Singapore Port Authority SCADA Integration Case Study

CONFIDENTIAL AND PROPRIETARY

DeepShield Systems, Inc.

Document Reference: CS-SPA-2023-001

1. Executive Summary

This case study documents the successful implementation of DeepShield Systems, Inc.'s ("DeepShield") industrial cybersecurity platform for the Singapore Port Authority's ("SPA") SCADA infrastructure during the period of March 2023 through September 2023. The integration encompassed comprehensive protection of maritime operational technology (OT) systems across four major terminal facilities.

2. Project Scope and Objectives

1. Primary deployment of DeepShield Maritime Shield(TM) v4.2 across:

- Container Terminal Operations Control Systems
- Automated Guided Vehicle (AGV) Networks
- Vessel Traffic Management Systems
- Terminal Operating System (TOS) Infrastructure

2. Implementation of real-time threat monitoring and response capabilities for:

- 847 networked OT devices
- 23 SCADA control systems
- 156 programmable logic controllers (PLCs)
- 4 terminal management networks

3. Technical Implementation

1. System Architecture

The deployment utilized DeepShield's proprietary three-layer security architecture:

- Layer 1: Deep packet inspection and protocol analysis
- Layer 2: AI-driven behavioral analytics
- Layer 3: Automated incident response and containment

2. Integration Points

- Primary SCADA network segmentation
- OT/IT convergence boundaries
- Legacy system interfaces
- Emergency shutdown systems (ESD)

3. Security Controls

- Real-time threat detection and response
- Zero-trust architecture implementation
- Automated asset discovery and inventory
- Continuous vulnerability assessment

4. Operational Results

1. Key Performance Metrics

- 99.99% system availability maintained
- Zero security incidents during implementation
- 100% critical asset coverage
- 47% reduction in false positive alerts

2. Operational Improvements

- 68% reduction in incident response time
- 92% automation of security workflows
- 100% compliance with maritime cybersecurity regulations
- Enhanced visibility across OT infrastructure

5. Compliance and Certification

1. Regulatory Framework

- Maritime and Port Authority of Singapore (MPA) requirements
- IEC 62443 industrial security standards
- ISO 27001:2013 information security management
- NIST Cybersecurity Framework

2. Certifications Achieved

- MPA Cybersecurity Code of Practice
- Classification Society Type Approval
- Lloyd's Register OT Security Certification

6. Risk Management

1. Risk Mitigation Measures

- Continuous monitoring and threat detection
- Automated incident response procedures
- Regular security assessments and penetration testing
- Backup and recovery systems implementation

2. Incident Response Protocol

- 24/7 Security Operations Center (SOC) support
- Defined escalation procedures
- Emergency response team activation
- Stakeholder communication framework

7. Confidentiality and Intellectual Property

1. This case study and all information contained herein is confidential and proprietary to DeepShield Systems, Inc. All rights reserved.

2. No part of this document may be reproduced, distributed, or transmitted in any form without the prior written permission of DeepShield Systems, Inc.

8. Legal Disclaimers

1. This document is provided for informational purposes only and does not constitute a warranty, guarantee, or contractual obligation.

2. DeepShield Systems, Inc. makes no representations or warranties regarding the accuracy, completeness, or reliability of the information contained herein.

9. Document Control

Document Owner: Legal Department

Version: 1.0

Last Updated: December 15, 2023

Classification: Confidential

Distribution: Authorized Personnel Only

10. Approval and Authorization

APPROVED AND AUTHORIZED BY:

_

Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

_

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: December 15, 2023

[END OF DOCUMENT]