SCADA SYSTEMS MONITORING GUIDELINES

DeepShield Systems, Inc.

Effective: January 1, 2024 - March 31, 2024

Document ID: DSS-SCADA-2024-Q1-001

1. PURPOSE AND SCOPE

1. These Guidelines establish mandatory protocols for monitoring Supervisory Control and Data Acquisition (SCADA) systems within DeepShield Systems, Inc.'s ("Company") operational environment and client deployments.

2. These Guidelines apply to all employees, contractors, and authorized third parties involved in SCADA system monitoring, maintenance, or security operations.

2. DEFINITIONS

1. "SCADA System" refers to the industrial control system architecture comprising computers, networked data communications, and graphical user interfaces for high-level process supervisory management.

2. "Critical Alert" means any system notification indicating potential compromise, unauthorized access attempt, or operational anomaly requiring immediate response.

3. "Monitoring Personnel" refers to authorized individuals responsible for SCADA system surveillance and incident response.

3. MONITORING REQUIREMENTS

1. System Coverage

a) Continuous 24/7 monitoring of all SCADA network segments

b) Real-time surveillance of control system communications

c) Active monitoring of all remote terminal units (RTUs)

d) Automated logging of all system events and operator actions

2. Personnel Requirements

a) Minimum two (2) certified monitoring personnel per shift

b) At least one (1) senior analyst on-call at all times

c) Quarterly certification renewal for all monitoring staff

d) Mandatory security clearance level "DSS-3" or higher

4. ALERT PROTOCOLS

1. Critical Alert Response

a) Maximum response time of 5 minutes for Critical Alerts

b) Immediate notification to Security Operations Center

c) Incident documentation per DSS-INC-2024 procedures

d) Mandatory escalation for alerts lasting >15 minutes

2. Alert Classification

a) Level 1: System anomaly - routine investigation

b) Level 2: Potential security threat - elevated response

c) Level 3: Confirmed intrusion attempt - immediate action

d) Level 4: System compromise - emergency protocols

5. DOCUMENTATION AND REPORTING

1. Required Documentation

a) Shift logs with system status updates every 30 minutes

b) Incident reports for all Level 2+ alerts

c) Monthly system performance analytics

d) Quarterly security assessment reports

2. Retention Requirements

a) Alert logs: minimum 3 years

b) System performance data: minimum 5 years

c) Incident reports: minimum 7 years

d) Personnel certifications: duration of employment +1 year

6. COMPLIANCE AND AUDIT

1. Internal Audits

a) Monthly review of monitoring procedures

b) Quarterly assessment of alert response times

c) Semi-annual security protocol evaluation

d) Annual comprehensive system audit

2. External Compliance

a) ISO 27001 standards adherence

b) NIST Cybersecurity Framework compliance

c) Industry-specific regulatory requirements

d) Client-mandated security protocols

7. SECURITY PROTOCOLS

1. Access Control

a) Multi-factor authentication for all monitoring stations

b) Biometric verification for physical access

c) Role-based access control (RBAC) implementation

d) Quarterly access review and adjustment

2. Communication Security

a) Encrypted communication channels

b) Secure VPN for remote access

c) Dedicated monitoring network segment

d) Regular security key rotation

8. EMERGENCY PROCEDURES

1. System Failure Response

a) Immediate activation of backup monitoring systems

b) Implementation of manual control procedures

c) Client notification within 15 minutes

d) Emergency response team deployment

2. Disaster Recovery

a) Activation of alternate monitoring facility

b) Implementation of continuity protocols

c) System restoration procedures

d) Post-incident analysis requirements

9. AMENDMENTS AND UPDATES

1. These Guidelines shall be reviewed and updated quarterly or as required by operational needs.

2. All amendments must be approved by the Chief Security Architect and VP of Engineering.

10. AUTHORIZATION

These Guidelines are hereby authorized and enacted by:

Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: January 1, 2024

End of Document