SECURITY OPERATIONS CENTER (SOC) PROCEDURES MANUAL

DeepShield Systems, Inc.

Version 3.2 - Last Updated: January 11, 2024

Document Classification: CONFIDENTIAL

1. INTRODUCTION AND SCOPE

1. This Security Operations Center (SOC) Procedures Manual ("Manual") establishes the operational framework and standard procedures for DeepShield Systems, Inc.'s ("Company") Security Operations Center, which provides 24/7 monitoring and incident response for industrial control systems (ICS) and operational technology (OT) environments.

2. This Manual applies to all SOC personnel, contractors, and authorized third parties accessing or operating within the Company's SOC facilities or systems.

2. DEFINITIONS

1. "Critical Alert" means any security event classified as Severity 1 or 2 according to the Company's Incident Classification Matrix.

2. "ICS Environment" means any industrial control system, SCADA network, or operational technology infrastructure monitored by the SOC.

3. "Incident Response Team" or "IRT" means the designated group of security professionals responsible for investigating and responding to security incidents.

4. "SOC Platform" means the Company's proprietary DeepShield(TM) security monitoring and response platform.

3. SOC ORGANIZATIONAL STRUCTURE

1. The SOC shall maintain the following staffing levels at all times:

a) One (1) SOC Manager

b) Two (2) Senior Security Analysts (Level 3)

c) Four (4) Security Analysts (Level 2)

d) Six (6) Junior Security Analysts (Level 1)

2. Shift Coverage Requirements:

a) Three (3) analysts minimum per shift

b) One (1) Level 2 or higher analyst must be present

c) Remote backup analyst on call 24/7

4. MONITORING AND DETECTION PROCEDURES

1. Continuous Monitoring

a) Real-time monitoring of all connected ICS environments

b) Automated threat detection using AI-driven analytics

c) Regular system health checks every 30 minutes

2. Alert Triage Process

a) Initial assessment within 5 minutes of alert generation

b) Severity classification per Incident Classification Matrix

c) Escalation to appropriate response team

3. Documentation Requirements

a) All alerts logged in SOC Platform

b) Detailed notes for investigation steps

c) Chain of custody maintenance for evidence

5. INCIDENT RESPONSE PROTOCOLS

1. Critical Alert Response

a) Immediate notification to IRT and affected client

b) Activation of incident response playbook

c) Executive briefing within 30 minutes

2. Containment Procedures

a) Isolation of affected systems

b) Implementation of emergency controls

c) Client coordination for operational impact

3. Recovery Operations

a) System restoration procedures

b) Verification of security controls

c) Return to normal operations checklist

6. REPORTING AND COMMUNICATION

1. Required Reports

a) Daily SOC activity summary

b) Weekly threat intelligence briefing

c) Monthly performance metrics

d) Quarterly trend analysis

2. Client Communications

a) Incident notification templates

b) Status update procedures

c) After-action report requirements

7. QUALITY ASSURANCE AND COMPLIANCE

1. Performance Metrics

a) Alert response time

b) False positive rate

c) Mean time to detection

d) Resolution accuracy

2. Compliance Requirements

a) Annual SOC 2 Type II audit

b) Quarterly internal audits

c) Monthly compliance reviews

8. TRAINING AND CERTIFICATION

1. Required Certifications

a) Level 1: Security+ or equivalent

b) Level 2: CISSP or equivalent

c) Level 3: GIAC or equivalent

2. Ongoing Training

a) Monthly technical training

b) Quarterly tabletop exercises

c) Annual certification renewal

9. CONFIDENTIALITY AND ACCESS CONTROL

1. All SOC personnel must maintain strict confidentiality regarding client information, security incidents, and SOC operations.

2. Access to SOC facilities and systems requires:

a) Valid security clearance

b) Signed confidentiality agreement

c) Biometric authentication

d) Regular access review

10. AMENDMENTS AND REVIEWS

1. This Manual shall be reviewed and updated annually or upon significant operational changes.

2. All amendments must be approved by:

a) Chief Security Architect

b) VP of Engineering

c) Chief Technology Officer

APPROVAL AND EXECUTION

This Manual is hereby approved and adopted:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: _

James Morrison

VP of Engineering

DeepShield Systems, Inc.

Date: _