Incident Response Playbook: Critical Infrastructure

DeepShield Systems, Inc.

Version 3.2 - Last Updated: January 11, 2024

Document Classification: CONFIDENTIAL

1. Purpose and Scope

1. This Incident Response Playbook ("Playbook") establishes mandatory procedures for responding to cybersecurity incidents affecting critical infrastructure protected by DeepShield Systems, Inc. ("DeepShield") solutions.

2. This Playbook applies to all incidents involving:

a) Industrial Control Systems (ICS)

b) Supervisory Control and Data Acquisition (SCADA) networks

c) Operational Technology (OT) environments

d) Maritime and subsea infrastructure

e) Critical manufacturing systems

2. Incident Classification Matrix

1. **Level 1 - Minor Incident**

- Isolated anomaly detection
- No operational impact
- Response Time: Within 4 hours

2. **Level 2 - Moderate Incident**

- Multiple system alerts
- Limited operational impact
- Response Time: Within 2 hours

3. **Level 3 - Severe Incident**

- Active breach detected
- Significant operational impact
- Response Time: Within 30 minutes

4. **Level 4 - Critical Incident**

- System compromise confirmed
- Critical infrastructure affected
- Response Time: Immediate

3. Initial Response Protocol

1. **Incident Detection and Validation**

- Automated alert through DeepShield Platform
- Manual verification by Security Operations Center (SOC)
- Preliminary impact assessment
- Incident level classification

2. **Notification Requirements**

- Internal: Security Response Team, Executive Leadership
- External: Affected Client, Regulatory Bodies (as required)
- Documentation of all communications

4. Technical Response Procedures

1. **Containment Measures**

- Implementation of AI-driven isolation protocols
- Network segmentation activation
- Emergency shutdown procedures (if required)
- Real-time system state preservation

2. **Investigation Process**

- Deep-layer security architecture analysis
- Threat vector identification
- System integrity verification
- Evidence collection and preservation

3. **Remediation Steps**

- Deployment of adaptive defense mechanisms

- System restoration procedures
- Security patch implementation
- Verification of operational stability

5. Communication Protocol

1. **Internal Communication**

- Incident Response Team activation
- Executive briefing requirements
- Status update frequency
- Documentation requirements

2. **Client Communication**

- Notification templates by incident level
- Regular status updates
- Technical briefing procedures
- Post-incident reporting

3. **Regulatory Reporting**

- Compliance requirements by jurisdiction
- Mandatory reporting timeframes
- Documentation standards
- Follow-up procedures

6. Recovery and Post-Incident Procedures

1. **System Restoration**

- Operational verification protocol
- Performance testing requirements
- Security control validation
- Documentation of restoration steps

2. **Post-Incident Analysis**

- Root cause analysis

- Impact assessment
- Control effectiveness evaluation
- Recommendations for improvement

3. **Documentation Requirements**

- Incident timeline
- Response actions taken
- System modifications made
- Lessons learned

7. Training and Maintenance

1. **Training Requirements**

- Annual team certification
- Quarterly tabletop exercises
- Technical skill validation
- Documentation review

2. **Playbook Maintenance**

- Quarterly review schedule
- Update procedures
- Version control
- Distribution protocol

8. Legal and Compliance

1. This Playbook shall be reviewed annually by DeepShield's Legal Department.

2. All actions taken pursuant to this Playbook must comply with:

- Client contractual obligations
- Applicable regulatory requirements
- Industry standards and best practices

9. Confidentiality

1. This document contains confidential and proprietary information of DeepShield Systems, Inc. and shall not be disclosed without written authorization.

Approval and Implementation

This Playbook is approved and implemented as of January 11, 2024.

–

Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

–

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

–

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.