NETWORK TRAFFIC ANALYSIS PROCEDURES

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 3.2

Classification: CONFIDENTIAL

1. PURPOSE AND SCOPE

1. This document establishes the procedures and protocols for network traffic analysis within DeepShield Systems, Inc.'s ("Company") operational technology (OT) and industrial control system (ICS) environments.

2. These procedures apply to all network monitoring, analysis, and threat detection activities conducted across the Company's proprietary deep-layer security architecture and client deployments.

2. DEFINITIONS

1. "Network Traffic" means all data flows, protocols, and communications traversing monitored industrial networks.

2. "Analysis Systems" means the Company's proprietary AI-driven monitoring platforms, including DeepShield Maritime(TM) and DeepShield ICS Protect(TM).

3. "Critical Infrastructure" means facilities, systems, and assets designated as essential under applicable regulations and standards.

4. "Anomaly Detection" means automated identification of network behavior deviating from established baselines.

3. MONITORING PROTOCOLS

1. Continuous Monitoring Requirements

a) All protected OT networks shall maintain 24/7/365 traffic monitoring using Company-approved analysis systems.

b) Monitoring must capture both north-south and east-west traffic flows within segmented industrial networks.

c) Traffic analysis shall occur at OSI layers 2-7 with particular focus on industrial protocols including Modbus, DNP3, and proprietary ICS communications.

2. Data Collection Parameters

a) Network traffic metadata shall be retained for a minimum of 180 days.

b) Full packet capture shall be maintained for a minimum of 30 days for all critical systems.

c) Encrypted traffic analysis must employ approved deep packet inspection (DPI) methods.

4. ANALYSIS PROCEDURES

1. Baseline Establishment

a) Network behavior baselines shall be established through minimum 30-day learning periods.

b) Baselines must be reviewed and updated quarterly or upon significant infrastructure changes.

c) Separate baselines shall be maintained for different operational states and maintenance windows.

2. Anomaly Detection

a) AI-driven analysis engines shall continuously evaluate traffic patterns against established baselines.

b) Minimum detection criteria shall include:

- Protocol violations
- Unauthorized connection attempts
- Command sequence anomalies
- Traffic volume deviations
- Temporal pattern variations

3. Threat Classification

a) Detected anomalies shall be classified according to the Company's five-tier threat matrix.

b) Classification must consider:

- Potential impact to operations
- Historical pattern correlation

- Asset criticality
- Attack vector analysis
- Threat intelligence correlation

5. RESPONSE PROTOCOLS

1. Automated Response

a) Tier 1-2 threats shall trigger automated response mechanisms including:

- Traffic filtering
- Connection termination
- VLAN segregation
- Alert generation

b) Automated responses must be logged and reviewed within 24 hours.

2. Manual Investigation

a) Tier 3-5 threats require immediate manual investigation by qualified security personnel.

b) Investigation procedures shall follow the Company's Incident Response Plan.

6. REPORTING AND DOCUMENTATION

1. Regular Reporting

a) Weekly summary reports shall be generated for all monitored networks.

b) Monthly trend analysis reports shall be provided to security management.

c) Quarterly effectiveness assessments shall be conducted and documented.

2. Incident Documentation

a) All Tier 3-5 events require detailed incident reports including:

- Traffic analysis logs
- Response actions taken
- Root cause determination
- Mitigation recommendations

7. COMPLIANCE AND REVIEW

1. These procedures shall be reviewed annually and updated as needed.

2. Compliance with these procedures shall be audited quarterly by the Security Operations team.

3. Deviations from these procedures must be documented and approved by the Chief Security Architect.

8. CONFIDENTIALITY

1. This document contains confidential and proprietary information of DeepShield Systems, Inc.

2. Unauthorized disclosure or distribution is strictly prohibited.

APPROVAL AND EXECUTION

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

DEEPSHIELD SYSTEMS, INC.

By:

Dr. Elena Rodriguez

Chief Security Architect

By:

Sarah Blackwood

Chief Technology Officer