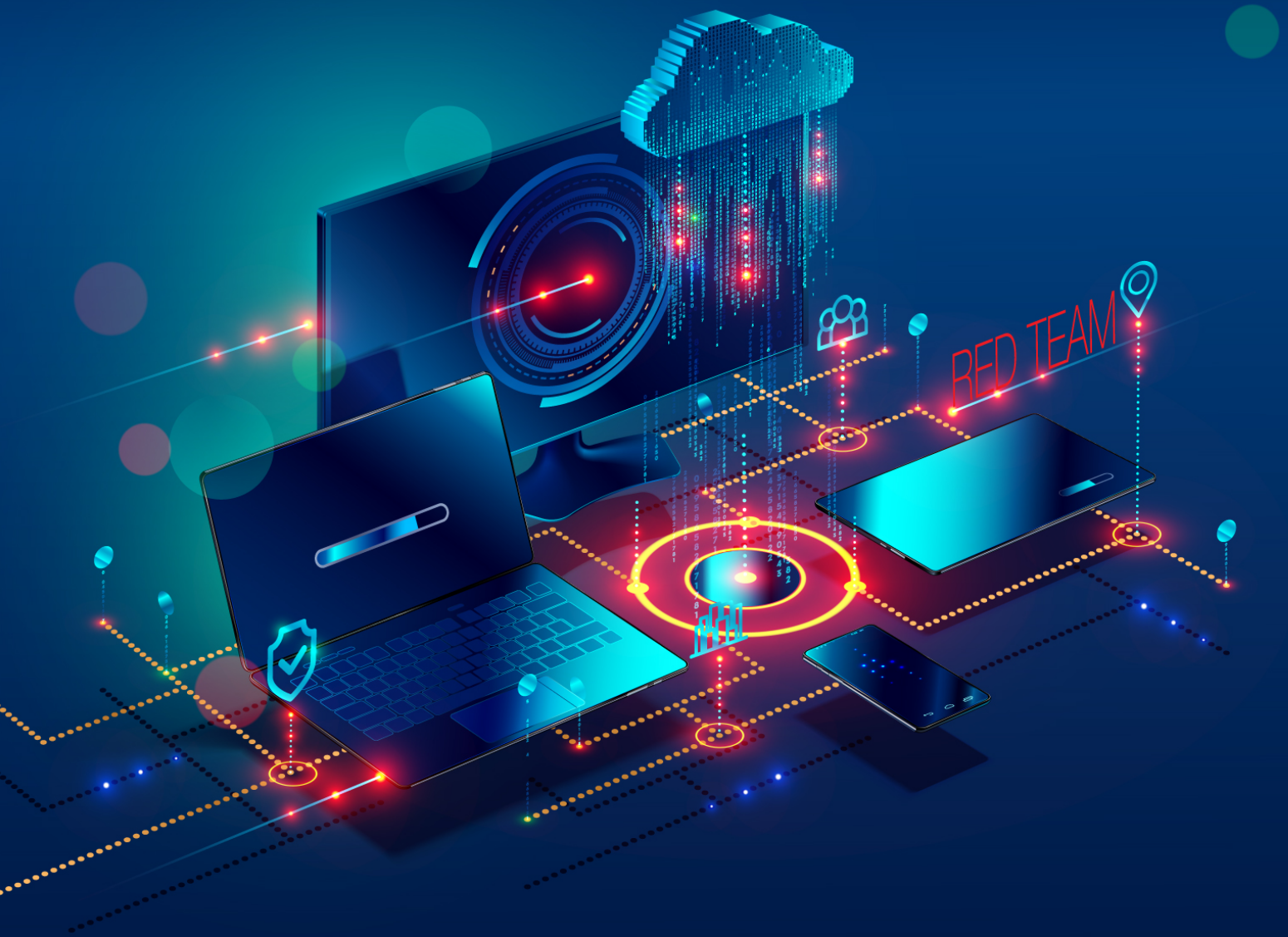
Red Team Attack Simulation

Want to get hacked, without being hacked?



themissinglink®

The term 'Red Team' was borrowed from military and intelligence operations. Red Teams were the offensive team, and would try to challenge the plan for offensive/defensive operations and identify gaps that could lead to failure.

The role of a Red Team operation in the cybersecurity world is much the same: challenge the organisation's security posture to identify gaps in their defences and demonstrate how the organisation would fare against real-world adversaries.

Most organisations strategically apply the defence-in-depth principle to their environments, ensuring that there are multiple layers of controls across people, processes, and technology. If any security control failed, another would compensate.

Applying this strategy takes time, resources, and effort. Most organisations have a vision for their security, a roadmap to achieve it, and are working diligently through a plan towards it. That plan may involve hardening the environment, installing cutting-edge security solutions, or hiring the best threat hunting and incident response teams.

But how can you validate that this massive investment is effective?

Penetration Testing vs Red Team Operations

For a long time, the security industry perceived Penetration Testing as the answer. In the beginning, it was true. However, years of accumulated red tape reduced Penetration Testing to limited-scope assessments, focussing only on the technology stack, executed with somewhat brutality, while ignoring layers upon layers of security controls.

As a result, Penetration Testing results often give stakeholders a false sense of security, such as when security solutions detect malicious activity, even though the penetration testers did not attempt to evade detection. And, conversely, a false sense of insecurity, for example when identified vulnerabilities are reported as critical, even though exploiting them when all the mitigating controls are in place is unlikely. Moreover, Penetration Tests never assess the organisation's response capabilities or the organisation's security posture as a whole.

