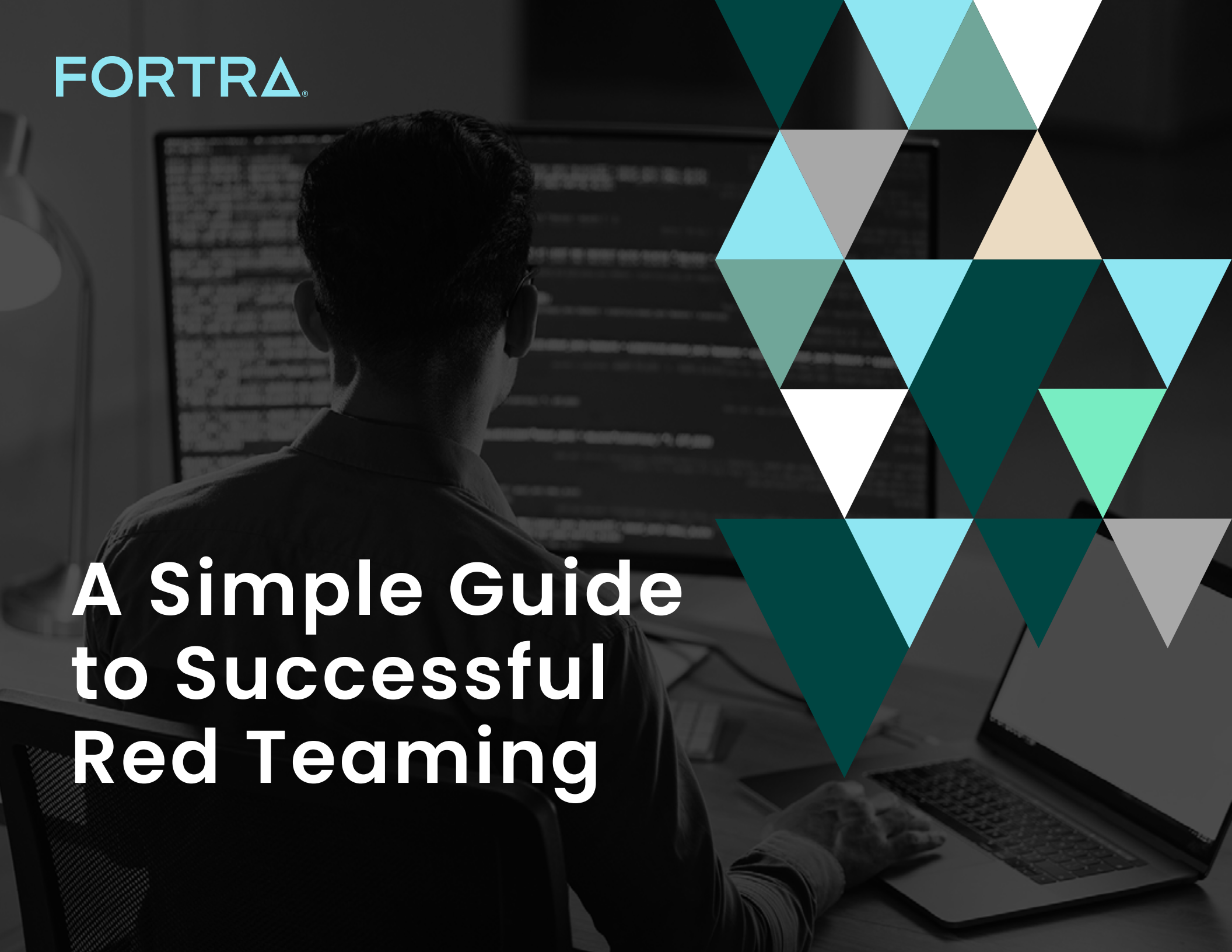
FORTRA



A Simple Guide to Successful Red Teaming

Table of Contents

As threat actors innovate their tactics, security teams need to match them step for step.

We can't fight new and complex threats with old and predictable techniques. It's time that the gloves come off and that organizations subject their networks, cloud resources, and internal assets to not only real-world threats, but real-world attacks – and that they do it before real-world cybercriminals get a chance to.

