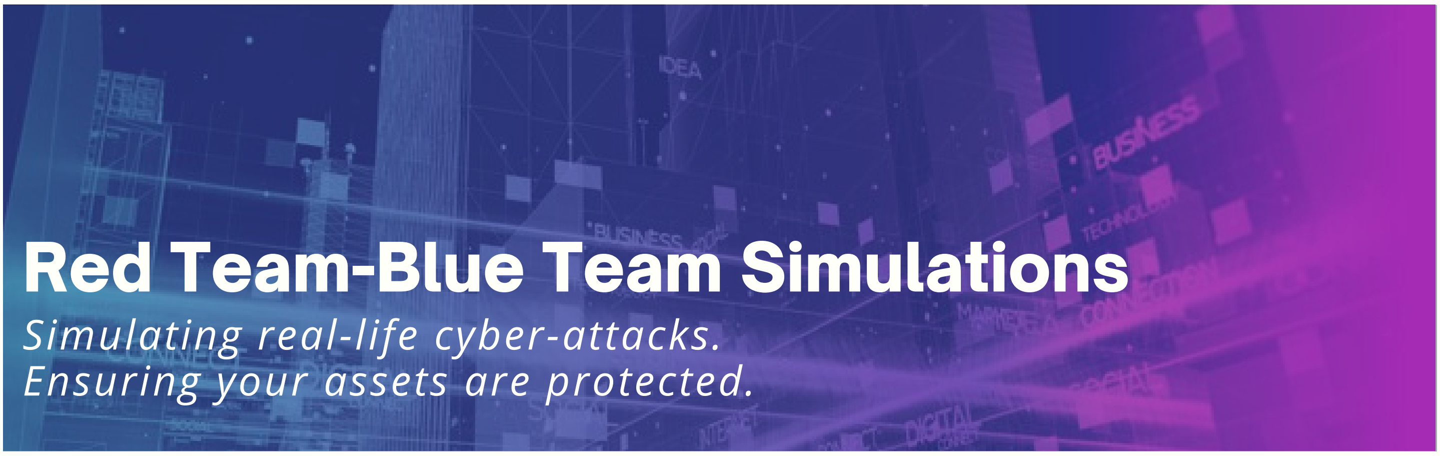
HOLISTICYBER | SOLUTION BRIEF

DEFEND WHAT MATTERS



Red Team-Blue Team Simulations

Simulating real-life cyber-attacks.
Ensuring your assets are protected.

What are Red Team-Blue Team Simulations?

HolistiCyber's red team-blue team simulations are intelligence-led security assessments designed to thoroughly test organizations' cyber resilience, threat detection, and incident response capabilities.

White-hat attackers with nation-state-grade defense expertise perform read team simulations. They reflect the methods and conditions of a real cyber-attack by utilizing the same tactics, techniques, and procedures (TTPs) used by cyber offenders. Using realistic TTPs ensures that the attacks challenge the effectiveness of the company's defenses, including technology, personnel, and processes.

Typically, these simulations are performed over a few weeks.
First, vulnerabilities are proactively exposed and then leveraged for the attacks. The efforts of the company's defenses are carefully examined, focusing on its blue-team efforts. A detailed and actionable list of remediation and mitigation options is provided, along with clear priorities. The goal is to mature the organization's security program and elevate its overall security posture.

How do Red Team-Blue Team Simulations work for me?

