SOC 2 Type II Audit Report

Independent Service Auditor's Report

Q4 2023 (October 1, 2023 - December 31, 2023)

DeepShield Systems, Inc.

Report of Independent Service Auditors

To the Board of Directors of DeepShield Systems, Inc.:

Scope

We have examined DeepShield Systems, Inc.'s ("DeepShield" or "the Company") description of its Industrial Cybersecurity Platform system for the period October 1, 2023 to December 31, 2023 (the "Description") and the suitability of the design and operating effectiveness of controls to meet the criteria for the security, availability, and confidentiality principles set forth in TSP section 100, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Service Organization's Responsibilities

DeepShield Systems, Inc. is responsible for:

- Preparing the Description and accompanying assertions
- Providing the services covered by the Description
- Specifying the control objectives and stating them in the Description
- Identifying the risks that threaten the achievement of the control objectives
- Selecting the criteria
- Designing, implementing, and documenting controls to meet the applicable Trust Services Criteria

Service Auditor's Responsibilities

Our responsibility is to express an opinion based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects:

The Description fairly presents the system throughout the period October 1, 2023 to December 31, 2023

The controls were suitably designed to provide reasonable assurance that the applicable Trust Services Criteria would be met if the controls operated effectively throughout the period

The controls operated effectively to provide reasonable assurance that the applicable Trust Services Criteria were met throughout the period

System Description

Overview of Services Provided

DeepShield Systems provides an integrated industrial cybersecurity platform that delivers:

- OT network monitoring and protection
- AI-driven threat detection
- Real-time anomaly identification
- Automated incident response
- Specialized maritime and subsea infrastructure security modules

Infrastructure

The DeepShield platform operates on a distributed architecture comprising:

- Primary data centers: AWS US-East-1 and US-West-2
- Edge processing nodes at customer sites
- Redundant monitoring facilities in Boston, MA and Austin, TX
- Backup and disaster recovery infrastructure in AWS US-West-1

Software

Key software components include:

- DeepShield Core Platform v4.2
- OT Network Analysis Engine v3.1
- Maritime Security Module v2.5
- Threat Intelligence Platform v3.3
- Customer Portal v4.0

People

Organizational structure includes dedicated teams for:

- Security Operations
- Platform Engineering
- Customer Success
- Compliance & Risk Management
- Research & Development

Control Environment

Control Framework

DeepShield maintains a comprehensive control environment aligned with:

- NIST Cybersecurity Framework
- IEC 62443 Industrial Security Standards
- ISO 27001:2013 Information Security Management

Risk Assessment

Quarterly risk assessments evaluate:

- Emerging cyber threats
- Operational technology vulnerabilities
- Industrial control system exposures
- Maritime infrastructure risks
- Compliance requirements

Monitoring Controls

Continuous monitoring includes:

- 24/7 Security Operations Center
- Automated system health checks
- Real-time threat detection
- Performance metrics tracking
- Compliance monitoring

Test of Controls and Results

Security Controls

Control ID	Description	Test Procedure	Result
SEC-01	Access control policies	Reviewed documentation and tested implementation	Effective
SEC-02	Encryption standards	Validated encryption protocols	Effective
SEC-03	Incident response	Simulated security incidents	Effective
SEC-04	Network segmentation	Tested network isolation	Effective

Availability Controls

Control ID	Description	Test Procedure	Result
AVL-01	System redundancy	Tested failover procedures	Effective
AVL-02	Backup systems	Validated backup integrity	Effective
AVL-03	Disaster recovery	Conducted DR exercises	Effective

Confidentiality Controls

Control ID	Description	Test Procedure	Result
CON-01	Data classification	Reviewed classification procedures	Effective
CON-02	Information handling	Tested data protection measures	Effective
CON-03	Third-party management	Evaluated vendor controls	Effective

Findings and Recommendations

Notable Findings

Control Implementation

- All tested controls were found to be effectively designed and operating
- No material weaknesses identified
- Minor opportunities for enhancement noted

System Performance

- Platform availability exceeded 99.99%

- All security incidents properly detected and remediated
- Backup systems performed as designed

Recommendations

Enhancement Opportunities

- Implement additional API security controls
- Enhance third-party risk monitoring
- Strengthen change management documentation

Forward-Looking Improvements

- Consider implementing zero trust architecture
- Expand maritime threat detection capabilities
- Enhance supply chain security controls

Independent Auditor's Opinion

In our opinion, in all material respects:

a) The Description fairly presents DeepShield Systems' Industrial Cybersecurity Platform system throughout the period October 1, 2023 to December 31, 2023.

b) The controls stated in the Description were suitably designed to provide reasonable assurance that the applicable Trust Services Criteria would be met.

c) The controls operated effectively to provide reasonable assurance that the applicable Trust Services Criteria were met throughout the specified period.

Restrictions on Use

This report is intended solely for use by the management of DeepShield Systems, Inc., its customers, and the independent auditors of its customers.

Prepared by:

CyberTrust Assurance LLP

Boston, Massachusetts

January 15, 2024

[SEAL]

CyberTrust Assurance LLP

AICPA SOC 2 Certified Auditor

License #CT20241234