Once, red teaming was seen as just a "nice addition"—not anymore. Now, as attack methods expand to include more in-depth campaigns, it is one of the only ways teams can gain real-world experience against these exploits. It also provides a level of comprehensive preparedness now inseparable from any true defense-in-depth approach.

"Red teaming shows security teams where they are, where they need to be, and – perhaps most importantly – how they would respond in a high-pressure environment with everything on the line."

They say you can't train those emergency instincts, but first responders do it every day. Think about red teaming as fire drills, earthquake preparedness, and critical injury simulation so that your first responders won't feel like deer in the headlights when the real thing strikes.

"Red teaming shows security teams where they are, where they need to be, and – perhaps most importantly – how they would respond in a high-pressure environment with everything on the line."

What is Red Teaming?

What is Red Teaming?

Red teaming is a live attack simulation that tests not only the strength of the network, but the teams' ability to respond.

In practice, it involves replicating the malicious tactics of a long-term embedded adversary in a network in order to improve an organization's ability to detect and mitigate intrusions. In this way, it is a far more global assessment of the strength of the security posture than penetration testing or vulnerability management alone, critical steps as those are.

Red teaming is the crown jewel that completes an exhaustive offensive cybersecurity strategy, and without which uncomfortable security questions will always remain.

- **Comprehensive** | While penetration testing and risk analysis does a lot for network architecture strength and security awareness, nothing tests the system as a whole – people, policies, processes, platforms, and all of that under pressure – like a red team assessment.
- **Simulates Attackers with Years of Preparation** | That's why a red team assessment requires a holistic view of the organization from the perspective of the attacker. In a real-world attack, the adversary has weeks, months, or even years of lead time to collect data and mine for sensitive information, credentials, and network architect specifics before ever launching their attack. When they do, they are ready.

  Similarly, red team (either hired or internal) are often given additional information before beginning in order to more accurately simulate an actual attack. This can include credential lists, network maps, or contact information of key players. **Once they begin, the in-house security team is put to the test as they work for days or even weeks defending against a coordinated malicious campaign**. And "though key parties may be informed that a red team campaign is taking place, most employees, including the organization's IT team, won't be notified until after the fact, making it as authentic as possible."
- **Intentionally Innovative to Keep Teams on their Toes** | The purpose of red teaming is to demonstrate the creative, unexpected, and unrelated routes threat actors can take to compromise internal assets. This serves as a valuable learning experience for the organization that is targeted. Red team consultants should become trusted partners of the organization's security team and provide guidance for how to strengthen security.

TLDR Takeaway: The outcome of red teaming is always a favorable one. Either the internal security team thwarts adversarial advances and that validates their current defensive measures, or blind spots are revealed and decision makers have even more specific information on where to shore up security measures.

Pen testing vs. Red Teaming

Pen testing vs. Red Teaming

To fully understand the unique benefits of red teaming, it's best to make the distinctions between it and pen testing explicitly clear. While they do share similarities, they are both crucial to a zero-trust approach for very different reasons. **In a nutshell, penetration testing has a broader and shallower scope, while the red team's scope is wider and deeper, attempting to go through every security layer**. However, it's worth delving into the intricacies.

The Purpose of Pen Testing:

- Exploits vulnerabilities
- Reduces the attack surface
- Assesses the quality of security controls
- Meets regulatory requirements
- Demonstrates the attack chain
- Operates within a defined scope
- Test focused on objectives
- Clear boundaries are set for pen testers
- There are certain test types: network, web application, social engineering, etc.

The Purpose of Red Teaming:

- Simulates an advanced threat actor
- Tests the defensive capabilities of the organization
- Engages people, processes, and technologies
- Assesses response deficiencies
- Evaluates telemetry and visibility
- Improves defender response time
- Lays out defined scenarios for measurable results

Pen Testing Use Cases:

Vulnerabilities | Identify the most critical vulnerabilities to attend to

Remediation | Confirm implementation of remediation measures (patching, reconfiguration)

Compliance | Verify compliance with mandated security measures

Upgrade Validation | Make sure improvements did not cause new problems

Employee Awareness | Security-test employees (phishing, ransomware)

Application Security | Validate app security prior to use

Red teaming is about what the security team can learn from adversarial attacks and how those learnings help them fortify security. Penetration testing is about uncovering as many attack paths as possible. Both methods are vital for a defense-in-depth security strategy and as means of hardening systems against attack.

