DeepShield Threat Intelligence Database Schema

CONFIDENTIAL AND PROPRIETARY

Document Version: 3.2

Last Updated: January 11, 2024

1. INTRODUCTION

This document defines the proprietary database schema and data architecture for DeepShield Systems, Inc.'s ("DeepShield") Threat Intelligence Platform. This schema specification is confidential, proprietary, and protected under U.S. and international intellectual property laws.

2. DEFINITIONS

1. "Schema" refers to the complete logical and physical database structure, including all tables, relationships, fields, and constraints defined herein.

2. "TIP" means DeepShield's Threat Intelligence Platform.

3. "ICS" means Industrial Control Systems.

4. "OT" means Operational Technology.

5. "SCADA" means Supervisory Control and Data Acquisition systems.

3. CORE SCHEMA COMPONENTS

1. Threat Actor Tables

- threat_actor_master (Primary key: actor_id)
- actor_attribution
- actor_techniques
- actor_infrastructure
- historical_campaigns

2. Vulnerability Database

- vulnerability_master (Primary key: vuln_id)
- affected_systems

- patch_status
- exploitation_vectors
- mitigation_strategies

3. Asset Intelligence
- asset_inventory (Primary key: asset_id)
- asset_relationships
- asset_vulnerabilities
- asset_configurations
- compliance_status

4. RELATIONSHIP DEFINITIONS

1. Primary Relationships
- One-to-many relationship between threat_actor_master and actor_techniques
- Many-to-many relationship between vulnerability_master and affected_systems
- One-to-many relationship between asset_inventory and asset_vulnerabilities

2. Secondary Relationships
- Cross-reference tables for complex relationships
- Temporal tracking tables for historical analysis
- Correlation tables for threat attribution

5. DATA TYPES AND CONSTRAINTS

1. Standard Field Types
- UUID fields for primary keys
- VARCHAR(255) for descriptive fields
- TIMESTAMP with timezone for all temporal data
- JSONB for flexible attribute storage
- BYTEA for binary data storage

2. Mandatory Constraints
- NOT NULL constraints on critical fields

- Foreign key constraints with CASCADE options
- Check constraints for data validation
- Unique constraints on identifier fields

6. SECURITY CLASSIFICATIONS

1. Data Classification Levels

- Level 1: Public Information
- Level 2: Internal Use Only
- Level 3: Confidential
- Level 4: Highly Confidential
- Level 5: Restricted Access

2. Access Controls

- Row-level security policies
- Column-level encryption
- Role-based access control mappings
- Audit logging requirements

7. COMPLIANCE AND REGULATORY REQUIREMENTS

1. The Schema shall maintain compliance with:

- NIST Cybersecurity Framework
- IEC 62443 Standards
- NERC CIP Requirements
- ISO 27001 Controls

2. Regulatory Data Storage

- Retention periods by data classification
- Geographical storage restrictions
- Audit trail requirements
- Compliance reporting capabilities

8. INTELLECTUAL PROPERTY RIGHTS

1. All aspects of this Schema, including but not limited to the structure, relationships, naming conventions, and optimization strategies, are the exclusive intellectual property of DeepShield Systems, Inc.

2. No part of this Schema may be copied, modified, or implemented without express written authorization from DeepShield Systems, Inc.

9. MODIFICATION AND MAINTENANCE

1. Schema modifications require:

- Security impact assessment
- Performance impact analysis
- Backwards compatibility review
- Migration plan documentation
- Executive approval

2. Version Control

- Major version changes require full security audit
- Minor versions must maintain backward compatibility
- Emergency patches must be documented within 24 hours

10. CONFIDENTIALITY

This Schema document contains trade secrets and confidential information of DeepShield Systems, Inc. Distribution is restricted to authorized personnel only. Unauthorized disclosure, copying, or use is strictly prohibited and may result in civil and criminal penalties.

EXECUTION

IN WITNESS WHEREOF, the undersigned acknowledges the confidentiality and proprietary nature of this Schema specification.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: January 11, 2024

By:

Name: James Morrison

Title: VP of Engineering

Date: January 11, 2024