

NJECC Co-op Buy: Call Now and Save!

NetReaper Labs' Pen Testing, Incident Response Plan



Netreaper Labs delivers cybersecurity solutions, including penetration testing, network engineering, vulnerability assessments, training, and incident response. Their expert team provides tailored reports, secure architecture design, and hands-on support to help you meet threats, ensure compliance —without breaking the budget.

In the testing, no network impact (denial-of-service) or direct exploits will be leveraged; vulnerabilities will be identified for exploit success probability. External – performed remotely. Internal – performed on-site (travel included in the cost). OSINT Dark Web – performed remotely. Assessments will also include network mapping and proposed recommendations for any remediations. Netreaper Labs Security Engineers will provide in-depth reporting and analytics of all network devices, and any subsequent vulnerabilities that are identified.

NJECC full cyber assessment for k-12 schools: \$11,789 (internal, external, dark web)

Internal Network Assessment

Netreaper Labs' onsite assessment uncovers internal vulnerabilities through hands-on testing, including malware simulations, firewall audits, wireless/wired exams, and Active Directory reviews. In this testing phase, security engineers from Netreaper Labs will run multiple reconnaissance, vulnerability scans, and exploit utilities on the target network. This testing will be used to identify any known or unknown security vulnerability that may be on the internal network. **NJECC internal pen test \$5889**

External Network Assessment

Netreaper Labs' remote assessment scans all internet-facing assets to uncover vulnerabilities, map resources, and test domain integrity. It includes web app testing and optional deep credentialed scans—delivering actionable insights with zero network impact. In this testing phase, security engineers from Netreaper Labs will run multiple web-based, or public facing network scans against the target network. This will include all devices hosted on the target network that have direct inbound Internet Access: **NJECC external pen test \$4689**

OSINT / Dark Web Assessment

The Dark Web does exist and this is an important step in identifying security vulnerabilities. Information contained on the Dark Web could identify existing potential exploits that may already be attacking and/or exfiltrating confidential sensitive data. This one-time scan service will provide a detailed dark web analysis of the network domain(s) including a searching for lists of stolen credentials, exposed documents, leaked source code, breached IT systems, phishing websites and pages, fake accounts in social networks, possible trademark infringements, or potential squatted domain names. This scan will include all users and members of the network domains. **NJECC dark web assessment \$2309**

Cybersecurity Incident Response Plan Netreaper uses best practices from CISA, NIST, CIS, and SANS to assist schools in building and refining their IR Plan. This living document (approx. 80-150 pages) defines roles, outlines response steps, and includes key contacts—tailored to your operations and industry. Services include plan creation, tabletop exercises, and expert analysis to ensure readiness and compliance.

Expert Guidance: Developed using trusted frameworks from CISA, NIST, CIS, and SANS.

Tabletop Exercises: Hands-on simulations to test and improve your response readiness.

Defined Roles & Contacts: Clear responsibilities and escalation paths for incident response.

Compliance Support: Helps meet regulatory and audit requirements.

Living Document: Versioned and designed for regular updates as your organization evolves.

NJECC Incident Response Plan \$8609 (includes any travel)

