SCADA SYSTEMS MONITORING GUIDELINES

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document ID: DSS-OPS-2024-001

1. PURPOSE AND SCOPE

1. These SCADA Systems Monitoring Guidelines ("Guidelines") establish the mandatory procedures and protocols for monitoring, maintaining, and securing 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 who access, operate, or maintain SCADA systems under the Company's purview.

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 Infrastructure" means systems and assets, whether physical or virtual, so vital that their incapacity or destruction would have a debilitating impact on security, economic security, or public health or safety.

3. "OT Environment" means the operational technology environment containing industrial control systems, including SCADA systems, distributed control systems (DCS), and other control system configurations.

3. MONITORING REQUIREMENTS

1. Continuous Monitoring Protocol

a) SCADA systems must be monitored 24/7/365 through the DeepShield Advanced Monitoring Platform.

b) Real-time telemetry data shall be collected at intervals not exceeding 500 milliseconds.

c) All monitoring activities must be logged with UTC timestamp and operator ID.

2. Performance Metrics

a) System availability shall be maintained at 99.999% or higher.

b) Response time for critical alerts shall not exceed 30 seconds.

c) Monthly performance reports shall be generated and reviewed by the Security Operations Center.

4. SECURITY CONTROLS

1. Access Control

a) Multi-factor authentication is mandatory for all SCADA system access.

b) Access privileges shall be reviewed quarterly and updated based on the principle of least privilege.

c) Remote access shall only be permitted through Company-approved secure channels.

2. Network Segmentation

a) SCADA networks must be physically or logically separated from corporate networks.

b) Firewall rules shall be reviewed monthly and updated as needed.

c) All inter-zone communications must be encrypted using approved protocols.

5. INCIDENT RESPONSE

1. Detection and Classification

a) Incidents shall be classified according to the Company's Severity Matrix.

b) Automated detection systems must generate alerts within 5 seconds of anomaly detection.

2. Response Protocol

a) Critical incidents require immediate escalation to the Security Operations Center.

b) Response teams must be activated within 15 minutes of critical alert generation.

c) Incident containment measures must be implemented within 30 minutes.

6. COMPLIANCE AND AUDIT

1. Regulatory Compliance

a) All monitoring activities must comply with applicable regulations including NERC CIP, IEC 62443, and ISO 27001.

b) Compliance assessments shall be conducted quarterly.

2. Audit Requirements

a) Internal audits shall be conducted semi-annually.

b) External audits shall be performed annually by certified third-party assessors.

c) Audit findings must be addressed within 30 days of report issuance.

7. MAINTENANCE AND UPDATES

1. System maintenance shall be performed according to the following schedule:

a) Daily: System health checks and log review

b) Weekly: Performance optimization and threat signature updates

c) Monthly: Security patch assessment and deployment

d) Quarterly: Full system backup and recovery testing

2. Change Management

a) All system changes require documented approval through the Change Advisory Board.

b) Emergency changes must follow expedited approval procedures.

8. DOCUMENTATION AND REPORTING

1. Required Documentation

a) System configuration documentation must be maintained and updated monthly.

b) Incident reports must be filed within 24 hours of resolution.

c) Training records must be maintained for all authorized personnel.

2. Reporting Requirements

a) Monthly performance reports shall be submitted to executive management.

b) Quarterly compliance reports shall be provided to the Board of Directors.

c) Annual security assessment reports shall be maintained for 5 years.

9. AMENDMENTS AND REVIEW

1. These Guidelines shall be reviewed annually and updated as necessary to reflect changes in technology, threats, and business requirements.

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

10. APPROVAL AND EXECUTION

APPROVED AND ADOPTED this 15th day of January, 2024.

DeepShield Systems, Inc.

By:

Dr. Elena Rodriguez

Chief Security Architect

By:

James Morrison

VP of Engineering