Red Team Services

Improve the effectiveness of your defensive capability and resilience to sophisticated attacks

Prepare your internal security team or security operations center (SOC) through a controlled, realistic attack simulation. By deploying various traditional and non-traditional penetration testing and social engineering techniques over a realistic timeline, we help you ascertain that your organization can detect and respond to the latest types of cyberattacks.

Not Your Father's Pen Test

Red Team exercises combine elements of social engineering with penetration testing to gain insight into how the environment will fare in a real-world attack scenario. Foundstone® Red Team services from McAfee® can assess the effectiveness and readiness of your security controls, awareness, incident detection, and response capabilities.

This exercise differs from a classic penetration test in that the team leverages tools and techniques that are often outside the scope of most pen testing. This includes phishing, simulated malware payloads, physical attacks, "dumpster diving," social engineering, and more. This more comprehensive engagement is performed over a less restrictive timeline to allow us to fully probe your network and people.

Attack scenarios can be crafted to emulate specific types of threat actors (enthusiasts, organized groups, and cybercriminals). We employ both traditional and non-traditional techniques to test your resilience against intrusions, data exfiltration, fraud, internal attack, corporate espionage, and physical compromise.

Our Red Team services can help you:

- Experience, assess, and remediate a real-world breach attempt in a controlled environment
- Identify and protect your most critical assets and vulnerabilities
- Reduce your response time to events and incidents

Exercise Scope

The scope of each engagement is custom-fit to your organization's needs and goals. Scenarios are defined based on a combination of our guidance, and what concerns you the most about your current security posture, or what you have heard and read from colleagues and in the news.

Two Types of Services

We offer two types of Red Team exercises:

Tabletop/Dry-Run Simulations

Role-playing scenarios conducted with client stakeholders in a boardroom setting. As these exercises are theoretical, many types of attack scenarios can be tested with zero operational impact.

Direct Attack

Engagements in which only a few individuals know you are "under attack" so you can test actual reactions and responses. These scenarios are highly customized to cover a wide range of either general or specific goals.

Example Scenarios

McAfee Professional Services Group has a portfolio of Red Team scenarios covering a range of different attack scenarios based on the real-world incidents we see, and you read about in the news.

- **DDoS Attack**: Tabletop simulated distributed denial-of-service (DDoS) attack involving security response and coordination within multiple operational teams
- **Advanced Persistent Threat:** Simulated advanced persistent threat (APT) intrusion involving incident detection, response, malware analysis and forensics capabilities, and fraud monitoring
- **Social Engineering**: The attacks performed can be used to steal employee's confidential information or get physical access to locations and digital assets.
- **Data Exfiltration:** Involves various methods to siphon data out of an enterprise network, ranging from basic to sophisticated scenarios
- **Hybrid Attack**: Combine all of the above to see how resilient your environment and security culture truly are. We have conducted engagements where the goal was to "gain physical access to the data center" or "get into my secret prototyping lab."
- **Timeline and Duration:** Penetration tests are usually for a very specific, time-boxed amount of time, but attackers are under no such limits. Testing will be randomized over a pre-determined period of time that lends itself to more thorough results.

Coverage Across Your Organization

Red Team exercises are conducted to practice and foster security awareness and communications between teams and identify potential deficiencies.

A Red Team exercise covers three facets of security:

People/Cultural Vigilance

Your people are often the weakest link. We can test awareness of social engineering and physical security controls like gates, locks, sensors, etc.

Technology/Assets and Controls

Targets existing and/or planned technology assets or systems, configurations, and vulnerabilities

Processes/Security Response

What actually happens in an attack? How will your teams respond? How will they escalate and coordinate with other teams to contain the incident?

The McAfee Difference

The Foundstone team has deep insight into real-world issues because we have teams that do security strategy, infrastructure and application security, incident response, and training. We see both the mistakes made—and where they lead.

The McAfee Professional Services team has a long history of working with clients across the globe, both as a technology partner to support our anti-malware, antispyware, and antivirus software solutions, and also as a strategic advisor with product-agnostic, program-level engagements. Our teams of security experts assess network vulnerabilities, evaluate gaps in information security programs, offer strategies that meet compliance goals, and even help develop programs to prepare for security emergencies.

Engagement Phases and Deliverables

A Red Team engagement typically includes multiple stages:

- **Stakeholder Interviews:** Working with you, we define a summary and exercise objectives.
- **Custom Red Team Exercise:** Design, develop, and document a customized scenario or threat actor.
- **Red Team Exercise(s) Execution:** Final Report including all findings and recommendations
- **Final Results Presentation:** Summary review with management and stakeholders including demonstrations and detailed explanation of outcomes and lessons learned

Related Foundstone Professional Services

Foundstone offers many other related services and training classes, including:

- IR Policy and Procedure Definition and Review
- IR Plan Testing
- On-Site IR Emergency Response Team
- Digital Forensics and Malware Analysis
- Threat Identification and Discovery
- Comprehensive Network and Infrastructure Security Assessment
- Software Security/Source Code Audits
- Threat Modelling

.

Learn More

We provide security consulting, customized product deployments, and training and advisory services. Let our consultants help your organization assess current policies, create new programs that meet compliance goals, and cost-effectively prepare for security emergencies. Speak with your technology advisor about our services or email us at **foundstone@mcafee.com**.

Get more information at **www.foundstone.com**.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com