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

1

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.

2

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, Security Innovation will use a mixture of offensive social engineering and computer network attack techniques as a real-world malicious actor would. Techniques used are physical pen test, phishing, vishing, attacks from the internet, and computer networking attacks in your internal networks.

3

Phase 3 | Clean Closure

Once the attack is over, the Clean Closure stage begins. This stage involves managing the digital remnants from the attack and providing the Blue team with evaluation sessions to review the incident timeline, fostering learning and awareness. The end result is a detailed technical report and an assessment of your overall security maturity within the threat landscape.

These phases are included in Security Innovation'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. It's 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 with configuring 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 across all segments, including finance, industry, and public sectors. Security Innovation, however, believes that there is no one-size-fits-all Red Teaming program that can effectively serve every type of organization. That's why Security Innovation uses service levels for Red Teaming, with a differentiation in the Red Team assessment's depth, variety, and duration. This allows you to choose the service level that best suits your organization's needs and budget.

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 primary goal for the Red Team is to achieve the defined objectives, rather than prioritizing stealth. Providing more information upfront can often make the process of assessing an organization's security posture more cost-effective.

RT Core

Red Teaming Core is a comprehensive attack simulation service designed for medium to large enterprises with in-house Blue Teams. This offering consolidates threat analysis and reconnaissance into realistic attack scenarios based on MITRE ATT&CK Techniques, Tactics, and Procedures (TTPs). Our engineers identify areas where the organization's defenses are already sufficient, allowing the assessment to focus on true vulnerabilities. By pre-determining these strengths and weaknesses, we can ensure the Red Teaming Core engagement remains cost-effective by only targeting critical needs.

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.

Red Teaming in OT

This is our Red Teaming Pro service designed specifically for organizations with critical operational technology (OT) assets. Using a layered approach, the Red Team first gathers information crucial for understanding your OT processes, then works to obtain access to your OT networks. Our tailored attacks targeting these industrial environments are carefully designed to mitigate any risks to your operations.

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. Security Innovation’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.

SECURITY INNOVATION
A BUREAU VERITAS COMPANY

About Security Innovation/ Bureau Veritas

Security Innovation is a leader in software security, providing comprehensive assessment solutions to secure software from design to deployment, across all environments, including web, cloud, IoT, and mobile. Leveraging decades of expertise and as part of Bureau Veritas, a global leader in Testing, Inspection, and Certification, we seamlessly integrate world-class security into development processes, safeguarding the way companies build and deliver products.

Security Innovation is a Bureau Veritas company. Bureau Veritas (BV) is a publicly listed company specialized in testing, inspection and certification. BV was founded in 1828, has over 80,000 employees and is active in 140 countries.

Related Services

PENETRATION TESTING

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

CYBER CRISIS EXERCISES

Security Innovation challenges your crisis management team with a realistic cyber threat scenario to test their collaboration and coordination. During a one-day tabletop exercise, your team will be presented with various simulated events to create a realistic and controlled cybersecurity incident. This session is beneficial for enhancing your cyber crisis management capabilities and preparing your team for potential high-impact incidents.

Interested?

Contact us today to start raising your cyber resilience.

sisales@securityinnovation.com

+1 877 839 7598

securityinnovation.com