RED TEAM EXERCISE GUIDELINES

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.0

Classification: CONFIDENTIAL

1. PURPOSE AND SCOPE

1. These Red Team Exercise Guidelines ("Guidelines") establish the framework and protocols for conducting authorized security assessment exercises at DeepShield Systems, Inc. ("Company") against industrial control systems (ICS), operational technology (OT) environments, and related critical infrastructure protection systems.

2. These Guidelines apply to all internal red team members, contracted security assessors, and relevant stakeholders involved in planning, executing, and evaluating red team exercises.

2. DEFINITIONS

1. "Red Team" refers to the authorized group of security professionals tasked with simulating real-world attacks against Company systems and infrastructure.

2. "Crown Jewels" refers to critical assets identified as high-value targets, including but not limited to:

a) DeepShield Maritime Protection Platform

b) SCADA Network Monitoring Systems

c) AI-Driven Threat Detection Engine

d) Client OT Environment Integration Points

3. "Exercise Window" refers to the authorized timeframe during which red team activities may be conducted.

3. AUTHORIZATION REQUIREMENTS

1. All red team exercises must receive prior written authorization from:

a) Chief Security Architect

b) VP of Engineering

c) Chief Technology Officer

d) Legal Department Representative

2. Authorization requests must be submitted at least 30 days before the proposed exercise start date and include:

- Detailed exercise objectives
- Scope definition
- Risk assessment
- Recovery procedures
- Team composition
- Timeline

4. OPERATIONAL CONSTRAINTS

1. Prohibited Activities:

- Disruption of live client environments
- Modification of production data
- Denial of service attacks against critical systems
- Social engineering targeting client personnel
- Physical security breaches without explicit authorization

2. System Restrictions:

- Testing limited to designated development and staging environments
- Production system testing requires additional C-level approval
- Client data must remain encrypted at rest and in transit
- All testing activities must be logged and monitored

5. DOCUMENTATION AND REPORTING

1. Required Documentation:

- Exercise plan with detailed attack scenarios
- Real-time activity logs
- System impact assessments
- Vulnerability findings

- Remediation recommendations

2. Post-Exercise Reports must include:

- Executive summary
- Technical findings
- Risk classification
- Evidence collection
- Recommended security improvements
- Lessons learned

6. CONFIDENTIALITY AND DATA HANDLING

1. All exercise-related information is classified as Confidential and subject to:

- Need-to-know basis access
- Secure storage requirements
- Data retention policies
- Non-disclosure agreements

2. Exercise findings must be:

- Encrypted at rest
- Transmitted via secure channels
- Stored in approved repositories
- Destroyed per retention schedule

7. INCIDENT RESPONSE AND ESCALATION

1. Emergency Procedures:

- Immediate exercise termination protocols
- System restoration procedures
- Stakeholder notification requirements
- Evidence preservation guidelines

2. Escalation Matrix:

- Technical issues: Lead Red Team   Security Architecture

- Business impact: CTO   CEO
- Client concerns: Account Management   Legal
- Regulatory issues: Legal   Board of Directors

8. COMPLIANCE AND GOVERNANCE

1. Exercises must comply with:

- Industry regulations (NERC CIP, IEC 62443)
- Client contractual obligations
- Internal security policies
- Relevant privacy laws

2. Governance Structure:

- Security Review Board oversight
- Quarterly program assessment
- Annual policy review
- Independent audit requirements

9. AMENDMENTS AND REVIEWS

1. These Guidelines shall be reviewed annually by the Security Review Board.

2. Amendments require approval from:

- Chief Security Architect
- Chief Technology Officer
- Legal Department
- CEO

APPROVAL AND EXECUTION

IN WITNESS WHEREOF, the undersigned have executed these Guidelines as of the Effective Date.

–

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

_

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

_

James Morrison

VP of Engineering

DeepShield Systems, Inc.

Date: January 15, 2024