Security Incident Response Workflow Design

DeepShield Systems, Inc.

Document Version: 1.2

Effective Date: January 15, 2024

Classification: Confidential

1. Purpose and Scope

1. This Security Incident Response Workflow Design ("Workflow") establishes the standardized procedures and protocols for responding to cybersecurity incidents affecting DeepShield Systems, Inc.'s ("DeepShield") industrial control system (ICS) security infrastructure and client environments.

2. This Workflow applies to all security incidents involving DeepShield's proprietary deep-layer security architecture, including but not limited to:

a) SCADA network breaches

b) OT system compromises

c) Maritime infrastructure attacks

d) Industrial automation system anomalies

e) Critical infrastructure security events

2. Definitions

1. "Security Incident" means any actual or suspected unauthorized access, breach, compromise, or disruption of protected systems or data.

2. "Response Team" means DeepShield's designated incident response personnel, including the Chief Security Architect, Security Operations Center (SOC) analysts, and relevant technical specialists.

3. "Client Environment" means any operational technology infrastructure protected by DeepShield's security solutions.

3. Incident Classification and Triage

1. Initial Assessment

a) Severity Level 1 - Critical: Direct threat to critical infrastructure operations

b) Severity Level 2 - High: Significant system compromise with potential operational impact

c) Severity Level 3 - Medium: Limited breach with containable impact

d) Severity Level 4 - Low: Minor security events requiring standard response

2. Response Time Requirements

- Level 1: Immediate response (15 minutes)
- Level 2: Rapid response (1 hour)
- Level 3: Standard response (4 hours)
- Level 4: Routine response (24 hours)

4. Response Procedures

1. Initial Detection and Notification

a) Automated detection through DeepShield's AI-driven threat detection system

b) SOC analyst verification and preliminary assessment

c) Notification to designated Response Team members

d) Client notification as per service level agreements

2. Containment and Analysis

a) Implementation of immediate containment measures

b) Isolation of affected systems where necessary

c) Deep-layer security architecture analysis

d) Threat vector identification and documentation

e) Impact assessment on connected systems

3. Remediation Actions

a) Deployment of adaptive defense mechanisms

b) System restoration procedures

c) Security patch implementation

d) Configuration adjustments

e) Real-time monitoring enhancement

5. Documentation Requirements

1. Incident Documentation

- Incident ID and classification
- Timeline of events
- Systems affected
- Actions taken
- Response team members involved
- Client impact assessment

2. Post-Incident Analysis
- Root cause analysis
- Effectiveness of response measures
- Recommendations for system improvements
- Updates to security protocols
- Client communication records

6. Communication Protocols

1. Internal Communications
- Designated communication channels
- Escalation procedures
- Status update frequency
- Management notification requirements

2. External Communications
- Client notification procedures
- Regulatory reporting requirements
- Public relations protocols
- Legal compliance documentation

7. Compliance and Audit

1. This Workflow shall comply with:
- ISO 27001 requirements
- NIST Cybersecurity Framework
- Industry-specific regulations

- Client contractual obligations

2. Regular audit requirements:

- Quarterly workflow effectiveness review
- Annual comprehensive assessment
- Third-party security audits
- Compliance verification documentation

8. Confidentiality

1. All information related to security incidents shall be treated as strictly confidential and shared only on a need-to-know basis in accordance with DeepShield's Information Security Policy.

9. Updates and Maintenance

1. This Workflow shall be reviewed and updated:

- Annually at minimum
- Following major security incidents
- Upon significant technology changes
- As required by regulatory updates

10. Authorization

This Security Incident Response Workflow Design is approved and authorized by:

Dr. Elena Rodriguez
Chief Security Architect
DeepShield Systems, Inc.

Sarah Blackwood
Chief Technology Officer
DeepShield Systems, Inc.

Date: January 15, 2024