NIGHTSHADE TECHNOLOGIES

CAPABILITY STATEMENT

CYBER RESILIENCY REDEFINED.

Offensive security. Threat-informed insight. Practical engineering. NightShade helps organizations validate exposure and strengthen operational resilience.

CORE CAPABILITIES

- Offensive Security Assessments
- Red Team Operations
- Cybersecurity Engineering
- Cybersecurity Consulting
- Malware & Vulnerability Research
- Threat-Informed Validation

THE NIGHTSHADE ADVANTAGE

Operator-led
Expert judgment guides testing and analysis.

Threat-informed
Relevant adversary behavior shapes each scenario.

AI-amplified
Intelligent automation extends operator tradecraft.

Validated risk
Attack paths connect exposure to operational impact.

Practical engineering
Controls aligned to real environments and missions.

Continuous resilience
Retesting and threat updates inform improvement.

HUMAN-LED. AI-AMPLIFIED.

info@nightshade-tech.com | (954) 358-9747
nightshade-technologies.com

NIGHTSHADE TECHNOLOGIES

SERVICES & APPROACH

OFFENSIVE INSIGHT. OPERATIONAL RESILIENCE.

Expert-led testing, adversary research, and practical engineering help your team understand exposure, validate defenses, and prioritize meaningful improvements.

CAPABILITIES IN PRACTICE

Offensive Security Assessments

Penetration testing and adversarial emulation validate exploit paths, identify weaknesses, and the operational impact of compromise.

Cybersecurity Engineering

Design, implement, and validate security controls that fit system functionality, mission requirements, and operational conditions.

Malware & Vulnerability Research

Analyze malicious software, investigate exploitable conditions, and connect technical evidence to detection and remediation priorities.

Red Team Operations

Realistic attack simulations evaluate how people, processes, and technology detect and respond to relevant adversary behavior.

Cybersecurity Consulting

Translate security priorities and compliance considerations into practical guidance aligned with your environment and resources.

Threat-Informed Validation

Shape scenarios using sector-specific intelligence and MITRE ATT&CK, then use iterative retesting to inform ongoing improvement.

OUR ENGAGEMENT APPROACH

01 Align

Define the environment, objectives, and relevant threat scenarios.

02 Validate

Test exploitability, attack paths, and control effectiveness.

03 Strengthen

Prioritize improvements and revalidate defenses as threats evolve.

HUMAN-LED. AI-AMPLIFIED.

info@nightshade-tech.com | (954) 358-9747
nightshade-technologies.com