Security Incident Response Plan

DeepShield Systems, Inc.

Version 3.1

Effective Date: January 15, 2024

1. Purpose and Scope

1. This Security Incident Response Plan ("Plan") establishes the procedures and responsibilities for responding to security incidents affecting DeepShield Systems, Inc.'s ("Company") industrial control system (ICS) security solutions, operational technology (OT) environments, and related critical infrastructure protection systems.

2. This Plan applies to all Company employees, contractors, and third-party service providers who have access to or maintain Company systems, particularly those handling customer OT environments and SCADA networks.

2. Definitions

1. "Security Incident" means any actual or suspected event that threatens the confidentiality, integrity, or availability of Company systems, customer environments, or protected data, including but not limited to:

a) Unauthorized access to ICS components

b) Malware detection in OT networks

c) Anomalous behavior in SCADA systems

d) Breach of maritime or subsea infrastructure controls

e) Compromise of deep-layer security architecture

2. "Incident Response Team" or "IRT" means the cross-functional team responsible for managing security incidents, comprised of:

a) Chief Security Architect (Team Lead)

b) VP of Engineering

c) Senior OT Security Engineers

d) Legal Counsel

e) Customer Success Representatives

3. Incident Classification and Severity Levels

1. Level 1 - Critical

- Direct impact on critical infrastructure
- Multiple customer environments affected
- Potential safety implications
- Response Time: Immediate (15 minutes)

2. Level 2 - High

- Single customer environment affected
- Significant system degradation
- No immediate safety risk
- Response Time: 1 hour

3. Level 3 - Medium

- Limited system impact
- No customer environment affected
- Routine security events
- Response Time: 4 hours

4. Incident Response Procedures

1. Detection and Reporting

a) All incidents must be reported to the IRT via:

- Security Operations Center: +1 (888) 555-0123
- Email: incident@deepshield.com
- Internal ticketing system: IRT-Alert

2. Initial Assessment

a) IRT Lead shall:

- Validate incident reports
- Assign severity level
- Initiate response protocols
- Document initial findings

3. Containment and Mitigation

a) Implement immediate actions to:

- Isolate affected systems
- Preserve evidence
- Deploy countermeasures
- Activate backup systems if required

4. Customer Communication

a) For Level 1 and 2 incidents:

- Notify affected customers within 1 hour
- Provide status updates every 2 hours
- Document all communications

5. Recovery and Post-Incident Analysis

1. System Recovery

a) Verify system integrity

b) Implement security patches

c) Restore from verified backups

d) Conduct security testing

e) Obtain customer approval for production restoration

2. Documentation Requirements

a) Incident timeline

b) Actions taken

c) Systems affected

d) Customer impact

e) Root cause analysis

f) Preventive measures implemented

6. Training and Plan Maintenance

1. Training Requirements

a) Annual incident response training for all technical staff

b) Quarterly tabletop exercises for IRT

c) Monthly security awareness updates

2. Plan Review

a) Quarterly review by Chief Security Architect

b) Annual audit by external security firm

c) Updates based on incident learnings and industry standards

7. Compliance and Reporting

1. Regulatory Requirements

a) Report incidents per applicable regulations:

- CISA requirements for critical infrastructure
- Maritime cybersecurity regulations
- State data breach notification laws

2. Documentation Retention

a) Maintain incident records for 5 years

b) Preserve chain of custody for evidence

c) Secure storage of incident artifacts

8. Confidentiality

1. All information related to security incidents shall be treated as confidential and shared only on a need-to-know basis.

9. Amendments

1. This Plan may be amended by the Chief Security Architect with approval from Legal Counsel and the CEO.

Approval and Version Control

Version: 3.1

Approved By: Dr. Elena Rodriguez, Chief Security Architect

Date: January 15, 2024

Next Review: July 15, 2024