Security Metrics and KPI Dashboard Guide

DeepShield Systems, Inc.

Document Version: 1.2

Effective Date: January 15, 2024

Classification: Confidential - Internal Use Only

1. Purpose and Scope

1. This Security Metrics and KPI Dashboard Guide ("Guide") establishes the standardized framework for measuring, tracking, and reporting security performance metrics across DeepShield Systems, Inc.'s ("Company") industrial control system (ICS) security operations and client deployments.

2. This Guide applies to all security monitoring activities conducted through the DeepShield(TM) Platform and associated security operations centers (SOCs).

2. Definitions

1. "Critical Metrics" refers to the core set of security performance indicators designated as essential for operational risk assessment.

2. "KPI Dashboard" refers to the Company's proprietary visualization interface for security metrics within the DeepShield(TM) Platform.

3. "Reporting Period" means the standard monthly measurement cycle, unless otherwise specified for particular metrics.

3. Core Security Metrics

1. Threat Detection Metrics

- Mean Time to Detect (MTTD): Target < 15 minutes
- False Positive Rate (FPR): Target < 0.5%
- Threat Classification Accuracy: Target > 99.5%
- Zero-Day Threat Detection Rate: Target > 95%

2. Response Metrics

- Mean Time to Respond (MTTR): Target < 30 minutes

- Incident Resolution Rate: Target > 98%
- Automated Response Success Rate: Target > 99%
- Manual Intervention Rate: Target < 5%

3. System Performance Metrics

- Platform Uptime: Target > 99.999%
- Sensor Network Health: Target > 99.9%
- Data Processing Latency: Target < 100ms
- API Response Time: Target < 250ms

4. Dashboard Configuration

1. Access Control

- Dashboard access shall be role-based according to the Company's security clearance matrix
- All access attempts shall be logged and audited
- Multi-factor authentication is required for administrative access

2. Visualization Requirements

- Real-time data updates at minimum 5-second intervals
- Customizable views based on user role and preferences
- Export capabilities in standard formats (CSV, PDF, XLSX)
- Automated alerting for metric threshold violations

5. Reporting Requirements

1. Standard Reports

- Daily Security Summary Report
- Weekly Trend Analysis Report
- Monthly Executive Dashboard
- Quarterly Compliance Review

2. Client-Specific Reporting

- Customized reporting templates per client requirements
- Automated report generation and distribution

- Secure delivery through encrypted channels
- Retention according to client contract terms

6. Compliance and Audit

1. All metrics shall be stored in compliance with:
- ISO 27001 requirements
- NIST Cybersecurity Framework
- Client-specific regulatory requirements
- Industry-standard retention policies

2. Audit Requirements
- Quarterly internal audits of metric accuracy
- Annual external validation of measurement systems
- Regular calibration of monitoring tools
- Documentation of all audit findings

7. Review and Updates

1. This Guide shall be reviewed and updated:
- Annually at minimum
- Upon significant platform changes
- Following major security incidents
- As required by regulatory changes

2. All updates must be approved by:
- Chief Security Architect
- VP of Engineering
- Compliance Officer

8. Confidentiality

1. All metrics, reports, and associated data are classified as Confidential Information under the Company's Information Security Policy.

2. Distribution of metrics and reports is restricted to authorized personnel only.

9. Disclaimer

This Guide contains proprietary and confidential information of DeepShield Systems, Inc. Unauthorized use, disclosure, or reproduction is strictly prohibited. The Company reserves the right to modify this Guide at any time without prior notice.

10. Authorization

APPROVED AND ADOPTED by DeepShield Systems, Inc.

By:

Dr. Elena Rodriguez

Chief Security Architect

Date: January 15, 2024

By:

James Morrison

VP of Engineering

Date: January 15, 2024