THREAT HUNTING PLAYBOOK v2.0

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Classification: CONFIDENTIAL

1. INTRODUCTION AND SCOPE

1. This Threat Hunting Playbook ("Playbook") establishes the standard operating procedures and methodologies for proactive threat detection and response within DeepShield Systems, Inc.'s ("Company") industrial control system (ICS) and operational technology (OT) environments.

2. This Playbook applies to all security operations personnel, incident response teams, and authorized third-party contractors engaged in threat hunting activities across the Company's protected infrastructure.

2. DEFINITIONS

1. "Threat Hunting" refers to the proactive and iterative searching through networks and datasets to detect and isolate advanced threats that evade existing security solutions.

2. "IOCs" means Indicators of Compromise, including but not limited to malicious IP addresses, file hashes, domain names, and behavioral patterns.

3. "OT Environment" encompasses all operational technology systems, industrial control systems, SCADA networks, and related infrastructure protected by the Company's security solutions.

3. THREAT HUNTING METHODOLOGY

1. Hypothesis Formation

- Development of threat scenarios based on current intelligence
- Analysis of potential attack vectors specific to industrial systems
- Identification of critical assets and potential compromise indicators

2. Data Collection and Processing

- Real-time telemetry from OT network sensors
- System logs from industrial control systems

- SCADA protocol analysis data
- Maritime subsystem monitoring feeds

3. Investigation Procedures

- Pattern analysis using Company's proprietary AI algorithms
- Behavioral anomaly detection in industrial processes
- Cross-correlation of security events across multiple facilities
- Deep-packet inspection of OT network traffic

4. EXECUTION PROTOCOLS

1. Authorization Requirements

- Level 1 Hunt: Security Team Lead approval
- Level 2 Hunt: CISO or designee approval
- Level 3 Hunt: Executive Committee approval

2. Documentation Requirements

- Hunt ID assignment and tracking
- Hypothesis documentation and validation
- Evidence collection and preservation
- Chain of custody maintenance
- Results reporting and archival

5. SPECIALIZED HUNTING PROCEDURES

1. Maritime Infrastructure

- Subsea control system analysis
- Vessel automation system monitoring
- Port facility OT network inspection
- Maritime communication protocol verification

2. Industrial Control Systems

- PLC logic analysis
- SCADA system behavioral baseline monitoring

- Industrial network protocol inspection
- Control system configuration verification

6. INCIDENT RESPONSE INTEGRATION

1. Upon discovery of potential threats, the following escalation procedures shall be initiated:
- Immediate notification to Security Operations Center
- Activation of relevant incident response teams
- Implementation of containment procedures
- Evidence preservation and documentation
- Stakeholder notification per incident severity

7. REPORTING AND METRICS

1. Required Documentation
- Weekly hunt summary reports
- Monthly trend analysis
- Quarterly effectiveness assessments
- Annual program review

2. Key Performance Indicators
- Mean time to detect (MTTD)
- False positive ratio
- Threat hunting coverage metrics
- Resolution time tracking

8. COMPLIANCE AND AUDIT

1. This Playbook shall be reviewed and updated annually or upon significant changes to:
- Threat landscape
- Regulatory requirements
- Technology infrastructure
- Company security policies

2. All threat hunting activities shall comply with:

- NIST Cybersecurity Framework
- IEC 62443 standards
- Maritime cybersecurity regulations
- Client contractual requirements

9. CONFIDENTIALITY

1. All information contained within this Playbook and generated during threat hunting activities is classified as Confidential and shall be protected in accordance with the Company's data classification policies.

10. APPROVAL AND MAINTENANCE

This Playbook is approved and maintained by:

APPROVED BY:

Dr. Elena Rodriguez
Chief Security Architect
DeepShield Systems, Inc.

Sarah Blackwood
Chief Technology Officer
DeepShield Systems, Inc.

Date: January 15, 2024

Version: 2.0
Document Control: DS-THP-2024-001
Classification: CONFIDENTIAL
Next Review Date: January 15, 2025