SECURITY OPERATIONS CENTER (SOC) STANDARD PROCEDURES

DeepShield Systems, Inc.

Effective Date: January 1, 2024

Document Version: 3.2

Classification: CONFIDENTIAL

1. PURPOSE AND SCOPE

1. This document establishes the standard operating procedures for DeepShield Systems, Inc.'s Security Operations Center (SOC), which provides 24/7/365 monitoring and incident response for industrial control systems (ICS), operational technology (OT) environments, and critical infrastructure protection services.

2. These procedures apply to all SOC personnel, contractors, and authorized third parties involved in security monitoring, incident response, and threat management activities.

2. DEFINITIONS

1. "Alert" means any system-generated notification indicating potential security concerns requiring analysis.

2. "Critical Infrastructure" refers to systems, networks, and assets vital to national security, economic security, or public health and safety.

3. "Incident" means any confirmed or suspected security breach, unauthorized access, or anomalous activity affecting protected systems.

4. "OT Environment" means operational technology systems used to monitor and control industrial processes.

3. SOC ORGANIZATION AND STAFFING

1. Organizational Structure

- Level 1: Security Analysts (24/7 monitoring)
- Level 2: Senior Security Engineers

- Level 3: Security Architects and Incident Response Leaders
- SOC Manager
- Chief Security Architect

2. Minimum Staffing Requirements

- At least three (3) Level 1 analysts per shift
- One (1) Level 2 engineer on-call
- One (1) Level 3 specialist available for escalation

4. MONITORING AND DETECTION

1. Continuous Monitoring

- Real-time monitoring of client OT networks
- SCADA system activity analysis
- Industrial protocol inspection
- Behavioral anomaly detection
- AI-driven threat pattern recognition

2. Alert Classification

- Priority 1: Critical (immediate response required)
- Priority 2: High (response within 15 minutes)
- Priority 3: Medium (response within 1 hour)
- Priority 4: Low (response within 4 hours)

5. INCIDENT RESPONSE PROCEDURES

1. Initial Assessment

- Validate alert authenticity
- Determine incident scope and impact
- Classify incident severity
- Initiate response protocols

2. Escalation Protocol

- Level 1 to Level 2: After 30 minutes without resolution

- Level 2 to Level 3: Critical incidents or unresolved within 2 hours
- Executive notification: All Priority 1 incidents

3. Client Communication

- Initial notification within defined SLA timeframes
- Regular status updates every 30 minutes for active incidents
- Post-incident reports within 24 hours

6. DOCUMENTATION AND REPORTING

1. Required Documentation

- Incident tickets with complete chronological details
- Response actions and outcomes
- System changes and configurations
- Client communications log
- Evidence preservation records

2. Regular Reports

- Daily shift handover reports
- Weekly incident summaries
- Monthly performance metrics
- Quarterly trend analysis

7. COMPLIANCE AND AUDIT

1. Regulatory Compliance

- Maintenance of NERC CIP compliance
- ISO 27001 controls implementation
- NIST Cybersecurity Framework alignment
- Industry-specific regulatory requirements

2. Audit Requirements

- Quarterly internal audits
- Annual external compliance audits

- Regular penetration testing
- Process effectiveness reviews

8. CONFIDENTIALITY AND DATA PROTECTION

1. All SOC personnel must maintain strict confidentiality regarding:
- Client identities and information
- Incident details and responses
- Security vulnerabilities
- Proprietary tools and procedures

2. Data handling requirements:
- Encryption of all client data
- Secure storage and transmission
- Access control and authentication
- Regular data disposal per retention policies

9. TRAINING AND CERTIFICATION

1. Required Certifications
- CompTIA Security+
- Certified Information Systems Security Professional (CISSP)
- Industrial Control Systems Security certification
- DeepShield proprietary certifications

2. Ongoing Training
- Monthly technical training sessions
- Quarterly tabletop exercises
- Annual certification renewal
- Emerging threat briefings

10. REVIEW AND UPDATES

1. This document shall be reviewed and updated:
- Annually at minimum

- Following major incidents
- Upon significant technology changes
- As required by regulatory changes

APPROVAL AND EXECUTION

APPROVED AND ADOPTED by DeepShield Systems, Inc.

Date: January 1, 2024

_

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

_

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.