CYE

The Step-by-Step Guide to Implementing a Winning **Red Team Strategy**

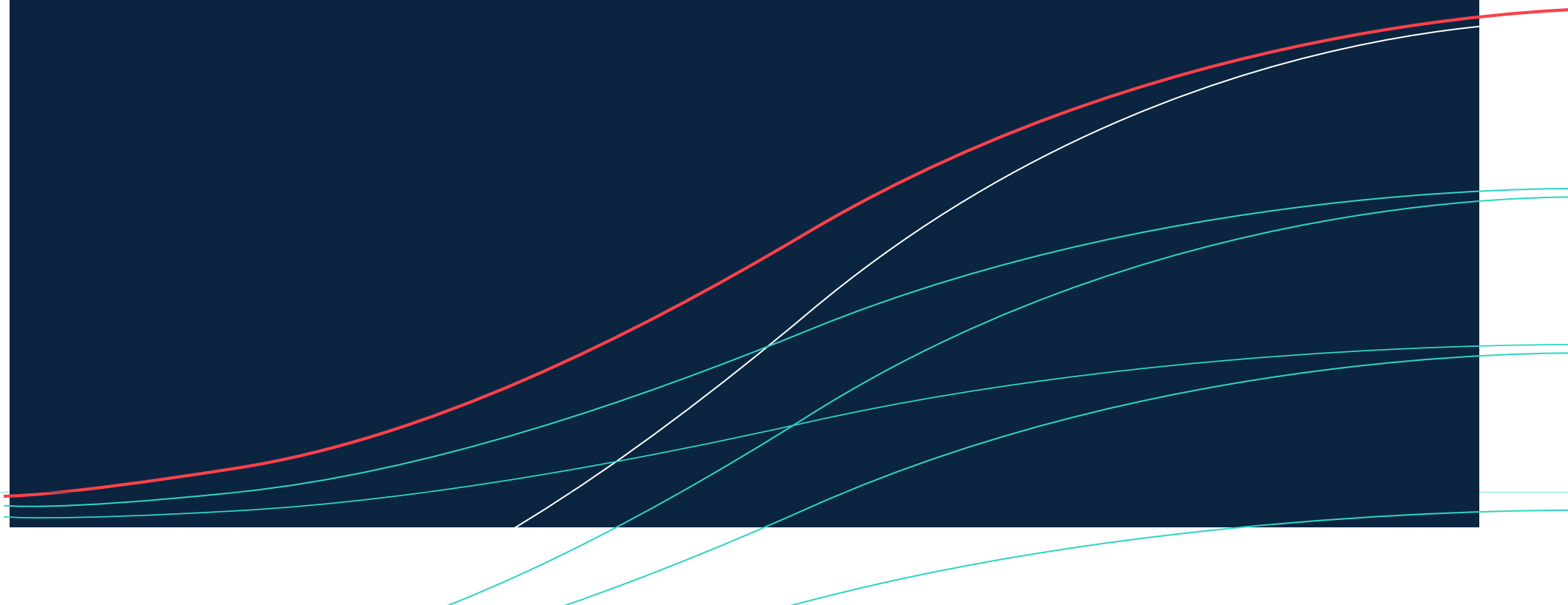


Table of Contents

Introduction Page 3

Steps to an Effective Red Team Strategy Page 5

- **Step 1:** Scoping the Engagement Page 5
- **Step 2:** Gathering General Information Page 6
- **Step 3:** Performing Research and Reconnaissance Page 7
- **Step 4:** Developing the Work Plan Page 8
- **Step 5:** Executing the Plan Page 9
- **Step 6:** Documenting and Communicating the Findings Page 10

How to Choose a Red Team Page 11

How CYE Can Help Page 12

Introduction

Red teams are in the news, yet many organizations have questions about exactly what they do, and how red teams can work with their own security groups. This guide explains what a red team is, why it is needed, how it operates, how to work with external and internal teams, and much more.

