Virtual Red Team

Continuous Pentesting Service

LEGION CYBERWORKS

PEN-TESTING | MANAGED SECURITY | INCIDENT RESPONSE | XDR

Continuous Security Verification

Finding and fixing vulnerabilities, default configurations, weak credentials, and other exposures one or two times a year is not sufficient. Vulnerability scanning does not leverage sophisticated attack paths and TTPs. Changes to your technology environment and the cyber-threat landscape are far too frequent for this to remain an acceptable practice.

Continuous pentesting helps organizations get secure, compliant, and addresses key security questions about their environment:

- Are my "crown jewels" systems and data secure?
- What urgent issues must I remediate immediately?
- How should I prioritize vulnerability fixes?
- Am I focused on the right defensive efforts?
- Are detection & remediation times improving?
- Are my security tools and procedures effective?
- Am I lowering the impact risk of a cyber attack?

Key Features

- Coverage for your internal, external, and cloud assets, delivered as a fully managed service billed monthly
- Tiers are available to fit any environment allowing you to roll in more advanced and diverse services
- Understand the impact that weaknesses can have on your business with our intuitive portal interface
- We provide the full attack path, proof of exploit, and detailed action log to help you tune your controls
- Detailed fix-action reports guide your remediation activities.
- Professional Services are available as a SOW to help you remediate gaps and weaknesses

Legion Cyberworks LLC 919-769-2916 111 E. Vance St. Suite C; Fuquay-Varina, NC 27526 sales@legioncyber.com

Prevention is Survival. Protect Your Business Through Proactive Security Services

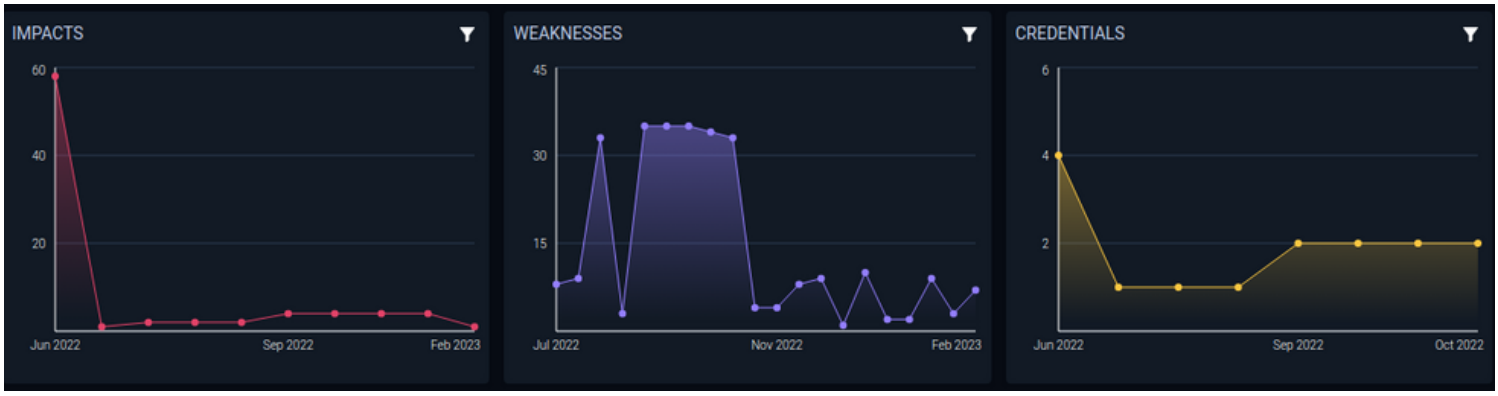
VRT Continuous PenTesting Service

Annual pentesting may meet compliance requirements but it is not sufficient for managing cyber risk year-round. Our Virtual Red Team continuous pentesting service ensures your ability to find, fix, and verify remediation proactively.

- Remove the time constraints of project-based pentesting
- Satisfy requirements for your SOC-2 controls, internal standards, and cyber insurance coverage
- Ensure compliance with state and federal regulations
- Prioritize vulnerabilities to maximize effectiveness
- Detailed fix-action reports guide remediation plans
- Retesting provides proof of remediation or gaps that need to be closed
- Find, fix, and verify that vulnerabilities are remediated on a frequent basis

Track Risk Factors and Improve Continuously

Your security posture is not static, attacker TTPs change frequently, threat actors become more automated and more effective. To keep pace, your security services need to adapt and change too.



- Establish a baseline and a frequent cadence for finding, fixing, and verifying that exploitable weaknesses within your environment are remediated
- Roll in our quarterly security controls assessment service which shows you the blind spots in your EDR, SIEM, SOC, and other controls and provides the details you need to close those gaps efficiently
- Conduct annual table-top exercises to role play cyber-attack scenarios so that you are prepared and ready to respond correctly

Legion Cyberworks LLC 919-769-2916 111 E. Vance St. Suite C; Fuquay-Varina, NC 27526 sales@legioncyber.com