SERVICE BRIEF

PENETRATION TESTING SERVICES

Red Team Attack Simulation

Simulate real-world attacks from the perspective of the adversary.

Typically, a penetration test will look for vulnerabilities in a network, attempt to exploit them, and determine not only the risk of the individual vulnerability, but also the overall risk to the organization. While penetration testing is an important part of a company's security controls, spurring remediation of all discovered vulnerabilities, your organization still needs more. What is the true risk to the organization under a sophisticated, targeted attack? Are your detection and response capabilities up to par? Are your security engineers and analysts prepared to protect your most critical assets? The best way to know is to simulate an adversary's path if they were to target your organization. Enter Rapid7's Red Team Attack Simulation.

For organizations with more mature security programs, a Red Team Attack Simulation is a comprehensive way to determine the true effectiveness of your security program.

WHAT IS A RED TEAM ATTACK SIMULATION?

A Red Team Attack Simulation is an exercise that focuses on an organization's defense, detection, and response capabilities. Rapid7 works with you to tailor the service to properly emulate the threats your specific organization faces. Our Red Team operators carry out real-world adversarial behavior and commonly used tactics, techniques, and procedures (TTPs) against which you can measure your program's effectiveness and your team's responsiveness in the context of an attempted breach. This allows you to pinpoint potential risks, including technical and organizational gaps in your defenses. By using custom tools, malware, and cutting-edge techniques, Rapid7 can identify the gaps in your security monitoring, detection, and response, so you emerge prepared and empowered to take on attackers.

Want to take this one step further? Rapid7 can incorporate a Blue Team component, which involves experienced incident responders assessing:

- Maturity of detection and monitoring controls
- Maturity of and adherence to your incident response (IR) plan
- IR coordination
- Communications
- Technical analysis capabilities

This combined approach, known as a "Purple Team Assessment," allows you to test controls while under a simulated, targeted attack.

060518