LevelBlue

Offensive Security

Reduce risk by proactively identifying vulnerabilities and threats.

Organizations are facing growing complexity in securing assets, endpoints, and employees across hybrid cloud, mobile, OT, IoT, and on-premises environments, as well as offices and critical infrastructure.

The LevelBlue approach

LevelBlue SpiderLabs' certified experts in vulnerability management, penetration testing, and scenario simulations collaborate with your team to understand your current security program and patch management processes. Based on this understanding, we design a targeted strategy aligned with your objectives. Following execution, we deliver clear findings and can partner with you to develop actionable remediation plans to address gaps, apply necessary patches, and advance your security maturity.

Vulnerability Management	Penetration Testing	Scenario Simulation
Inspection of endpoints to identify security gaps for exploitation	Pre-authorized, precise cyberattack on your environment to find security gaps	Attack simulation exercises to evaluate your processes, communications, and security
Managed Vulnerability Scanning ▪ Automated scanning to discover your internal and external internet-facing assets, resources, and endpoints ▪ Attack surface management to monitor for potential attack vectors and exposures ▪ Identification of vulnerabilities and removal of false positives	**Penetration Testing as a Service** ▪ Programmatic approach to penetration testing, with a system built end-to-end that can be easily implemented into your current operations ▪ Composed of various packages and tiers, giving you control over your testing programs and budget **Custom Testing** ▪ Customization of testing scope based on business needs	**Red Team** ▪ Ultimate test of people, processes, and technology, delivering real-world, scenario-based engagements **Purple Team** ▪ Use of our SpiderLabs red team (attackers) and your blue team (defenders) to perform intensive attack and response exercises **Tiger Team** ▪ Focused, goal-oriented testing to address specific security challenges

Benefits

- Partner with a certified, industry-recognized leader in ethical security testing and threat intelligence.
- Leverage end-to-end security capabilities adaptable to your organization's unique needs.
- Test all types of infrastructure, applications, systems, and endpoints specific to your industry and vertical.
- Streamline budgeting with a consistent and transparent pricing model aligned with your engagement scope.
- Gain expert-driven insights tailored to regulatory and industry requirements to support compliance obligations.
- Mature your security with red, purple, and tiger team exercises to identify vulnerabilities and improve response.
- Address risk effectively with complete findings and actionable remediation guidance tailored to your environment.

Compliance and regulatory partner for compliance excellence

As the world's largest pure-play MSSP, we design programs aligned with multiple compliance requirements, including NIST, ISO 27001, HIPAA, CMMC, DORA, NIS2, and Essential Eight.

Ongoing testing for long-term security

While ad hoc penetration testing provides valuable point-in-time insights, a pre-established security testing program offers a more comprehensive view of enterprise risk over time. LevelBlue provides managed and subscription-based testing services tailored to your desired frequency. We collaborate closely with your team to review findings, develop actionable remediation plans, and conduct continuous testing to address identified gaps. All results are accessible through the LevelBlue Platform, which includes current and historical test findings, remediation plans, and reports.

Comprehensive attack simulation: red, purple, and tiger teams

Understand how sophisticated attackers could gain a foothold and operate in your environment with our red, purple, and tiger team engagements. Driven by threat intelligence from the SpiderLabs team, our global managed security client base, investigations, threat hunts, intelligence from our partners, and open-source feeds, we simulate advanced attack techniques against your environment. Our team works to gain initial access and establish persistence within your network, using stealth to attempt data exfiltration while avoiding detection.

Mapped to the MITRE ATT&CK framework, our methods combine offensive strategies from red and purple teams with the agility and adaptability of tiger teams, providing a comprehensive test of your people, processes, and technology to mature your security operations.

LevelBlue accreditations

SpiderLabs is a CREST-registered advanced security team within LevelBlue focused on application security, incident response, penetration testing, physical security, and security research. The team has performed thousands of incident investigations and penetration and application security tests globally. In addition, the SpiderLabs team provides intelligence through bleeding-edge research and proof of concept tool development to enhance LevelBlue's products and services:

- More than 25 years of industry leadership in vulnerability research and findings, with 250+ specialized security experts and researchers
- The first global CREST-certified member organization to identify more than 120 CVEs and TTPs
- 200,000+ hours of pen tests delivered annually and 30,000+ vulnerabilities discovered annually, including 9,000 high/critical severity infrastructure and web app sources
- Recognized by leading industry analysts