Red Teaming

Your organization is under attack. The volume and sophistication of targeted and opportunistic attacks are increasing. Cyber fraud, ransomware, supply chain attacks, or insider threats are just some of the threats you face. Test how well your cyber defenses hold up against realistic malicious actors through Red Teaming.

Preparing your organization for such events requires more than deploying security controls. It also requires training your Blue Team to respond correctly to these low-frequency, high-impact events. The biggest gain from performing a Red Teaming assessment, besides finding previously unknown vulnerabilities, is the opportunity for your defenders to live through an actual attack in a safe setting.

What is Red Teaming?

Red Teaming is a security discipline originating in the military arena that simulates full-spectrum cyber-attacks. This allows you to measure your cyber defense's effectiveness against malicious actors and allows your defenders to practice their detection and response capabilities in a controlled environment and validate or refine them. Lastly, the Red Team can also expose gaps in your overall security defense capabilities by targeting your organization and not being confined by the constraints of a regular penetration test.

Suppose you want to know how good you are at detecting spearphishing attacks by sophisticated cybercrime actors or whether your detection capabilities are indeed seeing Advanced Persistent Threats (APTs). In that case, there is only one way to know: to test these **processes by performing these attacks as a malicious attacker would. The Red Team will simulate the attack. The Blue Team, responsible for defending, can be involved in various ways (or not at all). The White Team (the observers) can escalate and de-escalate when necessary.**

The Process of Red Teaming

Phase 1 | Planning and Preparation

Managing the process starts with planning and careful preparation. A dedicated project manager works together with the Red Team lead and the White Team to create a schedule and a dedicated set of rules of engagement. Throughout the engagement, this schedule is followed and adjusted where necessary. Risks and scenarios are assessed continually. The Red Team will constantly communicate with the White Team via weekly scheduled meetings, a secure chat group, and additional calls where necessary. This ensures that the White Team is in full control of the attack.

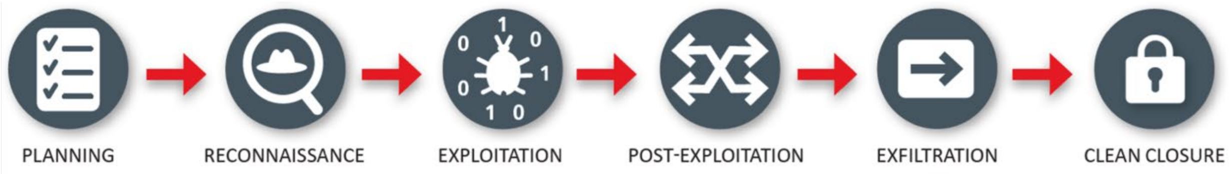
Phase 2 | The Attack

After careful consideration and planning, our consultants will go on the attack and attempt to access your so-called 'crown jewels' in any way possible. Depending on the target, Secura will use a mixture of offensive social engineering and computer network attack techniques as a real-world malicious actor would. Techniques used are mystery guest, phishing, vishing, attacks from the internet, and computer networking attacks in your internal networks.

Phase 3 | Clean Closure

Once the attack is over, the so-called clean closure stage begins. This stage does not only mean managing the leftover digital remnants of the executed attacks. It also means providing the Blue Team with one or more evaluation sessions where the complete timeline is replayed in a workshop, maximizing learning and awareness. The end result of this phase is a detailed technical report and a perspective on your overall security maturity in your threat landscape.

These phases are included in Secura's kill-chain for Red Teaming assessments:



The Different Teams

RED TEAM

The Red Team assumes the role of a hostile attacker who challenges the organization's cyber security. necessary to appoint teams on the client side as well.

BLUE TEAM

The Blue Team is in charge of defending the networks, systems, and applications. This includes both security professionals and administrators tasked to configure systems and applications.

WHITE TEAM

The White Team acts as a link between the Red Team and the Blue Team. This team is the only part of your organization that is aware of the assessment and therefore critical to the success of the attack simulation

PURPLE TEAM

When training the Blue Team has a higher priority to your organization compared to testing the real world readiness against cyber attacks, a Purple Team setting can be chosen. Here the Red and Blue Team work closely together to find gaps in your detection and mitigation capabilities.

Types of Red Teaming

Red Teaming is gaining popularity in all sectors, from financials to public organizations and even (critical) industry as a security discipline. Secura, however, believes that there is not one Red Teaming program that can fit every type of organization. That's why Secura uses service levels for Red Teaming, with a differentiation in the Red Team assessment's depth, variety, and duration. This allows you to choose which service level is the right fit for your organization and budget in consultation with our Red Team managers. Next, all-service levels work with the MITRE ATT&CK framework and offer the opportunity to work in a Purple Teaming setup (a combined effort between Red and Blue).

RT Modular

Are you up for the **next step after pentesting**? This modular approach uses the strengths and benefits of a full-scale Red Team assessment by **picking the most relevant attacks for your organization**. The stealth of the Red Team is secondary to obtaining objectives. Combined with **more information about your organization up front**, it's allows for an economical option to test the security awareness and digital security of your organization.

