Network Traffic Baseline Analysis Guide

DeepShield Systems, Inc.

Document Version: 2.4

Last Updated: January 11, 2024

Classification: Confidential & Proprietary

1. Purpose and Scope

1. This Network Traffic Baseline Analysis Guide ("Guide") establishes the standardized methodology and procedures for conducting baseline analysis of operational technology (OT) network traffic within industrial control system (ICS) environments protected by DeepShield Systems, Inc. ("DeepShield") security solutions.

2. This Guide applies to all network traffic analysis conducted on customer networks utilizing DeepShield's Deep-Layer Security Architecture(TM) and associated monitoring systems.

2. Definitions

1. "Baseline Period" means the initial 30-day monitoring period following system deployment during which normal network behavior patterns are established.

2. "Critical Control Points" refers to the designated network segments and nodes identified as essential for maintaining operational integrity.

3. "Traffic Pattern Signature" means the documented characteristics of normal network communications, including but not limited to protocol usage, data flow volumes, timing patterns, and endpoint relationships.

3. Baseline Analysis Requirements

1. Initial Data Collection

a) Minimum monitoring duration of 30 consecutive days

b) Coverage of all operational states and cycles

c) Documentation of scheduled maintenance windows

d) Capture of all protocol-specific traffic patterns

e) Recording of authorized device communications

2. Mandatory Analysis Parameters

a) Protocol distribution metrics

b) Peak and average bandwidth utilization

c) Source/destination relationship mapping

d) Temporal pattern analysis

e) Control system state correlation

f) Authentication event logging

4. Analysis Methodology

1. Data Collection Process

a) Deploy passive monitoring sensors at designated Critical Control Points

b) Enable full packet capture for specified protocols

c) Implement filtering rules per DeepShield's Protocol Analysis Framework

d) Maintain chain of custody for collected data

e) Apply data retention policies as specified in Section 7

2. Pattern Recognition Requirements

a) Establish protocol-specific behavioral models

b) Document recurring communication patterns

c) Identify operational dependencies

d) Map network topology relationships

e) Validate against known-good configurations

5. Documentation Requirements

1. Baseline Analysis Report must include:

a) Executive summary

b) Methodology description

c) Data collection parameters

d) Statistical analysis results

e) Pattern identification findings

f) Anomaly thresholds

g) Recommendations for monitoring rules

2. Supporting Documentation

a) Raw data retention specifications

b) Analysis tool configurations

c) Filtering rule sets

d) Validation procedures

e) Quality control measures

6. Security Controls

1. All baseline analysis activities must comply with:

a) DeepShield's Information Security Policy

b) Customer-specific security requirements

c) Industry regulatory standards

d) Data protection regulations

e) Confidentiality agreements

2. Data Protection Requirements

a) Encryption of collected data

b) Secure storage protocols

c) Access control mechanisms

d) Audit trail maintenance

e) Secure disposal procedures

7. Data Retention and Disposal

1. Retention Requirements

a) Raw traffic data: 90 days

b) Analysis results: 1 year

c) Baseline reports: 3 years

d) Configuration records: Duration of engagement

2. Disposal Procedures

a) Secure deletion of electronic records

b) Physical destruction of storage media

c) Documentation of disposal actions

d) Customer notification requirements

8. Legal Compliance

1. This Guide shall be implemented in accordance with:

a) All applicable federal and state laws

b) Industry regulatory requirements

c) Customer contractual obligations

d) DeepShield's compliance framework

9. Proprietary Rights

1. This Guide and all methodologies described herein are the exclusive property of DeepShield Systems, Inc. and are protected by intellectual property laws.

2. No part of this Guide may be reproduced, distributed, or transmitted without prior written authorization from DeepShield Systems, Inc.

10. Document Control

Document Owner: Chief Security Architect

Review Frequency: Annual

Last Review Date: January 11, 2024

Next Review Date: January 11, 2025

APPROVED BY:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

James Morrison

VP of Engineering

DeepShield Systems, Inc.

Date: _