blue mantis

Penetration Testing

Proactive protection against threats

Safeguarding your company's reputation and financial health against cybersecurity threats is more crucial than ever. But today's hybrid workforces, cloud IT environments, and mobile devices complicate cybersecurity posture management. What you need is a trusted cybersecurity ally who thinks like a hacker, fortifying your defenses before a catastrophic threat strikes.

Blue Mantis Penetration Testers act as your frontline defense, using hacker-like tactics to expose hidden network, systems, and cloud vulnerabilities and then fortify them against attack.

Benefits

- Simulates real-world external and internal attacks that expose hidden vulnerabilities and threats
- Identifies risks to your IT environment with a clear plan for strengthening your defenses
- Offers continuous service, including Social Engineering testing, for adaptive cyber defense

Comprehensive testing, trusted strategies

Blue Mantis Pen Testers provide a holistic view of your organization's cybersecurity posture. We augment your internal IT teams with an objective eye—using a wide array of tools and skills that simulate external attacks and insider threats to expose hidden vulnerabilities in your systems and business processes. Our pen testers can also help train your distributed workforce against social engineering attacks.

Blue Mantis Pen Testers use the industry-standard Penetration Testing Execution Standard (PTES) and hold Offensive Security Certified Professional certifications and SOC-2 accreditation to ensure the strictest confidentiality and rigor required by highly-regulated industries.

Blue Mantis Pen Test Services

- Network (WAN, LAN, and wireless) vulnerability and penetration testing
- Endpoint protection (EDR/XDR) and security tools review
- Application security and web application testing

- Cloud security assessment (all major cloud providers)
- Microsoft Entra ID (formerly Active Directory) health check and password audit
- Microsoft 365 security assessment

- Remote access and hybrid workforce security assessment
- System configuration, vulnerability and exploit review
- Data retention, backup, and disaster recovery assessment

- Information security policies and procedure review
- Social Engineering training program review
- Firewall security configuration assessment