Critical Infrastructure Protection Assessment

Shell Refineries Q4 2022

Prepared by DeepShield Systems, Inc.

Assessment Period: October 1 - December 31, 2022

Document Reference: DS-CIP-SHELL-2022Q4-001

1. Executive Summary

This Critical Infrastructure Protection Assessment ("Assessment") has been prepared by DeepShield Systems, Inc. ("DeepShield") for Shell Refineries' operational technology (OT) infrastructure pursuant to Master Services Agreement #MSA-2022-0472 dated March 15, 2022. The Assessment evaluates cybersecurity readiness across Shell's North American refinery operations, with particular focus on industrial control systems (ICS) and SCADA network infrastructure.

2. Assessment Scope

1. Facilities Assessed

- Shell Deer Park Refinery (Texas)
- Shell Norco Manufacturing Complex (Louisiana)
- Shell Puget Sound Refinery (Washington)

2. Systems Evaluated

- Distributed Control Systems (DCS)
- Safety Instrumented Systems (SIS)
- Process Control Networks (PCN)
- Industrial Control System (ICS) Components
- SCADA Infrastructure
- Operations Technology (OT) Networks
- Human-Machine Interface (HMI) Systems

3. Methodology

1. Assessment Framework

Assessment conducted using DeepShield's proprietary Deep-Layer Security Architecture(TM)

methodology, incorporating:

- NIST Cybersecurity Framework
- ISA/IEC 62443 Standards
- API 1164 Pipeline SCADA Security
- NERC CIP Requirements

2. Testing Procedures

- Network Architecture Review
- Control System Configuration Analysis
- Vulnerability Assessment
- Penetration Testing (Limited Scope)
- Security Control Validation
- Incident Response Capability Review

4. Key Findings

1. Critical Vulnerabilities

- Three (3) Level 1 vulnerabilities identified in legacy DCS systems
- One (1) Level 1 vulnerability in remote access infrastructure
- Two (2) Level 2 vulnerabilities in SCADA protocol implementations

2. System Hardening Status

- 87% compliance with baseline security controls
- 92% patch compliance for supported systems
- 73% compliance for legacy systems requiring compensating controls

3. Network Segmentation

- Adequate separation between IT and OT networks
- Implementation of DMZ architecture requires enhancement
- Additional network segregation recommended for critical processes

5. Recommendations

1. Immediate Actions (0-30 Days)

- Implement emergency patches for identified Level 1 vulnerabilities
- Update remote access authentication mechanisms
- Deploy additional network monitoring sensors

2. Short-Term Actions (31-90 Days)
- Enhance DMZ architecture
- Upgrade legacy system security controls
- Implement additional network segmentation
- Deploy advanced anomaly detection capabilities

3. Long-Term Strategic Initiatives (91+ Days)
- Develop comprehensive OT security modernization roadmap
- Implement zero-trust architecture for critical systems
- Enhance incident response capabilities
- Establish continuous monitoring program

6. Risk Assessment Matrix

1. Current Risk Profile
- Critical Risk Items: 4
- High Risk Items: 7
- Medium Risk Items: 12
- Low Risk Items: 23

2. Post-Remediation Projected Risk Profile
- Critical Risk Items: 0
- High Risk Items: 3
- Medium Risk Items: 8
- Low Risk Items: 35

7. Compliance Status

1. Regulatory Requirements
- CFATS: 94% Compliant

- NERC CIP: 89% Compliant
- API 1164: 91% Compliant
- ISA/IEC 62443: 86% Compliant

8. Confidentiality Notice

This document contains confidential and proprietary information of DeepShield Systems, Inc. and Shell Refineries. Distribution of this Assessment is restricted to authorized personnel only. All findings, recommendations, and technical details contained herein are subject to the confidentiality provisions of the Master Services Agreement referenced above.

9. Certification

This Assessment has been prepared and reviewed by qualified DeepShield personnel in accordance with industry standards and best practices.

Prepared by:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: December 31, 2022

Reviewed by:

James Morrison

VP of Engineering

DeepShield Systems, Inc.

Date: January 5, 2023

10. Disclaimer

This Assessment represents a point-in-time evaluation of cybersecurity controls and vulnerabilities. DeepShield Systems, Inc. makes no ongoing warranties or representations regarding the security status of assessed systems beyond the assessment period. Implementation of recommendations does not guarantee prevention of all possible security incidents or breaches.