Red Team and Penetration Testing for Mission-Critical Systems

Structured adversarial testing that simulates real-world attack techniques against mission systems, identifying exploitable vulnerabilities, validating defensive controls, and providing prioritized remediation guidance.

PRACTICE

Cyber Resilience and Zero Trust

CLIENT PROFILE

Federal agency or DoD program office requiring adversarial security testing to validate defensive controls before operational deployment or annual assessment

Challenge

- Uncertainty about whether defensive controls can withstand sophisticated attacks
- Compliance requirements for periodic adversarial testing and vulnerability assessment
- Need to validate security posture before deploying new systems to production

Approach

- Define rules of engagement, scope boundaries, and success criteria with stakeholders
- **Execute phased testing:** reconnaissance, exploitation, lateral movement, and objective achievement
- Document findings with attack chains, evidence, and risk-rated remediation recommendations
- Conduct purple team debrief with defenders to improve detection and response capabilities

Typical Outcomes

- Validated understanding of exploitable attack paths and defensive blind spots
- Risk-prioritized remediation roadmap with specific technical recommendations
- Improved SOC detection capabilities through purple team knowledge transfer

Procurement Paths

- GSA MAS for penetration testing and red team services
- CIO-CS (NITAAC) for cybersecurity assessment services

Compare vehicles and ordering steps on **How to buy**.

Partner Technology Examples

- Palo Alto Networks
- CrowdStrike
- Tenable
- Elastic Security

This is a representative use case. To request a briefing or a quote, contact Norseman Defense Technologies at 410.579.8600 or sales@norseman.com.