Red Teaming Use Cases:

External Breach | Exposes vulnerabilities most likely to be exploited in a breach

Embedded Long-Term Actor | Imitates the low-and-slow tactics of a persistent attacker

Assumed Breach | Provides detailed evidence of how much an attacker could accomplish once inside the network, system, or acting as an authorized user.

Purple Team Exercises | Train blue teams to better understand attack techniques. Purple teams make both red and blue teams two parts of a whole, working towards the same goal of security improvement. Red teams train blue teams through insight and infiltration, and blue teams train the red through patching gaps until they can't find the same vulnerability twice.

TLDR Takeaway: Perhaps the biggest difference is that while pen testers operate within certain parameters, red teamers are free to pursue their target using any means necessary.

Red Team Use Cases: What Does a Red Team Exercise Look Like?

Red Team Use Cases: What Does a Red Team Exercise Look Like?

To fully grasp the benefit, it helps to understand the various aspects that go into a red team exercise. Creating the most effective simulation requires several components:

- **Pre-seeded Knowledge** | It's unrealistic to expect red teamers to begin with no prior knowledge of the company since attackers would have been performing active reconnaissance for months. That's why many red teamers are provided with assets such as a detailed map of the network, credentials for key accounts, and knowledge about users in a position of value to the attacker.
- **Long-Term Operations** | Red team attacks can be low-and-slow. This helps keep the endgame in mind. Many organizations have an idea of where they stand at this moment, if all their security assets were at the ready and their team were on high alert. However, that's not when attackers strike. A typical red team engagement could take weeks, even months, to carry out and is true to the form of a real-world threat campaign. This kind of experience pays off as companies learn what it takes to secure their networks long-term, and which technologies to invest in to create real pain for embedded actors.
- **Cyber-War Gaming** | Organizations can also stage red vs. blue cyber-war games to sharpen in-house security staff. Under the supervision or auditing oversight of a managed Red Team service, teams can recreate an attack simulation while safely ironing out team roles, testing new technologies, and gaining increased communication skills.
- **Attack Simulations** | Red teams can also upskill network defense teams by designing and executing cyber security exercises. These fabricate a realistic attack scenario, believable hacker, and reasonable timeframe. Then, the red teamer is whitelisted any permissions the attacker would likely have and given permission to walk through the attack steps one by one. The methodical approach presents a way to discuss pain points one by one, validate procedures, and train blue operators to use them.

The purpose of red teaming is to validate security measures and educate the blue team by putting an organization to the test using up-to-date threat vectors it might encounter in the real world. These include vulnerability assessments, social engineering attacks like phishing, and penetration tests like Cobalt Strike. As Sun Tzu said, "If you know yourself but not the enemy, for every victory gained you will also suffer a defeat."

TLDR Takeaway: Red teaming requires understanding the enemy because, for a moment, you are the enemy.

The Benefits of Red Teaming

Security Benefits

The best defense is a good offense. Simulating how an attacker would really behave is the ultimate form of advanced security – test yourself before they test you. A real-world malicious hacker would perform an increasingly stealthy, long-term attack that would likely hit from various angles at once. There really is no way to prepare at scale for this type of attack unless you simulate it yourself.

The security upsides of a red team engagement encompass:

- **Discover ticking time-bombs** | Uncover attack vectors that attackers could exploit.
- **Learn likely attack paths** | Demonstrate how attackers could move throughout your system.
- **See how safe you really are** | Provide insight on your ability to prevent, detect, and respond to advanced threats.
- **Create Emergency Exits and Plan Bs** | Identify alternative options or outcomes of an action or attack plan.
- **Do first things first** | Prioritize remediation plans based on what is causing the greatest risk
- **Get buy-in on budget** | Build a business case for improvements, deploying new solutions, and other security spending

But it doesn't stop there.

Business Benefits

As more CISOs are stepping out of the security-only box and into the general 'business driver' role, enterprise-wide advantages are expected for cyber security initiatives. As we move further into the digital revolution, security will increasingly mean the ability to compete, land contracts, and enter new geographies. Hardening your network and human assets with red team engagements will not only ensure you have the chance to get there, but to stay there.

