rodriguez

Chief Security Architect

Date: January 11, 2024

/s/ James Morrison

VP of Engineering

Date: January 11, 2024