SECURITY LOGGING AND MONITORING PROCEDURES

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 3.2

Classification: Confidential

1. PURPOSE AND SCOPE

1. This document establishes the mandatory procedures for security logging and monitoring across DeepShield Systems, Inc.'s ("Company") operational technology (OT) environments, industrial control systems (ICS), and supporting infrastructure.

2. These procedures apply to all Company employees, contractors, and automated systems involved in the monitoring, collection, storage, and analysis of security logs and events.

2. DEFINITIONS

1. "Security Event" means any observable occurrence in a system or network indicating a potential breach of security policy, failure of safeguards, or a previously unknown situation that may be security relevant.

2. "SIEM" means Security Information and Event Management system, specifically the Company's DeepShield Enterprise Monitor platform.

3. "Critical Assets" means any Company or client ICS components, SCADA systems, or OT infrastructure designated as severity level 1 or 2 under the Company's Asset Classification Policy.

3. LOG COLLECTION AND RETENTION

1. Mandatory Log Sources

a) All Critical Assets must maintain detailed logging of:

- Authentication attempts and access control changes
- Configuration modifications
- System and process starts/stops
- Network traffic anomalies
- Security control activations/deactivations

- Firmware updates and patch applications

2. Retention Requirements

a) Level 1 Critical Asset logs: 24 months minimum

b) Level 2 Critical Asset logs: 18 months minimum

c) Supporting infrastructure logs: 12 months minimum

d) System health metrics: 6 months minimum

3. Log Protection

a) All logs must be encrypted at rest using AES-256

b) Log transmission must utilize TLS 1.3 or higher

c) Access to raw logs requires dual authentication

d) Integrity verification via SHA-512 hashing

4. MONITORING PROCEDURES

1. Real-time Monitoring

a) The Security Operations Center (SOC) shall maintain 24/7/365 active monitoring of all Critical Assets

b) Automated analysis must process all logs within 30 seconds of receipt

c) Critical alerts must be investigated within 5 minutes of generation

2. Automated Analysis Requirements

a) Machine learning models must be retrained monthly

b) False positive rates must remain below 0.1%

c) Pattern matching rules must be reviewed quarterly

d) Correlation rules must span minimum 30-day windows

3. Alert Classification

a) Severity 1 - Immediate response required (5 minutes)

b) Severity 2 - Rapid response required (15 minutes)

c) Severity 3 - Standard response required (1 hour)

d) Severity 4 - Routine investigation required (24 hours)

5. RESPONSE PROCEDURES

1. Initial Assessment

a) SOC analysts must follow the Incident Response Playbook

b) All alerts require documented initial assessment

c) Escalation paths must be clearly identified

d) Client notification requirements must be verified

2. Investigation Requirements

a) All investigations must be logged in the Incident Management System

b) Chain of custody procedures must be followed for all evidence

c) Regular status updates required per severity level

d) Root cause analysis mandatory for Severity 1 & 2 events

6. REPORTING AND METRICS

1. Required Reports

a) Daily SOC summary (internal)

b) Weekly security metrics dashboard

c) Monthly trend analysis

d) Quarterly compliance verification

e) Annual effectiveness review

2. Performance Metrics

a) Mean time to detect (MTTD) 1 minute

b) Mean time to respond (MTTR) 15 minutes

c) Alert processing accuracy 99.9%

d) System uptime 99.99%

7. COMPLIANCE AND AUDIT

1. Internal Audit Requirements

a) Quarterly review of logging coverage

b) Semi-annual procedure compliance audit

c) Annual effectiveness assessment

d) Random spot checks monthly

2. External Validation

a) Annual third-party security assessment

b) Bi-annual penetration testing

c) Quarterly compliance verification

8. REVIEW AND UPDATES

1. This document shall be reviewed and updated at least annually or upon significant changes to the Company's security infrastructure.

2. All updates require approval from the Chief Security Architect and CTO.

9. DOCUMENT CONTROL

Document Owner: Chief Security Architect

Last Review Date: January 15, 2024

Next Review Date: January 15, 2025

Version: 3.2

APPROVED BY:

Dr. Elena Rodriguez

Chief Security Architect

Date: January 15, 2024

Sarah Blackwood

Chief Technology Officer

Date: January 15, 2024