A red team is a group of highly skilled individuals who emulate the attack methods that an actual attacker would use. Sometimes called "ethical hackers," they help improve organizational cybersecurity by revealing gaps in cybersecurity defenses and how an actual attacker could exploit them. The goal of a red teaming exercise, according to NIST[1], is "to improve enterprise cybersecurity by demonstrating the impacts of successful attacks[2]." The red team can provide management with confidence in its security stance, based on results gathered in the context of the current cyberthreat landscape.

The red team generally works in conjunction with an internal blue team – the defenders – who are responsible for maintaining the organization's security posture. The red team conducts reconnaissance, infiltrates networks, and tries to reach valuable business assets, providing insights so the blue team can help the organization be prepared for the next attack. The red team is devious, mimicking the approach of sophisticated hackers; at the same time, it must remain ethical and professional. This calls for an experienced, professional team that is steeped in the tactics, techniques, and procedures (TTPs) of attackers as well as knowledgeable about the tools and frameworks they use.

Red team exercises generally take place once or twice a year. However, when a major attack happens, it makes sense to conduct a red team assessment focused on that specific attack (e.g., a ransomware attack that hits other organizations in the same industry). This can reveal gaps that the organization should address if it is to respond adequately.

Many organizations have their own internal red team, which conducts periodic red teaming exercises. Even so, most enterprises will want to enhance this with external. Internal teams can find themselves unduly influenced by company organization and politics, or may concentrate on a specific methods to the exclusion of others that might pose a bigger threat. The best approach is to use both internal and external red teams[3]. This gives flexibility to incorporate fresh perspectives and to address emerging threats quickly, bearing in mind that it takes on average 277 days[4] to discover and contain a breach.

[1] https://csrc.nist.gov/glossary/term/red_team

[2] https://csrc.nist.gov/glossary/term/red_team

[3] www.isaca.org/resources/isaca-journal/issues/2018/volume-5/red-teaming-for-cybersecurity#1

[4] www.ibm.com/reports/data-breach

Steps to an Effective Red Team Strategy

A red teaming engagement is not a quick undertaking. Several steps are involved and some of them can be lengthy.
They include:

1. Scoping the engagement
2. Gathering general information
3. Performing research and reconnaissance
4. Developing the work plan
5. Executing the plan, uncovering weaknesses and gaps while remaining undetected
6. Documenting and communicating the findings

Step 1 Scoping the Engagement

The first step is to conduct discussions between the target organization and the red team, with the purpose being to agree on the scope of the engagement, the ultimate goals, and especially the rules of engagement. Will the entire IT infrastructure be targeted, or just specific parts? Is the red team allowed to set up a command and control center? Are certain tactics prohibited?

Preparatory discussions will allow the team to fully understand which specific targets are in scope, and which types of attacks are permitted, such as web application attacks, network penetration attempts, and social engineering attacks such as spear phishing.

A key aspect of the preparatory phase is to ensure both the red team and the target organization fully understand the timing of the engagement. Because a typical engagement can last 4-5 months, it Is important to set expectations at the beginning. The red team will not inform the client when the cyberattack will be conducted, nor will the internal defense team be aware that a red team engagement is being planned. However, the organization should make sure that relevant logs are being aggregated and alerts have been configured as part of the normal security defense program. Also, it is very important to define a point of contact in the organization and a communication channel, in order to differentiate alerts raised by activities of the red team activity and a real threat.

Recommendation:
The red team should obtain a letter of authorization from the client/the organization's management granting it permission to conduct cyberattacks.

Step 2 Gathering General Information

The second step is to dig deep into the organization. This is when the team learns as much as possible about the target organization's employees, technology, and security defenses. This effort involves gathering detailed information on which applications are being run, what sites are being used, which services are fundamental to the organization, and the employees themselves. Employee information is especially important when it relates to those working in the security and SOC teams: knowing their physical location, normal working hours, specialties, and any personal information obtainable from social media and other open sources form part of the overall profile of the target organization.