The business boons of red teaming include:

- **Reporting** | As established teams retool for engagements that require full disclosure, red team reporting makes that possible.
- **C-suite advisory** | Red teams can tell executive teams how their enterprise will stack up against real-world threats, so they know how to allocate and prioritize security assets going forward.
- **Long-term ops** | A red team exercise reveals how a security team performs against long-tail attacks and is the only way organizations can gain this knowledge without experiencing one in the first place.
- **Security strategy** | As rapid innovation continues to spell competitiveness in the marketplace, being able to secure that rapid expansion becomes more than a safety measure; it becomes a tactical advantage.
- **Compliance** | Red teaming is becoming increasingly mandatory. For example, under the Digital Operations Resilience Act (DORA), financial entities in the EU will be required to use the Threat Intelligence-Based Ethical Red Teaming (TIBER) framework beginning in 2025. In the US, recent updates to NIST introduced a new control enhancement that calls for red teaming. With the Federal Information Security Modernization Act (FISMA) and FedRAMP both aligning with NIST requirements, red teaming will soon be required for federal agencies and contractors.

How Companies Can Leverage Red Team Engagement

How Companies Can Leverage Red Team Engagement

While red team benefits are essential for testing networks against sophisticated attacks, they must be weighed against an organization's cyber maturity, readiness, and preparation. Once those elements are in place, it's time to fine-tune use and get the most out of your engagements.

Your Red Team Readiness Checklist

You know you're ready for official red team activity when you can answer in the affirmative to the following scenarios:

- **You have new security assets** | After you've implemented new security software, programs, or tactics in your organization it's good to stress test them, and the teams that use them. See how ready they are for real-world action and identify quickly the areas of weakness so you can train your teams right from the start. Performing these tests without your employee base knowing will also enhance the authenticity of the results.
- **A breach has occurred** | Whether this has happened to your environment or not, when hearing of the latest data breach it is wise to see how your organization would respond in a similar scenario – and do so before it really has to.
- **Routinely and regularly** | As both threats and your organization continue to evolve, it is essential to test routinely and regularly to ensure that your current defenses are adequate to defend against emerging exploits.
- **When you have reached a certain level of cyber maturity** | This is when your security posture (including architecture, policies, and people) is strong enough to stand on its own and is ready for the next stage of testing and continuous improvement.

How Cyber Mature Must You Be?

Level 4: Attack Management | At this level, the whole picture is in view. Scans and penetration testing data are used to analyze how an attacker could move through the network, and which vulnerabilities they could use to access critical assets. **This is the point at which you are ready for red teaming**. The fifth and final level is the realization of a fully developed and mature security posture; one that takes the scope of the entire ecosystem into account, uses data from pen tests, scans, and red team engagements to identify trends, and implements remediation controls with advanced technology.

Level 3: Analysis and Prioritization | Often with the help of penetration testing, you've identified and verified threat potential, and ranked vulnerabilities based on exploitability within your network.

Level 2: Assessment and Compliance | Some thought has been given to industry best practices and compliance standards. At this level, companies should start looking into penetration testing.

Level 1: Scanning | At this level you've begun vulnerability scans that check for device misconfigurations and cover web and network vectors.

Level 0: Maturity is Non-Existent | This is ad-hoc vulnerability management with no cohesive strategy and only reactive measures like an antivirus or manual patching.

TLDR Takeaway: Ultimate security maturity is built on solid foundational security tactics that grow in complexity, culminating with red teaming.

Managed or In-House?

Managed or In-House?

Since red teaming r**equires extensive preparation, foreknowledge, and security prowess, many organizations choose to hire out**. When considering managed versus in-house red team options, it's important to consider a few realities of Red Teaming before making a decision. Here are a few things to keep in mind.

