CHEVRON REFINERY SCADA SECURITY ASSESSMENT

CONFIDENTIAL AND PRIVILEGED

Prepared by DeepShield Systems, Inc.

Assessment Date: October 15-29, 2023

Report Date: November 12, 2023

1. EXECUTIVE SUMMARY

This Security Assessment Report ("Assessment") documents the findings and recommendations resulting from DeepShield Systems, Inc.'s ("DeepShield") comprehensive evaluation of the Supervisory Control and Data Acquisition (SCADA) systems at Chevron Corporation's Richmond Refinery facility ("Facility"). The Assessment was conducted pursuant to Master Services Agreement #CHV-2023-0472 dated March 1, 2023.

2. SCOPE OF ASSESSMENT

1 Systems Evaluated

- Primary SCADA control network infrastructure
- Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs)
- Human-Machine Interface (HMI) systems
- Historian databases and data aggregation systems
- Network segmentation and security controls
- Industrial Protocol implementations (Modbus, DNP3, OPC-UA)

2 Assessment Methodology

The evaluation employed DeepShield's proprietary SHIELD-7 assessment framework, incorporating:

- Network architecture review
- Control system configuration analysis
- Protocol vulnerability assessment
- Threat modeling and risk quantification
- Security control effectiveness testing
- Incident response capability evaluation

3. KEY FINDINGS

1 Critical Vulnerabilities

- CVE-2023-27891: Buffer overflow vulnerability in legacy RTU firmware
- Unpatched security updates on 37% of PLCs
- Weak authentication mechanisms on auxiliary HMI terminals
- Insufficient network segmentation between IT and OT networks

2 High-Risk Issues

- Outdated protocol implementations on 12 field devices
- Non-compliant password policies on engineering workstations
- Incomplete system backup procedures
- Limited monitoring of third-party vendor access

3 Medium-Risk Issues

- Inconsistent patch management procedures
- Inadequate change management documentation
- Legacy systems operating beyond vendor support
- Insufficient physical access controls to remote terminals

4. RECOMMENDATIONS

1 Immediate Actions (0-30 days)

a) Implement emergency patches for identified critical vulnerabilities

b) Enable multi-factor authentication on all HMI systems

c) Review and update access control matrices

d) Deploy additional network monitoring sensors

2 Short-Term Actions (30-90 days)

a) Upgrade firmware on affected RTUs and PLCs

b) Implement enhanced network segmentation

c) Deploy DeepShield's AI-driven anomaly detection system

d) Establish formal vendor access management procedures

3 Long-Term Actions (90-180 days)

a) Develop comprehensive system modernization roadmap

b) Implement automated patch management system

c) Enhance disaster recovery capabilities

d) Establish continuous monitoring program

5. RISK QUANTIFICATION

1 Current Risk Profile

- Critical Risk Items: 4
- High Risk Items: 7
- Medium Risk Items: 12
- Low Risk Items: 23

2 Projected Risk Reduction

Implementation of recommended controls is expected to achieve:

- 85% reduction in critical risks
- 70% reduction in high risks
- 60% reduction in medium risks

6. COMPLIANCE CONSIDERATIONS

1 Regulatory Requirements

This Assessment evaluates compliance with:

- NIST SP 800-82r3
- IEC 62443
- API 1164
- NERC CIP Standards

2 Industry Standards

Assessment methodology aligned with:

- ISA/IEC 62443 Series
- NIST Cybersecurity Framework
- Center for Internet Security (CIS) Controls

7. CONFIDENTIALITY AND LIMITATIONS

1 This Assessment and all findings contained herein are confidential and subject to the Non-Disclosure Agreement between DeepShield Systems, Inc. and Chevron Corporation dated February 15, 2023.

2 This Assessment represents a point-in-time evaluation and does not guarantee future security posture or freedom from cyber threats.

8. CERTIFICATION

This Assessment was conducted by DeepShield Systems, Inc.'s certified security professionals in accordance with industry standards and best practices.

Prepared by:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Reviewed by:

James Morrison

VP of Engineering

DeepShield Systems, Inc.

Date: November 12, 2023

[DIGITAL SIGNATURE AND CERTIFICATION DETAILS OMITTED]