Penetration Testing Guidelines - OT Systems

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.4

Classification: Confidential

1. Purpose and Scope

1. These Penetration Testing Guidelines ("Guidelines") establish the requirements and procedures for conducting security penetration testing on Operational Technology (OT) systems within DeepShield Systems, Inc. ("Company") and its clients' environments.

2. These Guidelines apply to all penetration testing activities involving industrial control systems (ICS), SCADA networks, maritime control systems, and other OT infrastructure managed or protected by the Company.

2. Definitions

1. "OT Systems" means operational technology systems, including but not limited to industrial control systems, programmable logic controllers (PLCs), distributed control systems (DCS), human-machine interfaces (HMI), and related industrial automation components.

2. "Penetration Test" means a controlled and authorized attempt to identify security vulnerabilities and weaknesses in OT Systems through systematic testing and assessment procedures.

3. "Testing Team" means qualified security professionals authorized by the Company to conduct penetration testing activities.

3. Pre-Testing Requirements

1. Authorization Requirements

a) Written approval from the Chief Security Architect

b) Signed client authorization for client-owned systems

c) Detailed scope definition and testing boundaries

d) Risk assessment and mitigation plan

e) Emergency response procedures

2. System Documentation

a) Current network architecture diagrams

b) System inventory and asset classification

c) Critical process documentation

d) Safety system interconnections

e) Backup verification documentation

4. Testing Methodology

1. Passive Assessment Phase

a) Network traffic analysis

b) Protocol identification

c) Asset discovery and enumeration

d) System behavior baseline establishment

2. Active Testing Phase

a) Controlled vulnerability scanning

b) Protocol-specific testing

c) Authentication mechanism assessment

d) Access control validation

e) Industrial protocol fuzzing

3. Prohibited Activities

a) Denial of service testing on production systems

b) Exploitation of safety-critical systems

c) Modification of control logic

d) Testing during critical operations

e) Unauthorized firmware modifications

5. Safety Controls

1. Mandatory Safety Measures

a) Real-time monitoring of system parameters

b) Emergency stop procedures

c) System restoration capabilities

d) Physical safety monitoring

e) Immediate access to system experts

2. Testing Windows

a) Testing limited to approved maintenance windows

b) Coordination with operational staff

c) Clear communication channels

d) Defined rollback points

6. Documentation Requirements

1. Test Documentation

a) Detailed test plans

b) Risk assessments

c) Testing schedules

d) Communication protocols

e) Emergency procedures

2. Reporting Requirements

a) Daily status reports

b) Incident documentation

c) Vulnerability findings

d) Mitigation recommendations

e) Executive summary

7. Confidentiality and Data Protection

1. All testing results, system information, and related documentation shall be treated as strictly confidential and subject to the Company's data classification policies.

2. Testing data must be encrypted at rest and in transit using Company-approved encryption standards.

8. Compliance and Regulatory Requirements

1. Testing activities must comply with:

a) NERC CIP standards

b) IEC 62443 requirements

c) Maritime cybersecurity regulations

d) Client-specific compliance requirements

e) Industry-specific standards

9. Incident Response

1. In the event of any unplanned system impact:

a) Immediately halt testing activities

b) Notify designated emergency contacts

c) Implement recovery procedures

d) Document incident details

e) Conduct post-incident review

10. Review and Updates

1. These Guidelines shall be reviewed annually by the Chief Security Architect and updated as necessary to reflect changes in technology, threats, and industry standards.

11. Enforcement

1. Violation of these Guidelines may result in disciplinary action, up to and including termination of employment or service agreements.

Approval and Authorization

These Guidelines are approved and authorized by:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date:

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: