


Red Teaming

Measure how well your organization can withstand a real-life attack



Although vulnerabilities may seem small on their own, when they're tied together to form an attack path, they can cause significant damage. Our Red Team models how a real-world adversary might attack a system and how that system would hold up under attack. After a Red Teaming exercise, you'll have a better understanding of your organization's security posture as it relates to specific threat actors attacking a set of defined assets, and you'll know where to focus your efforts for improvement.

We seek out exploitable security holes

Our Red Team identifies immediately exploitable security holes across an organization's attack surface using a variety of composite attack vectors by chaining together seemingly separate or cross-domain vulnerabilities. This includes relationships between systems, software, and people. Some areas of risk we may look for are:

- Personally Identifiable Information (PII), Primary Account Numbers (PAN), or Protected Health Information (PHI) on employee workstations or network shares
- Sensitive data written to log files
- Unmasked data in reporting dashboards
- Encryption keys in source code

We simulate real-world targeted attacks

Our attack process chains together seemingly separate vulnerabilities for a holistic view of your applications, networks, and team behaviors. Each Red Teaming exercise consists of seven essential steps:

1. Goal setting

You'll determine the specific goals and objectives of the attack.

2. Reconnaissance

Our Red Team identifies network services, Web applications, and employee portals.

Answer the age old question: What's our risk?



3. Penetration testing

We perform application penetration testing and network penetration testing to reveal vulnerabilities (e.g., cross-site scripting).

4. Social engineering

Our Red Team uses common manipulation techniques such as email and phone-based phishing to find “human vulnerabilities”—people who unknowingly reveal confidential company information.

5. Exploit and escalate

Our Red Team gains access inside the network through one of the vulnerabilities they discover. This may include physical facQ

The Synopsys difference

Synopsys offers the most comprehensive solution for building integrity—security and quality—into your SDLC and supply chain. We've united the leading testing technologies, automated analysis, and experts to create an incomparable portfolio of products and services. This portfolio enables companies to develop customized programs for detecting and remediating defects and vulnerabilities early in the development process, minimizing risk and maximizing productivity. We don't stop when the test is over. As a recognized leader in **Application Security Testing**, we offer onboarding and deployment assistance, remediation guidance, and training solutions that empower you to optimize your investment.

For more information go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: software-integrity-sales@synopsys.com