SECURITY EVENT INVESTIGATION PROCEDURES

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document ID: SEC-INV-2024-001

Version: 2.0

1. PURPOSE AND SCOPE

1. This document establishes the mandatory procedures for investigating and responding to security events affecting DeepShield Systems, Inc.'s ("Company") industrial control system (ICS) security solutions, operational technology (OT) environments, and related critical infrastructure protection systems.

2. These procedures apply to all security events impacting:

a) Company's proprietary deep-layer security architecture

b) Customer SCADA networks and industrial automation systems

c) Maritime and subsea infrastructure protection modules

d) AI-driven threat detection systems

e) Real-time monitoring infrastructure

f) Automated incident response mechanisms

2. DEFINITIONS

1. "Security Event" means any observed or suspected occurrence that may indicate a compromise or threat to the Company's or customers' systems, including but not limited to:

- Unauthorized access attempts
- System anomalies
- Data breaches
- Malware detection
- OT protocol violations
- Industrial control system irregularities

2. "Investigation Team" refers to the cross-functional team responsible for investigating security events, comprising representatives from:

- Security Operations
- Engineering
- Legal Department
- Customer Success
- Executive Leadership (as required)

3. INITIAL RESPONSE PROCEDURES

1. Event Detection and Classification

a) All security events shall be immediately logged in the Incident Management System

b) Events shall be classified according to the following severity levels:

- Level 1: Critical - Immediate threat to critical infrastructure
- Level 2: High - Significant system compromise
- Level 3: Medium - Limited system impact
- Level 4: Low - Minor security concern

2. Notification Requirements

a) Level 1 events require immediate notification to:

- Chief Security Architect
- VP of Engineering
- General Counsel
- CEO

b) Level 2-4 events follow standard escalation protocols

4. INVESTIGATION PROCESS

1. Evidence Collection

a) Create forensic copies of affected systems

b) Preserve all relevant logs and system data

c) Document chain of custody for all evidence

d) Maintain investigation timeline

e) Record all investigative actions

2. Analysis Requirements

a) Conduct root cause analysis

b) Identify attack vectors and methods

c) Assess scope of impact

d) Evaluate effectiveness of existing controls

e) Determine regulatory reporting obligations

3. Documentation Standards

a) All findings must be documented in the approved template

b) Include technical details and supporting evidence

c) Document remediation recommendations

d) Prepare executive summary

e) Maintain investigation confidentiality

5. REMEDIATION AND REPORTING

1. Remediation Planning

a) Develop immediate containment measures

b) Create short-term mitigation strategy

c) Establish long-term security improvements

d) Define success metrics

e) Assign responsibility for implementation

2. Required Reports

a) Initial Incident Report (within 24 hours)

b) Preliminary Findings Report (within 72 hours)

c) Final Investigation Report (within 10 business days)

d) Post-Incident Review (within 30 days)

6. CUSTOMER AND REGULATORY NOTIFICATIONS

1. Customer Communications

a) Legal Department must approve all customer notifications

b) Follow contractual notification requirements

c) Maintain communication log

d) Provide regular status updates

2. Regulatory Reporting

a) Comply with applicable reporting deadlines

b) Submit required documentation

c) Coordinate with external counsel as needed

d) Maintain copies of all submissions

7. CONFIDENTIALITY AND PRIVILEGE

1. All investigation materials shall be marked "CONFIDENTIAL - ATTORNEY-CLIENT PRIVILEGED"

2. Investigation communications must be restricted to essential personnel

3. External communications require Legal Department approval

8. REVIEW AND UPDATES

1. This procedure shall be reviewed annually by the Security Operations team

2. Updates require approval from:

- Chief Security Architect
- General Counsel
- VP of Engineering

APPROVAL

APPROVED BY:

Dr. Elena Rodriguez

Chief Security Architect

Date: January 15, 2024

James Morrison

VP of Engineering

Date: January 15, 2024