THREAT INTELLIGENCE COLLECTION & ANALYSIS

Standard Operating Procedure

DeepShield Systems, Inc.

Document ID: SOP-TI-2024-001

Effective Date: January 15, 2024

Version: 2.1

1. PURPOSE AND SCOPE

1. This Standard Operating Procedure ("SOP") establishes the protocols and requirements for threat intelligence collection, analysis, and dissemination within DeepShield Systems, Inc. ("Company") to support the protection of industrial control systems (ICS) and operational technology (OT) environments.

2. This SOP applies to all Company personnel involved in threat intelligence operations, including but not limited to security analysts, threat researchers, and incident response teams.

2. DEFINITIONS

1. "Threat Intelligence" means processed information regarding actual or potential threats to Company clients' industrial control systems, SCADA networks, and related OT infrastructure.

2. "Collection Sources" means approved channels for gathering threat data, including proprietary sensors, third-party feeds, industry partnerships, and open-source intelligence (OSINT).

3. "Maritime-Specific Intelligence" means threat data specifically relevant to maritime and subsea infrastructure protection systems.

3. COLLECTION METHODOLOGY

1. Authorized Collection Sources

a) DeepShield proprietary sensor network

b) Licensed third-party threat feeds

c) Industry information sharing partnerships

d) Government advisory channels

e) Open-source intelligence platforms

2. Collection Requirements

a) All intelligence collection must comply with applicable laws and regulations

b) Data collection must be documented in the approved tracking system

c) Sources must be validated for reliability and accuracy

d) Maritime-specific collection requires additional verification protocols

4. ANALYSIS PROCEDURES

1. Initial Assessment

a) Automated triage using DeepShield AI analysis engine

b) Human analyst review of high-priority threats

c) Correlation with existing threat databases

d) Impact assessment for specific client sectors

2. Validation Requirements

a) Minimum two independent sources for critical threats

b) Technical verification of exploit mechanisms

c) Operational impact analysis

d) False positive elimination procedures

5. DISSEMINATION PROTOCOLS

1. Classification Levels

a) Critical - immediate action required

b) High - action required within 24 hours

c) Medium - action required within 72 hours

d) Low - informational awareness

2. Distribution Methods

a) Automated alerts through DeepShield platform

b) Secure client portal notifications

c) Direct communication for critical threats

d) Regular threat intelligence bulletins

6. QUALITY CONTROL

1. Analysis Quality Metrics

a) False positive rate monitoring

b) Time to detection measurements

c) Analysis accuracy tracking

d) Client feedback integration

2. Review Requirements

a) Quarterly audit of collection sources

b) Monthly analysis methodology review

c) Weekly threat assessment calibration

d) Daily collection coverage verification

7. COMPLIANCE AND DOCUMENTATION

1. Required Records

a) Source validation documentation

b) Analysis worksheets and reports

c) Dissemination logs

d) Quality control metrics

2. Retention Requirements

a) Raw intelligence data: 180 days

b) Analysis reports: 3 years

c) Dissemination records: 2 years

d) Audit logs: 5 years

8. CONFIDENTIALITY

1. All threat intelligence data collected and analyzed under this SOP shall be treated as Company Confidential Information and protected accordingly.

2. Access to threat intelligence systems and data shall be restricted to authorized personnel with

appropriate security clearance levels.

9. AMENDMENTS AND REVIEWS

1. This SOP shall be reviewed annually by the Chief Security Architect.

2. Amendments require approval from both the Chief Technology Officer and Chief Security Architect.

APPROVALS

APPROVED BY:

Dr. Elena Rodriguez
Chief Security Architect
Date: January 15, 2024

Sarah Blackwood
Chief Technology Officer
Date: January 15, 2024

DOCUMENT CONTROL

Version History:

- 2.1: January 15, 2024 - Updated collection sources and retention requirements
- 2.0: July 1, 2023 - Major revision incorporating maritime-specific protocols
- 1.0: March 15, 2022 - Initial release

End of Document