IOActive.

Research-fueled Security Services

Red and Purple Teams:

Building Operational Resiliency Through Real-world Threat Emulation

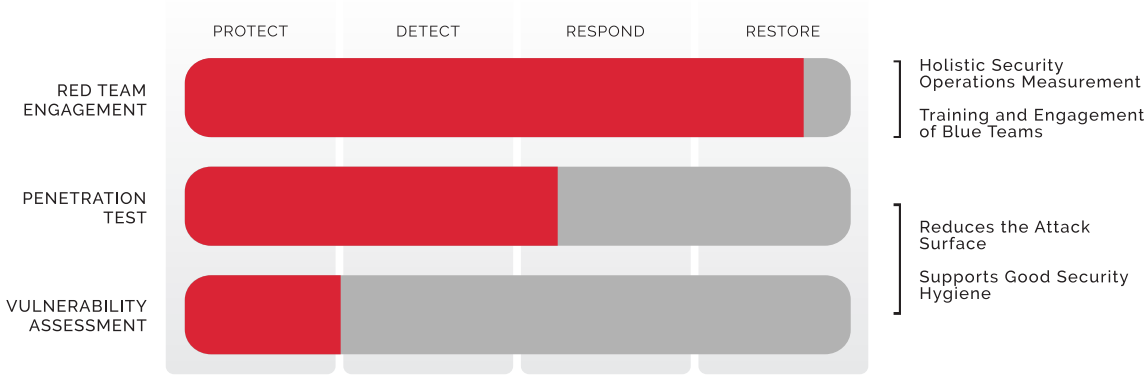
Who better to evaluate security effectiveness – compliance auditors or attackers? Vulnerability assessments and penetration tests are critical components of any effective security program, but the only real way to test your operational resiliency is from an attacker's perspective. Our red and purple teams bring you this insight through full threat emulation, comprehensively simulating a full range of specific attacks against your organization – cyber, social, and physical.

We can provide or advise on the creation of continuous, independent, and customized real-world attacker-emulation services that work with your blue team – your own security operations personnel – to prepare them to face the adversaries your enterprise is likeliest to encounter.

Our original research and breach analysis give us detailed insight into how hackers have penetrated organizations across a diverse range of sectors and circumstances. Our red team brings this unique experience and insight to bear on your behalf to help you focus on effective security.

KEY TAKEAWAYS

- Our red teams evade and subvert security controls to test your defenses
- Attacker's perspective to determine the true impact to physical, cyber, and human assets
- Research-fueled threat emulation to perform covert, real-world attacks
- Purple teams can start with "assumed breaches" to focus on specific attack scenarios
- Collaboration with your blue team improves detection and incident response capabilities
- Measurable objectives and actionable recommendations improve resiliency



RED TEAM SERVICE

Using threat emulation, our red team adopts the tactics, techniques, and procedures (TTPs) of an attacker determined to get inside your network, to understand your resiliency to a real-world, targeted attack. These multi-month engagements are custom crafted to address the most likely threats and security controls that need to be tested, and the most valuable targets and critical assets that need to be secured.

Campaigns employ stealthy, multi-vector attacks, emulating real threat actors' methods targeting technical, physical, and human assets to penetrate your security defenses. Once the red team campaign is complete, we transfer the learnings to your blue team with the goal of improving your security and incident response programs through measurable objectives.

PURPLE TEAM SERVICE

Purple teaming brings the red and blue teams together, collaborating to identify high-priority threats and likely attack paths, with the goal of identifying gaps in the ability of your security controls to detect or block attacks. We design attack paths and campaigns appropriate to your company's environment and industry, and methodically emulate the attacks. Purple team engagements start at the beginning of the attack and progress through each phase or can be accelerated by starting with an "assumed breach" scenario. These engagements require greater blue team involvement during planning and execution to ensure your team has the ability to detect and respond where and when it matters. We deliver immediate feedback throughout attack execution, working closely with your blue team to assess the level of attack visibility and validate whether existing security controls and processes are effective.

Red and Purple Team Services often include social engineering and physical penetration testing, or these services can be deployed independently.

SOCIAL ENGINEERING

Emulating the same methods used in today's largest breaches, our team uses social engineering to exploit the human element of your organization. We employ techniques such as spearphishing, voice calls (vishing), texting (smishing), onsite impersonation, pretexting, and social network attacks to gain access to your critical physical and IT assets.

PHYSICAL PENETRATION TESTING

Using any means necessary, our team infiltrates your headquarters and branch offices by hacking camera systems, cloning RFID cards, pretexting (fabricating scenarios), tailgating, and social engineering. We think like an attacker and breach your defenses accordingly.

SC MEDIA AWARDS

One of the Most Important Cybersecurity Companies of the Last 30 years

2 of 3 Most Important Researchers of the Last 30 years

REBOOT 19 SC Media Reboot Leadership Awards

ABOUT IOACTIVE

IOActive is a trusted partner for Global 1000 enterprises, providing research-fueled security services across all industries. Our cutting-edge security teams provide highly specialized technical and programmatic services including full stack penetration testing, program efficacy assessments and hardware hacking. IOActive brings a unique attacker's perspective to every client engagement to maximize security investments and improve clients' overall security posture and business resiliency.

