BLACKDUCK®

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 goal/asset you want our Red Team to target.

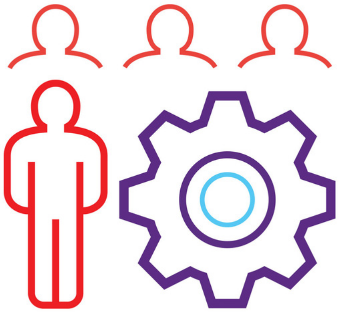
2. Reconnaissance

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

3. Penetration testing

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

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



Our Red Team uncovers where you need to spend more time, budget, and effort on security.

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 facility exploitation and/or business process tampering. An example of this is “tailgating” or posing as employees or contractors to gain access to a physical workplace.

6. Obtain target

Our Red Team accesses sensitive corporate assets.

7. Remediation

At the end of each assessment, we will conduct a live read-out with the appropriate organization stakeholders to review each vulnerability identified during the assessment, answer any questions that the team might have around each vulnerability, and discuss mitigation/remediation strategies.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.