SECURITY TOOL CONFIGURATION STANDARDS

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 3.2

Classification: Confidential

1. PURPOSE AND SCOPE

1. This Security Tool Configuration Standards document ("Standards") establishes mandatory configuration requirements for all security tools deployed within DeepShield Systems, Inc.'s ("Company") technology infrastructure, with particular emphasis on industrial control system (ICS) security solutions and operational technology (OT) environments.

2. These Standards apply to all security tools utilized in the Company's proprietary deep-layer security architecture, including but not limited to:

a) Network monitoring systems

b) Threat detection platforms

c) SCADA security controls

d) Maritime infrastructure protection modules

e) Automated incident response systems

2. DEFINITIONS

1. "Security Tools" means any software, hardware, or integrated system components used to protect, monitor, detect, or respond to security threats.

2. "Critical Configuration" means essential security parameters that directly impact the effectiveness of security controls.

3. "OT Environment" means operational technology systems used in industrial control and automation processes.

3. BASELINE CONFIGURATION REQUIREMENTS

1. Authentication and Access Control

a) Multi-factor authentication mandatory for administrative access

b) Role-based access control (RBAC) implementation required

c) Minimum password length of 16 characters

d) Password rotation every 90 days

e) Session timeout after 15 minutes of inactivity

2. Logging and Monitoring

a) Security event logging enabled at maximum detail level

b) Log retention period of 365 days minimum

c) Real-time alert configuration for critical events

d) Automated log backup every 24 hours

e) Tamper-detection mechanisms enabled

4. SPECIALIZED OT SECURITY CONFIGURATIONS

1. SCADA Network Protection

a) Deep packet inspection enabled

b) Protocol-specific filtering rules

c) Whitelist-based communication control

d) Industrial protocol validation

e) Asset inventory automation enabled

2. Maritime Infrastructure Controls

a) Subsea communication encryption

b) Position-based authentication

c) Vessel tracking integration

d) Maritime-specific threat signatures

e) Emergency isolation protocols

5. COMPLIANCE AND AUDIT

1. Configuration Validation

a) Weekly automated configuration checks

b) Monthly manual security audits

c) Quarterly compliance reviews

d) Annual third-party assessment

2. Documentation Requirements

a) Configuration change logging

b) Deviation justification records

c) Incident response documentation

d) Compliance validation reports

6. MAINTENANCE AND UPDATES

1. Regular maintenance windows must be established for:

a) Security signature updates

b) Firmware upgrades

c) Configuration optimization

d) Performance tuning

e) Threat intelligence integration

2. Emergency Updates

a) Critical vulnerability patching within 24 hours

b) Zero-day threat response procedures

c) Emergency configuration rollback capabilities

7. EXCEPTIONS AND DEVIATIONS

1. All exceptions to these Standards must be:

a) Documented in writing

b) Approved by Chief Security Architect

c) Reviewed quarterly

d) Time-limited to maximum 6 months

e) Risk-assessed and mitigated

8. ENFORCEMENT

1. Compliance with these Standards is mandatory for all Company employees, contractors, and third-party service providers.

2. Violations may result in:

a) Immediate system access revocation

b) Disciplinary action

c) Contract termination

d) Legal action as appropriate

9. REVIEW AND UPDATES

1. These Standards shall be reviewed and updated:

a) Annually at minimum

b) Upon significant technology changes

c) Following major security incidents

d) As required by regulatory changes

APPROVAL AND EXECUTION

APPROVED AND ADOPTED by the undersigned authorized representatives of DeepShield Systems, Inc.

Date: January 15, 2024

Dr. Elena Rodriguez

Chief Security Architect

Sarah Blackwood

Chief Technology Officer

James Morrison

VP of Engineering