SCADA SECURITY PROTOCOL

Saudi Aramco Refineries Implementation

DeepShield Systems, Inc.

Document No. DSS-SAR-2023-0142

Effective Date: January 15, 2024

1. INTRODUCTION

1 This SCADA Security Protocol ("Protocol") is established by DeepShield Systems, Inc., a Delaware corporation ("DeepShield"), for implementation at Saudi Aramco refineries pursuant to Master Services Agreement No. SA-DS-2023-891 dated December 1, 2023.

2 This Protocol governs the deployment, operation, and maintenance of DeepShield's Industrial Control System (ICS) security solutions within the operational technology (OT) environment of designated Saudi Aramco refinery facilities.

2. DEFINITIONS

1 "Critical Infrastructure" means the operational technology systems, industrial control systems, and SCADA networks essential to refinery operations.

2 "Deep-Layer Architecture" means DeepShield's proprietary security framework incorporating AI-driven threat detection, real-time monitoring, and adaptive defense mechanisms.

3 "Security Event" means any detected or suspected unauthorized access, anomalous behavior, or cyber threat within the protected OT environment.

3. SCOPE OF IMPLEMENTATION

1 Geographic Coverage

This Protocol applies to all Saudi Aramco refineries where DeepShield's security solutions are deployed, including but not limited to:

(a) Ras Tanura Refinery

(b) Yanbu Refinery Complex

(c) Riyadh Refinery

(d) Jeddah Refinery

2 System Coverage

The Protocol encompasses:

(a) SCADA control systems

(b) Distributed Control Systems (DCS)

(c) Programmable Logic Controllers (PLCs)

(d) Human-Machine Interfaces (HMIs)

(e) Industrial networking infrastructure

4. SECURITY MEASURES

1 Network Segmentation

DeepShield shall implement:

(a) Physical and logical separation of OT and IT networks

(b) Dedicated security zones for critical control systems

(c) Controlled access points between security zones

(d) Multi-layer authentication protocols

2 Monitoring and Detection

The following capabilities shall be maintained:

(a) Real-time network traffic analysis

(b) Behavioral anomaly detection

(c) Asset inventory and change management

(d) Threat intelligence integration

(e) AI-powered pattern recognition

5. INCIDENT RESPONSE

1 Response Protocol

Upon detection of a Security Event:

(a) Immediate notification to designated security personnel

(b) Automated containment measures activation

(c) Incident classification and escalation

(d) Root cause analysis initiation

2 Recovery Procedures

Implementation of:

(a) System restoration protocols

(b) Data backup and recovery processes

(c) Operational continuity measures

(d) Post-incident analysis and reporting

6. COMPLIANCE AND REPORTING

1 Regulatory Compliance

Adherence to:

(a) Saudi Arabian cybersecurity regulations

(b) International industrial security standards

(c) Industry-specific compliance requirements

(d) DeepShield's internal security policies

2 Documentation Requirements

Maintenance of:

(a) Security event logs

(b) System configuration records

(c) Audit trails

(d) Compliance reports

7. CONFIDENTIALITY

1 All information related to the implementation, operation, and maintenance of security measures under this Protocol shall be treated as strictly confidential.

2 Access to security-related information shall be restricted to authorized personnel on a need-to-know basis.

8. LIABILITY AND INDEMNIFICATION

1 DeepShield's liability shall be limited as specified in the Master Services Agreement.

2 This Protocol does not create additional warranties or representations beyond those explicitly stated

in the Master Services Agreement.

9. TERM AND MODIFICATION

1 This Protocol shall remain in effect for the duration of the Master Services Agreement.

2 Modifications to this Protocol must be made in writing and approved by authorized representatives of both parties.

EXECUTION

IN WITNESS WHEREOF, the undersigned has executed this Protocol as of the Effective Date.

DEEPSHIELD SYSTEMS, INC.

By: _

Name: Dr. Marcus Chen

Title: Chief Executive Officer

Date: January 15, 2024

APPROVED BY:

By: _

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: January 15, 2024