MALWARE RESPONSE PROTOCOL v2.5

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Control #: SEC-MRP-2024-01

1. PURPOSE AND SCOPE

1. This Malware Response Protocol ("Protocol") establishes mandatory procedures for identifying, containing, eradicating, and recovering from malware incidents affecting DeepShield Systems, Inc.'s ("Company") infrastructure, operational technology environments, and customer-deployed systems.

2. This Protocol applies to all Company employees, contractors, and authorized third parties who access or maintain Company systems or customer deployments.

2. DEFINITIONS

1. "Malware" means any software intentionally designed to cause damage to computer systems, servers, clients, or networks, including but not limited to viruses, worms, trojans, ransomware, spyware, and advanced persistent threats (APTs).

2. "Critical Infrastructure Systems" means operational technology (OT) environments, industrial control systems (ICS), SCADA networks, and related infrastructure protected by Company solutions.

3. "Incident Response Team" or "IRT" means the cross-functional team responsible for executing this Protocol, led by the Chief Security Architect or designated alternate.

3. INITIAL RESPONSE PROCEDURES

1. Detection and Reporting

a) All suspected malware incidents must be reported immediately to the Security Operations Center (SOC).

b) The SOC shall initiate the Incident Response Team notification cascade within 15 minutes of initial detection.

c) Customer-impacting incidents require notification to the Customer Success team within 30 minutes.

2. Initial Assessment

a) The IRT shall conduct preliminary impact analysis within 1 hour of detection.

b) Systems shall be classified as:

i) Level 1 - Critical Infrastructure Impact

ii) Level 2 - Internal Systems Impact

iii) Level 3 - Isolated Endpoint Impact

4. CONTAINMENT AND ERADICATION

1. Containment Procedures

a) Immediate isolation of affected systems through network segmentation

b) Suspension of affected user accounts and access credentials

c) Implementation of additional monitoring on adjacent systems

d) Documentation of all containment actions in the incident log

2. Evidence Preservation

a) Creation of forensic images prior to remediation

b) Preservation of logs and system state information

c) Chain of custody documentation for all collected evidence

d) Secure storage of evidence following Company retention policies

3. Eradication Steps

a) Identification and removal of malware using approved tools

b) Verification of system integrity post-removal

c) Implementation of additional security controls

d) Validation of successful eradication through monitoring

5. RECOVERY PROCEDURES

1. System Restoration

a) Restoration from verified clean backups where available

b) Clean installation and reconfiguration where necessary

c) Application of all security patches and updates

d) Verification of system functionality

2. Access Restoration

a) Reset of all compromised credentials

b) Implementation of additional authentication measures

c) Staged restoration of user access

d) Verification of access control effectiveness

6. NOTIFICATION AND REPORTING

1. Internal Communications

a) Executive briefing within 4 hours of detection

b) Regular status updates to affected departments

c) Post-incident summary to all employees

2. External Communications

a) Customer notifications per service level agreements

b) Regulatory notifications as legally required

c) Law enforcement contact when appropriate

d) Public relations statements if necessary

7. POST-INCIDENT ACTIVITIES

1. Analysis Requirements

a) Root cause analysis within 72 hours

b) Impact assessment documentation

c) Effectiveness evaluation of response actions

d) Identification of security gaps and recommendations

2. Protocol Updates

a) Review and revision of this Protocol based on lessons learned

b) Update of related security procedures and controls

c) Enhancement of detection and prevention capabilities

8. COMPLIANCE AND TRAINING

1. All IRT members must complete annual incident response training.

2. This Protocol shall be reviewed and updated at least annually.

3. Compliance with this Protocol is mandatory and violations may result in disciplinary action.

9. AUTHORITY AND GOVERNANCE

This Protocol is issued under the authority of the Chief Security Architect and approved by the Chief Technology Officer.

Approved by:

Dr. Elena Rodriguez
Chief Security Architect
Date: January 15, 2024

Sarah Blackwood
Chief Technology Officer
Date: January 15, 2024

Document Control: v2.5
Last Updated: January 15, 2024
Next Review: January 15, 2025