GET A FULL PICTURE OF
SECURITY RISKS AND GAPS

GoSecure also offers comprehensive Penetration Testing programs that help organizations assess their defenses in key areas.

GoSecure Penetration Testing programs are designed to emulate risks from the real world based on the needs of the organization.

Testing programs include:
- External Network Security
- Internal Network Security
- Web Application Tests
- Code Reviews
- Mobile App / Device Testing
- Wi-Fi / Endpoint Testing
- Social Engineering / Anti-Phishing Programs
- Physical Security

GoSecure ethical hackers are Offensive Security Certified Professionals (OSCP)—ensuring that the team is meeting the highest standards in the industry for skills, expertise and testing methodologies.

IMPROVE YOUR DEFENSES

When an attack strikes, it’s too late to test the security controls and response capabilities of an organization. Red & Purple Team engagements offer strategic services that help assess detection, response, investigation and future prevention abilities within an organization. These custom engagements, tailored to the objectives of the organization, assess organizational risk and readiness to protect against and respond to breaches.

RED VS PURPLE TEAMS

With GoSecure Red Team strategic engagements, experienced security professionals test the in-house capabilities at an organization by combining multiple available attack techniques to emulate real-world threats. Within an organization, teams such as the Security Operations Center (SOC), Incident Response, etc., act as the Blue Team to defend against the attacks—which can come at any time, from technological, social engineering and physical threat vectors. The target objectives for this type of engagement are defined by the organization.

A Purple Team is comprised of both the internal security team and external professionals who work collaboratively through a series of scenarios while the external experts share their knowledge and techniques with the in-house team. Purple Team engagements are typically long term, offering the opportunity to resolve issues found during the exercises at the time and then re-test those gaps to determine if they have been addressed—while increasing the capabilities of the in-house team.

Both approaches can improve security posture, find gaps in cybersecurity defenses and help organizations prepare to respond to real-world attacks.
ABOUT GOSECURE

GoSecure is a recognized cybersecurity leader and innovator, pioneering the integration of endpoint, network, and email threat detection into a single Managed Detection and Response service. The GoSecure Titan platform delivers predictive multi-vector detection, prevention, and response to counter modern cyber threats. GoSecure Titan MDR offers a detection to mitigation speed of less than 15 minutes, delivering rapid response and active mitigation services that directly touch the customers’ network and endpoints. For over 10 years, GoSecure has been helping customers better understand their security gaps and improve their organizational risk and security maturity through MDR and Advisory Services solutions delivered by one of the most trusted and skilled teams in the industry.

To learn more, please visit: https://www.gosecure.net.

LEARN MORE
www.gosecure.net/red-purple-team-services

CONTACT US
www.gosecure.net/sales-contact
1-855-893-5428

BENEFITS OF RED TEAM ENGAGEMENTS

- Organizations with cybersecurity programs can test current capabilities and decision-making of the team against threats developed to mimic real-world attacks.
- Red Team engagements can help organizations that invest in technology and resources like Security Incident & Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Endpoint Detection & Response (EDR) or a Security Operations Center (SOC) find gaps and optimize those programs.
- Leadership and compliance can gain perspective from experts that understand the threat landscape.
- GoSecure provides a comprehensive, custom report with the testing conducted, observed Blue Team response and actionable recommendations.

BENEFITS OF PURPLE TEAM ENGAGEMENTS

- Organizations get rapid but long-lasting improvement in security maturity through the GoSecure “Test, Fix and Test Again” approach to Purple Team Engagement.
- For the in-house team, the collaborative approach to Purple Team engagements offers an opportunity to improve security practices and learn new techniques. Through hands-on mentoring with the external experts, the organization benefits from knowledge and skill transfer while improving their detection and response processes.
- As gaps are identified through the real-world scenarios, a case can be made for added investment in security for an organization. Purple Team engagements identify areas to allocate people and technology where it’s needed to protect against breaches.
- Purple Team reports detail the changes that have already been accomplished and the resulting improvements to security posture.