When dealing with an organization with multiple sites, the red team gathers specific information for each region, determining any specific working hours, holidays, and customs that could impact operations and reveal optimal off-hours when a red team attack would be more difficult to detect.

Step 3 Performing Research and Reconnaissance

This is the phase that allows the red team to gather in-depth information about the targets for the engagement. Information included in this phase may include:

Networks and operations: included are the IP address ranges as well as any open network ports, API endpoints for mobile devices, and security controls in place. The team looks for potential infiltration and exfiltration points.

Employee information: target individuals are identified and detailed information gathered on each employee in the organization. Valuable information includes email addresses, social media profiles, phone numbers, departments and titles, ID numbers, and the like. The red team finds high-value targets, such as employees working in the security or SOC teams, as well as those who are likely to have elevated privileges. The team also attempts to identify employees that are likely to fall victim to social engineering attacks, such as non-technical personnel.

Vulnerabilities: this activity involves focusing on the latest vulnerabilities, since there is a high likelihood that those have not yet been patched by the target organization. The team will include specific vulnerabilities in the eventual work plan, and will develop custom attack and exploitation methods for each of them.

Step 4 Developing the Work Plan

When all the foregoing information has been gathered, the red team creates its work plan focusing on attack methods, dates, times, and targets. The team will create social engineering attacks that are specific to the target organization, as well as developing malicious payloads and falsified personas as needed. All the methods used by the red team must emulate the TTPs of actual attackers.

Clearly, such planning and preparation calls for sophisticated engineering work; the team will need to develop its own methods of exploiting new or emerging vulnerabilities. Savvy red teams will build a lab that duplicates the exact environment of the target company. In the lab, the team conducts in-depth research into each vulnerability that will be exploited, and creates its own methods of exploiting it. Then, each method is thoroughly tested before it is executed, to make sure it will not trigger an alert. All of this is complex and time-consuming, yet the end result will be a higher rate of success.

Social engineering attacks are a key tool in the red team's arsenal. Based on information gathered during the research and reconnaissance phase, the team will be able to determine which types of attacks could target those employees who are most likely to fall victim.

Recommendations:
Make sure the red team has a sophisticated lab that is capable of duplicating the exact target environment, and customizing exploits for emerging vulnerabilities.

Make sure to choose a red team that is experienced in creating custom social engineering attacks, and doesn't simply use common attack methods that are likely to be detected. These might include brute force attacks, password spray attacks, or widely available phishing emails.

Social engineering and password attack methods

- **MFA request bombing:** multi-factor authentication is a valuable tool in preventing account takeover since it requires the user to provide an additional factor in addition to username and password. However, older versions of MFA that employ one-time passwords or push prompts can be used to trick users by sending multiple MFA requests to the device, until the user finally breaks down and accepts the authentication.
- **Spear phishing attacks:** targeted email attacks appear to come from a trusted sender, often using information gleaned from open sources such as social media postings. The goal is either to infect the user's device with malware, or to get the user to reveal information, such as his credentials.
- **Business Email Compromise (BEC):** the email appears to come from a trusted business or person, such as the CEO, HR or finance department of the organization. Instead of being legitimate, it contains a phishing link, a malicious attachment or other method for gaining access to the network.

Step 5 Executing the Plan

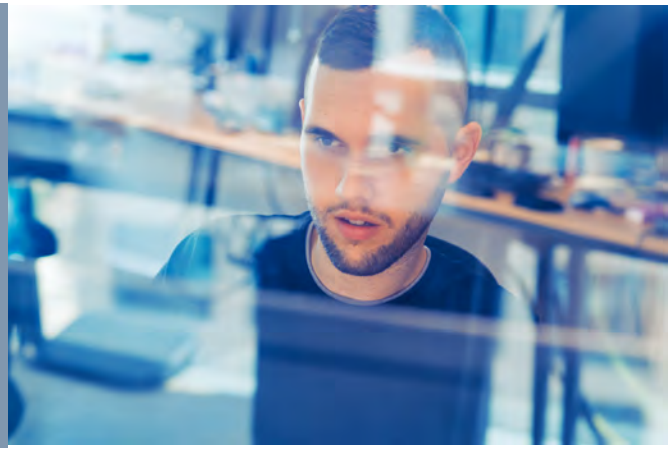
The red team will base its timetable on the best dates and times to try to gain access to each of the relevant regions. Executing the plan according to this timetable, the team tries to break into the network via an unpatched vulnerability attack, custom social engineering attacks, or other method custom-crafted to evade detection.