RT Core

Red Teaming Core is a **full-blown attack simulation for medium to large businesses that employ their own Blue Teams**. This type will condense threat landscape analysis and reconnaissance into challenging attack scenarios. These scenarios are based on real-world threat actors, and Secura will emulate these groups by using similar Techniques, Tactics, and Procedures (TTPs) as defined in the MITRE ATT&CK Framework. To stay within an attractive budget, so-called Leg Ups are discussed up front to make sure the assessment can continue when your defenses in a specific area are already sufficient to delay the Red Team enough.

RT Pro

The Pro variant of Red Teaming is a step up for organizations with very mature Blue Teams and a high level of cyber resilience. Attacking a mature organization such as yours requires much more effort by the Red Team to, for example, deploy malware that bypasses your EDR solution. Here the Red Team works as a completely independent group.

The Red Teaming Pro is the most realistic simulation of attacks by Advanced Persistent Threats (APTs) against your organization.

ZORRO

ZORRO stands for "ZOrg Red teaming Resilience Oefeningen". This framework, developed by Z-CERT, is aimed at structurally **improving the cyber resilience of participating healthcare providers and the overall healthcare sector.** Secura offers a cost-effective testing program that meets requirements of the ZORRO methodology.

RT in OT

Similar to our Red Teaming Pro service, but specifically **focused on organizations that include OT-assets as their crown jewels.** In a layered approach the Red Team will first try to obtain information that is critical for the comprehension of your OT-processes, and next to obtain strategic access to your OT networks. Our attacks targeting these industrial environments use a tailor-made process to mitigate any risks to your operation.

TIBER

TIBER stands for Threat Intelligence Based Ethical Red Teaming and is part of the **financial sector's* effort to improve cyber resilience under the guidance of the Dutch National Bank.** Also, more cyber security frameworks and regulations mention TIBER-like tests for other sectors. Secura will work with you to ensure that your organization will be tested according to the correct requirements.

*For European organizations in the Financial Services sector, Secura will also work with you to get ready for the upcoming **DORA (Digital Operational Resilience Act)** regulation and associated **Advanced Red Teaming (ART)**

Success of Red Teaming

When is a Red Teaming exercise a success? Some would say "when the crown jewels or flags have been reached without being detected by the blue team". However, this definition also implies that the blue team will have learned little. On the other hand, it means that a plausible and realistic attack path has been exposed, that can now be closed or mitigated. We consider it a success when the Red Team has had a proper challenge, yet identified many new attack paths or unknown vulnerabilities requiring solutions. In the end, you will know your systemic cyber risks, and will be capable of mitigating them. This is the ultimate goal of Red Teaming.

Red Teaming is very different from traditional Pentesting. A Red Team can combine vulnerabilities from different classes of attacks, for example, social engineering and attacks on the external infrastructure, to find otherwise unknown weaknesses. This is contrary to pentests, where the scope is limited to a single network or application.

Red Teaming tests your defenders' capability to detect, respond and mitigate attacks in a realistic setting. It trains them to react during a real attack and shows them where detection capabilities need to be improved. Secura's experience in red teaming, combined with our capabilities, passion and sector-specific experience, provides our customers with the best possible basis for the clean, solid execution and management of Red Teaming engagements.

Our Related Services

Secura provides a full spectrum of security services. Typically, our customers have more needs than just Red Teaming services. Related services that Secura offers are for instance:

VULNERABILITY ASSESSMENT AND PENTESTING

With a more focused scope, Secura can investigate specific applications, infrastructures and networks. Using the mindset of a hacker, we identify vulnerabilities and provide remediation advice.

TABLE TOP CRISIS MANAGEMENT

Secura confronts your crisis management team with a challenging but realistic cyber threat incident to test cooperation and coordination. During a one-day tabletop session, your team will be presented with so-called injects, providing a realistic feel in a simulated and controlled environment. A tabletop session is beneficial for developing your cyber crisis management skills and preparing the team for other high-impact incidents.

Secura
A BUREAU VERITAS COMPANY

Why Secura?

An attacker uses a vast arsenal of tools to abuse all aspects of your digital security, technology, physical security, and human behavior to access your most important crown jewels. To mimic this type of attack requires a team of experienced hackers and social engineers with the proper knowledge, broad experience, and many specialties. Secura has built this knowledge, experience, and specialties into its team over the past twenty plus years. Therefore, our multidisciplinary team consists of top specialists with knowledge and experience in the three security domains: technology, physical security, and human behavior.

Our Red Teamers hold relevant certifications such as Certified Red Team Professional (CRTP), Certified Red Team Operator (CRTO), Certified Red Team Expert (CRTE), Master Level Social Engineer (MLSE), and many others.

Secura's experience in red teaming, combined with our capabilities, passion, and industry-specific experience, provides our clients with the best possible foundation for clean, solid execution and management of Red Teaming engagements.

Secura
A BUREAU VERITAS COMPANY

Interested?

Contact us today:

Follow us:

☎ +31 88 888 31 00

✉ info@secura.com

🌐 secura.com

BUREAU VERITAS 1828

BUREAU VERITAS

Shaping a World of Trust