AUTOMATED RESPONSE SYSTEM TECHNICAL DESIGN

CONFIDENTIAL AND PROPRIETARY

Document No.: TD-2023-114

Version: 2.1

Last Updated: December 15, 2023

1. DOCUMENT CONTROL

1 This Technical Design Document ("Design Document") is the confidential and proprietary information of DeepShield Systems, Inc., a Delaware corporation ("DeepShield" or the "Company").

2 Distribution of this Design Document is restricted to authorized personnel who have executed applicable non-disclosure agreements with DeepShield Systems, Inc.

2. SYSTEM OVERVIEW

1 The DeepShield Automated Response System ("DARS") is an integrated cybersecurity defense platform designed for industrial control systems (ICS) and operational technology (OT) environments.

2 Core Architecture Components:

a) Threat Detection Engine (TDE-7)

b) Response Orchestration Module (ROM)

c) Industrial Protocol Analysis Framework (IPAF)

d) Secure Command Gateway (SCG)

e) OT Network Isolation System (OTNIS)

3. TECHNICAL SPECIFICATIONS

1 System Architecture

1.1 The DARS platform utilizes a distributed microservices architecture with the following characteristics:

- Containerized deployment model
- Redundant processing nodes

- Real-time data processing capability: 50ms latency
- Throughput capacity: 100,000 events per second per node
- High-availability configuration (99.999% uptime)

1.2 Network Integration Requirements:

- Support for standard industrial protocols (Modbus, DNP3, OPC-UA)
- IPv4/IPv6 dual-stack implementation
- VLAN segregation capability
- QoS support for critical traffic

4. PROPRIETARY TECHNOLOGIES

1 Protected Intellectual Property

The following components constitute protected intellectual property of DeepShield:

1.1 ThreatMatrix(TM) Analysis Engine

- Patent pending (US Application No. 17/234,567)
- Proprietary threat correlation algorithms
- Machine learning model architecture

1.2 ResponseCore(TM) Framework

- Registered trademark (Reg. No. 88765432)
- Automated response orchestration logic
- Custom protocol handlers

5. SECURITY CONTROLS

1 Authentication and Authorization

1.1 Multi-factor authentication implementation:

- Hardware security key support
- Biometric verification capability
- Role-based access control (RBAC)
- Privileged access management (PAM)

1.2 Encryption Standards:

- AES-256 for data at rest
- TLS 1.3 for data in transit
- Hardware security module (HSM) integration

6. COMPLIANCE AND CERTIFICATION

1 The DARS platform maintains compliance with:

- IEC 62443 (Industrial Network and System Security)
- NIST SP 800-82 (Industrial Control Systems Security)
- ISO/IEC 27001:2013 (Information Security Management)

2 Third-party Security Certifications:

- Common Criteria EAL4+
- UL 2900-2-2 (Network-Connectable Industrial Control Systems)

7. IMPLEMENTATION REQUIREMENTS

1 Hardware Requirements:

- Minimum processor: Intel Xeon E5-2680 v4 or equivalent
- Memory: 128GB RAM minimum
- Storage: 2TB NVMe SSD
- Network: Dual 10GbE interfaces

2 Software Dependencies:

- Operating System: Hardened Linux (RHEL 8.4 or higher)
- Container Runtime: Docker Enterprise Edition
- Database: PostgreSQL 13.0 or higher

8. CONFIDENTIALITY AND INTELLECTUAL PROPERTY

1 All information contained in this Design Document, including but not limited to system architecture, algorithms, protocols, and implementation details, constitutes confidential trade secrets of DeepShield Systems, Inc.

2 No part of this Design Document may be reproduced, distributed, or transmitted in any form

without the express written permission of DeepShield Systems, Inc.

9. DOCUMENT VALIDATION

APPROVED AND ADOPTED by DeepShield Systems, Inc. on December 15, 2023.

By:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

By:

James Morrison

VP of Engineering

DeepShield Systems, Inc.

10. REVISION HISTORY

Version 2.1 - December 15, 2023

- Updated security controls section
- Added new compliance certifications
- Revised hardware requirements

Version 2.0 - June 30, 2023

- Major architecture revision
- Added ResponseCore(TM) Framework
- Updated implementation requirements

Version 1.0 - January 15, 2023

- Initial document release