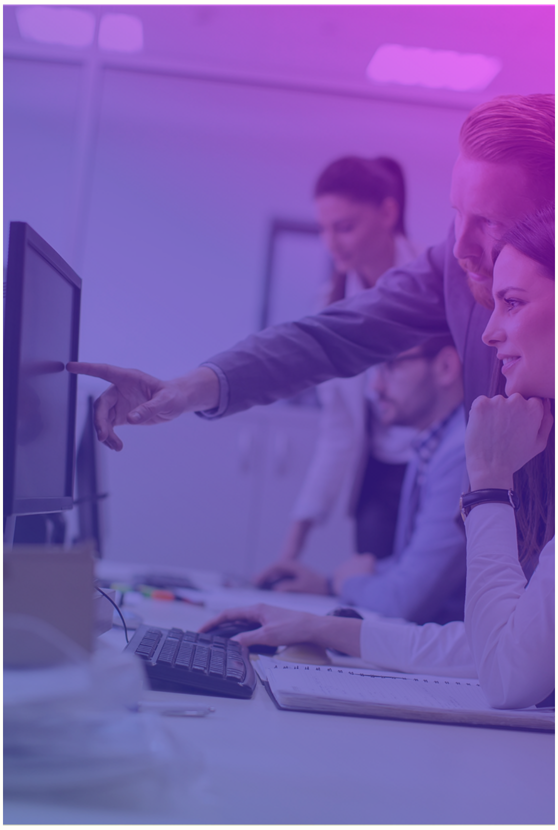
1. **Reconnaissance & identifying critical threats** - an organization can't protect against unknown threats. The simulation starts with intelligence gathering and identifying key threats while creating a list of critical cyber risks and attack pathways.
2. **Planning, staging & weaponization** - obtaining and configuring resources to conduct an attack, including setting up servers to perform Command & Control (C2), social engineering, and procurement of malicious code/malware from the darknet.
3. **Attack delivery** – the red team simulates attacks on different departments and IT systems within the organization.
4. **Reporting & analysis** - At the end of a simulation, the blue team gives the red team indicators of compromise (IoCs) that it has identified. These are compared to data collected during the simulation and incorporated into a **report**. The red team works closely with the blue team to show its TTPs, how to better detect and respond to offensive methods during incidents and analyzes the timeline of the attack. The analysis includes top priorities, precise remediation workflows, and actionable tactics to suit the company's business needs.

WHAT SHOULD YOU EXPECT?

- **Analysis of how the organization detects and responds to real-world cyber-attacks.**
- **Threat identification and real-life testing of the effectiveness of security technologies, people, and processes.**
- **Mapping exploitable routes and processes which provide access to IT systems and facilities.**
- **Pin-pointing the methods most likely to be used to disrupt business continuity.**
- **Clear prioritization of security threats that need to be handled immediately vs. items that do not pose an immediate risk.**
- **Straight-forward remediation and mitigation tactics and workflows.**
- **100% success rate.**

Often, Red team simulations are carried out without notifying a company's blue team so that it will respond and treat the activity like an actual attack. For example, when movement is detected on a compromised system being used to access the target's internal network, the blue team will likely remove that access, pushing the red team back in its progression.

Red team simulations typically rely on existing IoCs and capabilities that are already built into operating systems, processes, and other security gaps. We also use tooling to bypass endpoint detection and response solutions and avoid common threat-hunting queries by teams focused on finding nefarious activities through PowerShell/ Sysmon/ event logs. Typically, during a simulation, the team focuses on specific targets such as DevOps teams or end-users to gain elevated privileges required to achieve common attacker objectives.



Step 1

Reconnaissance & Identifying critical threats
Defining critical indicators of compromise, attack patterns and pathways, attack targets, and schedule.

Step 2

Planning, staging & weaponization
Includes network and attack sophistication, configuration, architecture, and data flow.

Step 3

Attack delivery - Attacks by top white-hat experts, including lateral movement across networks, privilege escalation, physical compromise, command and control actions, and data exfiltration

Step 4

Reporting & analysis
Probability and damage assessments; actionable plan on handling risks and fixing top security priorities.

Why HolistiCyber?

1. **Nation-state-grade expertise** - our staff of white-hat security experts is composed of former military and government offensive practitioners who can examine the attack surface from the vantage point of the attacker and not only from the company's vantage point. We have a solid grasp of the sophisticated tooling available to today's attackers and access to those attack tools.
2. **Holistic approach** - we tie compliance, remediation, and mitigation solutions to each company's unique business objectives and workflows. Security should complement productivity and growth and avoid hindering them.
3. Our engagements have a **100% success rate**.

"HolistiCyber's red teaming experts have a deep knowledge of data security and have performed realistic attacks at the highest technical and legal standards.
These dedicated professionals have significantly improved our cybersecurity program by using the same mindset and tooling of cyber-criminals and providing in-depth analysis and complete post-test care."
CISO, sizeable financial corporation, USA