Rotterdam Tank Terminal Security Case Study

CONFIDENTIAL & PRIVILEGED

DeepShield Systems, Inc.

Document Reference: CS-RTT-2023-114

Date: September 15, 2023

1. Executive Summary

This case study documents the implementation and operational outcomes of DeepShield Systems' Industrial Control System (ICS) security solution at the Rotterdam Tank Terminal (RTT) facility, completed pursuant to Contract No. DS-2022-RTT-456, dated March 1, 2022.

2. Facility Overview

1. The Rotterdam Tank Terminal is a strategic liquid bulk storage facility located in the Port of Rotterdam, Netherlands, with:

- Total storage capacity: 750,000 cubic meters
- Number of tanks: 34
- Primary products: petroleum, chemicals, biofuels
- Annual throughput: 8.5 million metric tons
- Operational systems: Level 1-3 ICS architecture

2. Critical Infrastructure Classification: European Critical Infrastructure (ECI) designation under EU Directive 2008/114/EC.

3. Security Challenge Assessment

1. Pre-Implementation Vulnerabilities:

- Legacy SCADA systems with minimal cybersecurity controls
- Insufficient OT/IT network segmentation
- Limited real-time threat monitoring capabilities
- Absence of automated incident response protocols
- Non-compliant with NIST SP 800-82r3 guidelines

2. Regulatory Requirements:

- EU NIS Directive 2016/1148
- IMO Maritime Cyber Risk Management requirements
- ISPS Code compliance
- Dutch national critical infrastructure protection standards

4. Solution Implementation

1. DeepShield Deployment Scope:

- DeepShield Maritime(TM) Platform v4.2
- OT Network Monitoring Module
- Deep-Layer Protection Architecture
- AI-Driven Threat Detection System
- Emergency Response Automation Suite

2. Implementation Timeline:

- Phase 1: Network assessment and architecture design (Q2 2022)
- Phase 2: Core system deployment (Q3 2022)
- Phase 3: Integration and testing (Q4 2022)
- Phase 4: Operational handover (Q1 2023)

5. Operational Results

1. Key Performance Metrics (First 6 Months):

- 99.99% system uptime
- Zero security incidents resulting in operational disruption
- 127 potential threats automatically detected and mitigated
- Average incident response time reduced from 45 minutes to 90 seconds
- 100% compliance with regulatory requirements achieved

2. Cost-Benefit Analysis:

- Annual security operating costs reduced by 32%
- Insurance premiums decreased by 15%
- Operational efficiency improved by 8.5%
- ROI achieved within 9 months of deployment

6. Legal and Compliance Achievements

1. Certifications Obtained:

- ISO 27001:2022 certification
- IEC 62443 compliance
- Dutch NCSC security requirements
- EU GDPR compliance validation

2. Audit Results:

- Successfully passed Port Authority security audit
- Achieved highest rating in independent penetration testing
- Compliant with all applicable maritime security regulations

7. Confidentiality and Usage Rights

1. This case study and all information contained herein is confidential and proprietary to DeepShield Systems, Inc. ("DeepShield").

2. Usage Rights: This document may be used solely for internal due diligence purposes and may not be disclosed to third parties without DeepShield's prior written consent.

3. All technical specifications, methodologies, and performance metrics contained herein are protected under U.S. Patent Nos. 11,234,567 and 11,234,568.

8. Verification and Authentication

The undersigned hereby certify that the information contained in this case study is accurate and complete to the best of their knowledge as of the date first written above.

```

_

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

_

James Morrison
```

VP of Engineering

DeepShield Systems, Inc.

Date: September 15, 2023

```

## 9. Disclaimer

This document is provided for informational purposes only and does not constitute a guarantee of results. Actual performance may vary based on specific deployment conditions and operational parameters. DeepShield makes no warranties, express or implied, regarding the information contained herein.

[END OF DOCUMENT]
```