Managed vs. In-House Red Teaming

- **Do you have the cycles required to prepare?** | A red team engagement worthy of reporting to higher-ups requires extensive preparation, foreknowledge, and security prowess. Consider if this is an additional burden your team can handle in its current state, or if doing so will result in other unfavorable security trade-offs.
- **Are you risking familiarity blind spots?** | In-house assessments are hard to maintain and even harder to perform objectively, as those too close to the architecture or too familiar with the network are prone to blind spots. Managed red team and pen testing services who test frequently - and without the knowledge of the staff - get an accurate indication of how their organization would fair against attackers on any given day; not just how their team could perform on its best day.
- **Are you cyber mature enough?** | When considering managed versus in-house Red Team options, it is also important to look at the above cyber maturity model and consider if your organization can achieve those milestones with your given resources. Organizations that are still maturing their cyber strategy do not necessarily need to miss out on the benefits of red teaming. However, they might be better served choosing a managed security services provider to help them first get to that level of readiness and then launch their subsequent red team engagements.

TLDR Takeaway: Assess your time, technology, expertise, and overhead, to determine whether you need in-house red teaming or if you need to partner with a managed red team provider.

Managed: Using as third party to conduct red team engagements and report findings to you.

In-House: Employing highly skilled staff within your organization to conduct red team engagements.

How to Choose a Managed Red Team Provider

A managed partner can offload the burden of lifting you to cybersecurity maturity before even beginning your red team engagements. Then, they can pick up from there. However, not all red teams are created equal.

You need to have the right relationship. A red team needs to be symbiotically paired with the blue, and with the executive security staff at large. That means the 'keys to the kingdom' in many instances, so don't trust this to just anyone. While it may take months to know every new hire on your team – or who they know – you can sidestep that issue by opting for a red team provider that has their reputation on the line and a line of Fortune 500 clients.

Your Managed Red Team needs to have the right tools. Find a red team with a diverse, advanced tool set. The right tools make all the difference when attacking networks, applications and systems that have also been protected by the best. To launch a full-scale attack with limited resources, time, focus, tooling, or malicious expertise is to sell the whole operation short. You could waste a lot of time and still not be adequately prepared for the threats that are to come.

TLDR Takeaway: It's important to know what to look for in a red team partner, as they will hold your trust, strategy, and (for a moment) network in their hands.

Maximizing Your Red Team Engagement

Once you have decided on your approach, you're ready to maximize your red team results. Here's how to set the stage, whether managed or in-house.

- **Have the right conditions**. Red teamers need an open learning culture with the ability to continuously train and improve their skill set.
- **Set clear objectives**. Plan from the outset. This will not work as an afterthought but should be an integral part of your security posture and should have measurable goals in mind.
- **Get the right tools**. Make sure that you provide your team with the right testing, vulnerability management, and further assessment tools for analysis.
- **Focus on key issues**. Red teaming should produce quality thinking and advice, not qualitative results. A lot of time and resources will go into red teaming your environment, and level-setting before the games get underway will make sure you, your team, and your red team don't waste any of it.

"Red teaming should produce quality thinking and advice, not qualitative results."

Conclusion

There are things about your organization that you will learn via red teaming that you cannot learn in any other way. Even if you waited for a real-world attack to teach you, those lessons would come too late. Armed with an effective red team approach, you will be prepared to:

- **Test your tools** | CISOs can't afford to fall behind in the CI/CD cycle, but they need to know that the new solutions they implement today aren't just languishing or being underutilized tomorrow. Red teaming is a great way to get ahead of tool waste and maximize the assets already at your disposal.
- **Test your talent |** Teams need to have the opportunity to not only learn the platforms in the classroom but test their knowledge in the lab. Not only your tools but your talent needs to see the threats beforehand so they can perform the actions and build confidence that they will be able to respond with clarity in the future.
- **Honor security as business-driver** | Cybersecurity objectives and an organization's growth goals are increasingly seen as inseparably intertwined. As a go-to resource for risk assessment, M&A decisions, and supply chain decisions, security teams need to be ready with facts on-hand. Now, more than ever, companies need the business benefits that enhanced reporting, C-suite guidance, and reliable long-term security operations provide.

To help you advance towards this end. Whether it's your in-house red team or a third party you've engaged, the team should be using the top red team tools available, including Cobalt Strike and Outflank Security Tooling. Together with penetration testing software or services, they form the basis of a unified offensive security strategy designed to help organizations keep pace with the continuous assaults of an evolving threat landscape. That way, when the attack comes, they'll be the ones doing the surprising.

Today's businesses may not be able to stop the wave of oncoming threats, but they can defend against it with the battle-tested confidence only red team operations can provide.

FORTRA®

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-ip-gd-1024-r1-db