Incident Escalation Matrix

Document ID: IEM-v1.2

Effective Date: January 15, 2024

Last Updated: January 15, 2024

Document Owner: Security Operations Department

Classification: CONFIDENTIAL

1. Purpose and Scope

1. This Incident Escalation Matrix ("Matrix") establishes the formal escalation procedures and response protocols for security incidents affecting DeepShield Systems, Inc.'s ("DeepShield") industrial control system (ICS) security operations and client environments.

2. This Matrix applies to all employees, contractors, and authorized third parties involved in incident response activities related to DeepShield's security operations.

2. Incident Severity Levels

1. **Level 1 - Critical**
- Complete system failure affecting multiple clients
- Confirmed breach of critical infrastructure
- Active cyber attack affecting operational technology (OT) systems
- Life-safety systems compromise
- Maritime control system breach

2. **Level 2 - High**
- Partial system outage affecting single client
- Suspected unauthorized access to ICS
- Advanced persistent threat (APT) detection
- SCADA system anomalies
- Critical sensor malfunction

3. **Level 3 - Medium**
- Non-critical system alerts

- Minor configuration issues
- Isolated security events
- Performance degradation
- Policy violations

4. **Level 4 - Low**
- Routine maintenance issues
- Minor technical inquiries
- Documentation updates
- Non-urgent client requests
- System optimization needs

3. Escalation Tiers and Response Times

1. **Tier 1 - Security Operations Center (SOC)**
- Initial incident assessment
- First response within 15 minutes
- Incident logging and classification
- Basic containment measures
- Escalation determination

2. **Tier 2 - Technical Response Team**
- Advanced incident analysis
- Response within 30 minutes
- Specialized containment strategies
- Client communication coordination
- Incident stabilization

3. **Tier 3 - Security Architecture Team**
- Root cause analysis
- Response within 1 hour
- System-wide impact assessment
- Advanced threat mitigation

- Recovery planning

4. **Tier 4 - Executive Response Team**
- Strategic decision-making
- Response within 2 hours
- Stakeholder management
- Legal/regulatory compliance
- Crisis communication

4. Escalation Procedures

1. **Initial Assessment**
- SOC analyst evaluates incident severity
- Documents initial findings
- Implements immediate containment
- Notifies appropriate tier
- Initiates incident ticket

2. **Escalation Triggers**
- Incident duration exceeds 30 minutes
- Multiple clients affected
- Regulatory reporting required
- Physical infrastructure impact
- Data breach indicators

3. **Communication Protocol**
- Primary: Secure incident management system
- Secondary: Encrypted messaging platform
- Tertiary: Direct phone contact
- Emergency: 24/7 incident hotline
- Executive: Secure conference bridge

5. Authority and Responsibilities

1. **SOC Manager**

- Incident classification oversight
- Resource allocation
- Tier 1-2 escalation approval
- Initial client notification
- Incident report review

2. **Chief Security Architect**

- Technical response leadership
- Tier 3 escalation management
- Solution architecture review
- Recovery strategy approval
- Post-incident analysis

3. **CTO/Executive Team**

- Strategic response oversight
- External communication approval
- Regulatory compliance ensuring
- Resource authorization
- Crisis management leadership

6. Documentation Requirements

1. All incidents must be documented including:

- Incident timeline
- Response actions taken
- Resources deployed
- Client impact assessment
- Resolution details

2. Post-incident documentation must include:

- Root cause analysis
- Corrective actions

- Preventive measures
- Lessons learned
- Improvement recommendations

7. Review and Updates

1. This Matrix shall be reviewed:

- Quarterly for operational effectiveness
- Following major incidents
- Upon significant system changes
- As required by regulatory updates
- Annually at minimum

8. Compliance and Governance

1. This Matrix complies with:

- ISO 27001 requirements
- NIST Cybersecurity Framework
- Industry regulatory standards
- Client contractual obligations
- Corporate security policies

Authorization

APPROVED AND ADOPTED by DeepShield Systems, Inc.

By:

Dr. Marcus Chen

Chief Executive Officer

Date: January 15, 2024

By:

Sarah Blackwood

Chief Technology Officer

Date: January 15, 2024