Incident Response Automation Framework Guide

DeepShield Systems, Inc.

Document Version: 2.4

Last Updated: January 11, 2024

Classification: CONFIDENTIAL

1. Purpose and Scope

1. This Incident Response Automation Framework Guide ("Framework") establishes the authorized protocols and procedures for DeepShield Systems, Inc.'s ("Company") automated incident response capabilities within its Industrial Control System (ICS) security platform.

2. This Framework applies to all automated response actions implemented through the DeepShield(TM) Platform across customer operational technology (OT) environments, SCADA networks, and maritime/subsea infrastructure deployments.

2. Definitions

1. "Automated Response Action" means any programmatic security countermeasure executed by the Platform without direct human intervention.

2. "Critical Infrastructure Systems" means customer industrial control systems designated as critical to operations per NIST SP 800-82r3 guidelines.

3. "Platform" means the Company's proprietary DeepShield(TM) Industrial Cybersecurity Platform and all associated modules.

4. "Response Policy" means the customer-specific automation rules and parameters configured within the Platform.

3. Authorization Framework

1. All automated response capabilities must be:

a) Explicitly authorized in writing by the customer's designated security authority

b) Configured according to customer-approved Response Policies

c) Limited to pre-defined actions within approved operational parameters

d) Subject to automatic rollback capabilities

e) Logged with complete audit trails

2. The Platform shall maintain segregation between:

a) Detection functions

b) Response decision engines

c) Execution mechanisms

d) Logging/audit systems

4. Automated Response Categories

1. Network Segmentation Actions

- Dynamic VLAN reconfiguration
- Port-level access control
- Traffic filtering rule updates
- Emergency network isolation

2. System Protection Actions

- Critical process protection
- Configuration lockdown
- Emergency backup initiation
- Fail-safe mode activation

3. Threat Containment Actions

- Malicious connection termination
- Compromised device quarantine
- Command validation filtering
- Protocol restriction enforcement

5. Safety Controls and Limitations

1. The Platform shall enforce the following safety controls:

a) No automated actions affecting safety-instrumented systems

b) Mandatory human approval for actions impacting critical processes

c) Automatic timeout/rollback for incomplete response sequences

d) Real-time notification of all automated actions

e) Emergency manual override capabilities

2. Response Policy configurations must include:

a) Explicit action whitelisting

b) Maximum impact thresholds

c) Process criticality exclusions

d) Time-of-day restrictions

e) Geographic scope limitations

6. Audit and Documentation Requirements

1. The Platform shall maintain comprehensive logs of:

- All automated response triggers
- Decision criteria evaluation
- Actions executed
- System state changes
- Override/rollback events

2. Documentation requirements include:

a) Current Response Policy configurations

b) Authorization audit trails

c) Testing/validation records

d) Incident response reports

e) Performance metrics

7. Compliance and Testing

1. All automated response capabilities shall:

a) Undergo quarterly validation testing

b) Maintain compliance with NERC CIP standards

c) Align with ISA/IEC 62443 requirements

d) Support NIST Cybersecurity Framework controls

2. Annual third-party assessment of:

- Algorithm effectiveness
- Safety control operation
- Policy enforcement
- Audit trail completeness

8. Liability and Indemnification

1. The Company's liability regarding automated response actions shall be limited as specified in the Master Services Agreement.

2. Customers must maintain appropriate insurance coverage for operational risks related to automated response deployment.

9. Modifications and Updates

1. This Framework may be updated by the Company with 30 days written notice to customers.

2. Emergency updates may be implemented immediately if required to address critical security vulnerabilities.

Approval and Implementation

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

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

By:

Name: James Morrison

Title: VP of Engineering