secarma
CYBERSECURITY EXPERTS

A Advise C Certify T Test

Red Teaming

Red Teaming is a proactive and systematic approach to cybersecurity assessment where skilled professionals simulate real-world cyberattacks on an organisation's systems, networks, and personnel.

The goal is to identify vulnerabilities, weaknesses, and security gaps to help the organisation improve its defences and preparedness against real threats. The exercise is usually conducted with the knowledge or co-operation of only a small group of people from the client organisation.

Who Is It For?

Red Teaming is chosen by any organisation that has a strong focus on cybersecurity and risk management:

- **Corporate Enterprises.** Large corporations and multinational companies often hire Red Teams to assess the security of their networks, applications, and infrastructure. They want to identify vulnerabilities before malicious actors can exploit them.
- **Banks and Financial Institutions.** With a wealth of customer information to safeguard, Red Team exercises are used to assess the security and compliance of core systems.
- **Technology Companies.** Risks to commercially valuable intellectual property can be evaluated and more clearly identified using a Red Team exercise.
- **Critical Infrastructure Providers.** Water plants, energy services and transportation are potential targets for malicious actors. Red Teaming can help identify risks that basic security testing will not cover.
- **E-commerce and Retail.** Online retailers and e-commerce platforms store sensitive customer data and process financial transactions. Red Teams help them identify and mitigate security risks.

What We Test

A Red Team exercise is always carefully scoped to ensure that the client's specific objectives are addressed. A great deal of preparation goes into every Red Team engagement, including the creation of test infrastructure, domains, personal identities, and malware payloads all designed to breach the client's infrastructure.

Typically, a combination of the following areas is tested:

- **Social Engineering:** Simulated social engineering attacks are often a crucial part of Red Team engagements. This includes phishing attempts, pretexting, and other techniques to assess an organisation's susceptibility to manipulation.
- **Physical Security:** Red Teams may conduct physical security assessments, including attempting to gain unauthorised access to facilities, server rooms, and sensitive areas within an organisation.
- **IoT and OT Security:** Assessing the security of Internet of Things (IoT) devices and operational technology (OT) systems, which are increasingly becoming targets for cyberattacks.
- **Third-Party and Supply Chain Risk:** Often overlooked, the evaluation the security of third-party vendors and partners who have access to an organisation's systems or data.

3 Archway, Birley Fields, Manchester M15 5QJ
0161 513 0960
secarma.com
actnow@secarma.com

- **Network Security:** Red Teams often assess the security of an organisation's network infrastructure. This includes testing firewalls, routers, switches, and other network devices for vulnerabilities and misconfigurations.
- **Web Applications:** Web applications are a common target for attackers. Red Teams assess the security of web applications by attempting to exploit vulnerabilities such as SQL injection, cross-site scripting (XSS), and authentication flaws.
- **Endpoint Security:** Testing the security of individual devices such as computers and mobile devices to identify vulnerabilities and determine if attackers can gain access to sensitive data or compromise the devices.
- **Incident Response:** Testing an organisation's incident response capabilities by simulating a security incident and evaluating how well the organisation can detect, respond to, and recover from the attack.

How can we help?

A Red Team exercise is exactly that, a team exercise. At Secarma we have in-house expertise in malware development, web application and network security, and social engineering and manipulation techniques.

We also boast deep knowledge of cryptography, malware analysis, and Endpoint Detection and Response (EDR) evasion techniques.

We can assemble an expert team specifically for your engagement, ensuring that the right skills are brought into play as the exercise unfolds.