Red Team Testing

DATASHEET

Simulate an All-Out Attack

When your organization becomes a target, do you know how well your employees and infrastructure would hold up? TraceSecurity's Red Team Testing is an advanced persistent threat assessment that simulates the way an attacker would use all available resources to breach your organization.

Using a combination of reconnaissance, social engineering, and penetration testing, our analysts will spend several weeks attempting to compromise your IT infrastructure. They'll do a deep dive on the internet, gathering any publicly available company information – things like employee names, titles, and contact info, vendors information, IP addresses, and more. Leveraging this information, the analysts will carry out targeted phishing, vishing, and smishing attacks to further compromise your employees and gain access to company data.

No matter what the analysts were able to find online and coerce out of your employees, they will continue their attacks on your external, internal, and wireless networks. Using the same manual attack vectors as real-world hackers, our analysts will attempt to crack your external and wireless networks in the hopes of pivoting into internal systems. If able (meaning something isn't properly configured), the analysts will see just how much they can compromise in your internal systems.

Red Team Testing Includes:

- Blind reconnaissance of company and employee information
- Targeting phishing, vishing, and smishing campaigns
- Onsite social engineering attempts
- External, internal, and wireless penetration testing

Frequently Asked Questions

What is the difference between Red Team Testing and Purple Team Penetration Testing?
Red Team Testing simulates an all-out attack against your organization, including reconnaissance, social engineering, and penetration testing. Purple Team Penetration Testing is a coordinated effort between TraceSecurity's Red Team and your Blue Team, monitoring penetration testing attempts in real time.

What is the value of a Red Team Test?
A Red Team Test is the most adversarial simulation available. By performing blind reconnaissance, we simulate the way a real-world attacker would zero in on your company and your employees, performing attacks based on your publicly available information.

What if you can't find any usable information on the internet?
This is extremely unlikely. The reality of running a business necessitates information being publicly available on the internet.

Do I need to provide my employee emails and phone numbers for social engineering?
No, in order to meet the objective of the Red Team Test, we want to manually find that information online. After reconnaissance is complete, you may optionally submit additional emails and phone numbers to be included.

Will this hurt my network?
This is extremely unlikely. We do not attempt any denial-of-service attacks.

Will onsite physical security testing cause any damage to my facilities?
If any, physical damage would be minimal based on the level of testing discussed during scoping.

How much time will you need from our internal team before and during testing?
Because of this service's adversarial approach, there is minimal need for coordination with the point of contact before and during testing.

How long does a Red Team Test typically take?
This depends very much on the size and complexity of your IT environment. At most, testing could take up to four weeks.