SECURITY MONITORING ESCALATION PROCEDURES

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 3.2

Classification: CONFIDENTIAL

1. PURPOSE AND SCOPE

1. This document establishes the mandatory procedures for escalating security incidents detected within DeepShield Systems' Industrial Control System (ICS) Security Monitoring Operations.

2. These procedures apply to all Security Operations Center (SOC) personnel, incident response teams, and designated on-call engineers responsible for monitoring client OT environments.

2. DEFINITIONS

1. "Critical Infrastructure Event" means any detected anomaly or threat affecting client operational technology systems designated as Critical Infrastructure Protection (CIP) assets.

2. "Severity Levels" refer to the standardized incident classification system:

- Severity 1 (S1): Critical impact requiring immediate response
- Severity 2 (S2): High impact requiring rapid response
- Severity 3 (S3): Medium impact requiring standard response
- Severity 4 (S4): Low impact requiring routine response

3. "Response Time" means the maximum allowable time between incident detection and initiation of response procedures.

3. MONITORING RESPONSIBILITIES

1. Primary Monitoring

- 24/7 SOC staffing with minimum two (2) L1 analysts per shift
- Continuous real-time monitoring of DeepShield Security Platform alerts
- Baseline environment profiling and anomaly detection
- Initial incident triage and classification

2. Secondary Monitoring

- L2 analysts providing advanced analysis support
- OT specialists monitoring industrial protocol behaviors
- Maritime security specialists for subsea infrastructure clients
- Threat intelligence integration and correlation

4. ESCALATION PROCEDURES

1. Severity 1 Incidents

- Immediate notification to SOC Manager and Security Director
- 15-minute maximum response time
- Activation of Incident Response Team
- Client notification within 30 minutes
- Hourly status updates until resolution

2. Severity 2 Incidents

- Notification to SOC Manager
- 30-minute maximum response time
- L2 analyst engagement required
- Client notification within 1 hour
- Status updates every 4 hours

3. Severity 3 Incidents

- Standard ticket creation and tracking
- 2-hour maximum response time
- L1 analyst handling with L2 consultation
- Client notification within 4 hours
- Daily status updates

4. Severity 4 Incidents

- Routine ticket handling
- 8-hour maximum response time
- L1 analyst handling

- Client notification in next scheduled report

5. NOTIFICATION CHAIN

1. Internal Escalation Path

L1 SOC Analyst

L2 Senior Analyst

SOC Manager

Security Director

CTO

CEO (for S1 incidents only)

2. Client Notification Requirements

- Primary Technical Contact
- Secondary Technical Contact
- Client Security Manager
- Executive Sponsor (S1 incidents only)

6. DOCUMENTATION REQUIREMENTS

1. Incident Records

- Timestamp of detection
- Initial severity classification
- All escalation actions taken
- Response team members involved
- Client communications log
- Resolution actions and timeline
- Post-incident analysis findings

2. Required Reports

- Incident Summary Report
- Technical Analysis Report
- Root Cause Analysis (S1 and S2 only)
- Remediation Recommendations

- Compliance Impact Assessment

7. COMPLIANCE AND AUDIT

1. All escalation activities must comply with:

- ISO 27001 requirements
- NIST Cybersecurity Framework
- Client-specific compliance obligations
- Maritime cybersecurity regulations (where applicable)

2. Quarterly audits of escalation procedures including:

- Response time compliance
- Documentation completeness
- Client notification compliance
- Resolution effectiveness

8. REVIEW AND UPDATES

1. This procedure shall be reviewed and updated:

- Annually at minimum
- Following any S1 incident
- Upon significant platform changes
- As required by regulatory changes

9. AUTHORITY AND ENFORCEMENT

1. These procedures are authorized by the Chief Security Architect and CTO of DeepShield Systems, Inc.

2. Compliance with these procedures is mandatory for all relevant personnel.

3. Violations may result in disciplinary action up to and including termination.

Approved by:

Dr. Elena Rodriguez

Chief Security Architect

Date: January 15, 2024

Sarah Blackwood

Chief Technology Officer

Date: January 15, 2024