Once the team has gained access to the network, it works covertly, gaining a foothold and establishing persistence. All the while, the team mimics normal users so as not to raise an alarm. The red team will set up a command and control center (C2) so that it can communicate externally while remaining undetected inside the network.

While inside, the team gathers information and does further reconnaissance, moving laterally across the network. In so doing, it finds opportunities to escalate privileges and perform other actions designed to reach the goal of taking over the domain (in AD environments). When that happens, the red team will have access to every computer and user in the organization. If this had been a real attacker, the damage could have been severe, including blocking the entire security team. When the red team takes over the domain, it is usually considered a win.

Recommendations:
Make sure the red team has the capability to establish its own C2 in order to remain stealthy while gathering information, and does not resort to off-the-shelf products that are easy to detect.

If the SOC team receives an alert, and POC verifies it is due to red team activity, allow the team to proceed as they normally would. Only intervene if business disruption will occur – e.g., reimaging that could take key servers offline for hours or days.



Step 6 Documenting and Communicating the Findings

During the execution phase, the red team documents all actions taken and results that occurred. The last step of the red team engagement is to report the actions, reactions, and results to relevant parties, including IT management, CSO, CISO, CIO, and others as appropriate. The report should clearly and completely document what worked and what didn't. It should include details on discovered vulnerabilities and how a real attacker could exploit them.

The report should also include recommendations for future actions. It can highlight best practices for remediation, as well as the most cost-effective mitigation plans based on the specific needs of the organization.

Recommendations:
For completeness, the red team report should include information on alerts found by the security/SOC team.

Ensure the red team can present findings directly to senior management.

How to Choose a Red Team

CISOs considering a red team strategy as part of their security plan often face the choice of creating a team in-house or hiring a third party. Engaging an external team is almost always a good approach, whether or not the organization has an internal team, since it provides flexibility, impartiality, and a broad, experienced team. In fact, given the scarcity of qualified red teamers in the market, it might prove difficult to build a robust internal team. Therefore, looking to external providers may make sense for almost any organization.

Selecting a red team provider involves making sure the provider has the tactical, technical, and strategic skills required, including a deep awareness of systems, protocols, security tools and measures.

In addition, key capabilities include:

- A solid track record of successful red team engagements in similar organizations
- A proven ability to act ethically and professionally
- Strong social engineering skills: ability to create custom social engineering attacks tailored to the target organization
- A sophisticated lab that can duplicate the environment of the target organization
- Strong cybersecurity development skills including the ability to customize exploits of emerging vulnerabilities
- The ability to create a covert command and control capability
- Excellent communication skills with all levels of the organization

How CYE Can Help

CYE's cybersecurity optimization platform, Hyver, enables businesses to assess, quantify, and mitigate cyber risk so they can make better security decisions and invest in effective remediation. CYE combines technology with red team activity to deliver the most comprehensive organizational security assessments and contextual risk analysis and insights. CYE provides complete visibility into possible attack routes; streamlines and prioritizes the remediation process, and allows security leaders to better understand the true cost of threats and remediation. Using CYE, companies can eliminate the need for numerous cybersecurity tools and reduce the likelihood and the impact of cyberattacks.

Next Steps

Learn more about red teams vs. blue teams

Read how red teams help CYE optimize cybersecurity with Hyver

Discover how to choose a cyber risk quantification strategy

CYE

Would you like to learn more about how CYE can help you in your red teaming efforts?

Contact us