On the other hand, Red Team operations challenge the organisation's security posture holistically. This is done/accomplished by simulating a real threat actor, negotiating all of the security controls in the environment with finesse and sophistication while targeting not only the technology stack but also the people and processes, to achieve objectives that strategically align with the organisation's goals.

Many people think that Red Team operations are advanced Penetration Tests, assessments that involve social engineering or a physical intrusion. While a Red Team operation may sometimes involve social engineering or a physical intrusion, such statements demonstrate a lack of understanding of the concept.

"But isn't a full-scale red operation an overkill for a small organisation or one with limited maturity?"

Shades of Blue

Every organisation has a different security maturity level. Organisations have different kinds of security solutions in place; some organisations have an internal Blue Team (defensive security professionals), while others outsource their SOC to external vendors; some employ a large team of security experts, while others have a vigilant team of IT enthusiasts that love cybersecurity.

No matter what the organisation's level of maturity is, a Red Team operation will always bring new information to light and help address gaps and weaknesses in the security posture.

33%

of organisations say their internal teams fail to catch Red Teams

Source: darkreading.com

Shades of Red

Not all Red Team operations are the same. Just as every organisation's operational environment is unique, every Red Team exercise must be tailored to the environment. Every operation is tailored to achieve bespoke objectives while playing to the strengths and weaknesses of the organisation's defences.

An effective Red Team must strategically align with the organisation's goals. We often hear stories from our clients about Red Team exercises that succeed in reaching their defined objectives, but they underwhelmingly failed to provide any value to the organisation. The reason for that is an exercise with little to no planning and tactics without strategy.

"Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat." The Art of War, Sun Tzu

To ensure that doesn't happen, we always kick-off Red Team exercises with a design phase.

The Art and Science of Adversary Simulation

During the design phase, we study the organisation's goals, their current environment (or how they perceive their current environment), where they want to go, and how they plan to get there. Then we analyse the data, identify critical factors, and devise an operational approach that will test their assumptions and challenge the plan.

The organisation will always strive to either change something for the better or maintain something that is considered good. When it comes to the organisation's security posture, our Red Team will endeavour to question whether:

- The target state is indeed better than the current state
- The plan, if successful, will lead to the target state
- The plan is achievable

At the end of the design phase, we formalise the Red Team's intent and then begin the detailed planning activities. We tailor every aspect of the execution plan to what we know about the environment to blend in and successfully negotiate the security controls that are in place.

Once we commence the execution of the plan, new information about the environment starts flowing. We process this information and adapt our approach and tradecraft accordingly. The plan always changes during execution.

"Plans are worthless, but planning is everything." President Dwight Eisenhower

When our operators execute the Red Team's plan, their mastery of the science of adversary tactics allows them to exploit and utilise available opportunities. They need to thoroughly understand their options when it comes to the different attack techniques that they can use in any given situation, and how to adapt their procedures or tools to fit the environment in which they operate.

Just like an artist can come up with a genius design but without mastering the science of the paint, brush, canvas, contrast, etc. the result will not be a masterpiece. Our operators must intimately understand operating systems, communications protocols, attack techniques and tools, human nature, business and IT processes, etc. We strive to seamlessly combine applicable elements of all these factors into every manoeuvre, and we always strive to create a masterpiece.

The Red Team employ Tactics, Techniques, and Procedures (TTPs) in their manoeuvres:

Tactics are short-term tactical goals that are executed during an attack, such as gaining an initial foothold or establishing a command and control channel with an implant.

Techniques are the means of achieving these tactical goals, such as establishing a command and control channel over an application layer protocol and using an encrypted channel.

Procedures are the detailed steps prescribing how to execute a technique.

Our operators apply the "offence in-depth" principle to the TTPs and maintain a high degree of "situational awareness", which allow them to make educated decisions while modifying procedures or choosing an alternative technique altogether in order to succeed.

A Multidimensional Mature Approach

Many different considerations affect a Red Team exercise:

- The level of sophistication of the simulated threat actor
- The range of TTPs employed by the Red Team
- Whether the operation is covert or fully coordinated with the Blue Team
- The amount of time and budget that is allocated to the operation
- The maturity level of the organisation
- The complexity of the defined objectives
- Whether a certain APT is emulated or a specific threat profile is defined

Our team of renowned experts will help you tailor the exercise to your budget in a way that will maximise the value you get out of it. We help to determine the objectives and approach, activities, and whether some elements of the attack chain should be "white-carded" (assumed breach) and the level of visibility the Blue Team should have.

In some cases, an assumed breach scenario is appropriate, in which the initial access vector is white-carded. This approach allows the exercise to focus on the post-exploitation phase of the attack and put more emphasis on detection and response.

sparke HELMORE LAWYERS

> A Red Team engagement consists of many little battles, some won, some lost, and that's when you start to appreciate what you do well, and what needs improvement. Importantly, the team at The Missing Link are incredibly skilled and 100% emotionally invested in the challenge. We know we will be tested, and we know that The Missing Link team will beat us several times along the way, and that's great – we learn, and we don't make the same mistake twice.
>
> A key benefit for us is it allows us to test the response of our other digital security vendors. It's almost impossible to validate the ROI for most of these products without subjecting them to very thorough testing.
>
> The Red team exercises are brilliant, the IT team love the experience, and it raises their level of engagement. We're really looking forward to the next exercise.

Hugo Evans | IT Security and Platforms Manager, Sparke Helmore

Red + Blue = Purple

When the organisation is keen to test the effectiveness of specific controls or assess their incident response capabilities, a purple teaming exercise is the best option. In such an exercise, the Red Team aligns with the blue team, providing them full visibility of the offensive activities. This helps the Blue Team to identify indicators of compromise in the environment, understand the impact of the Red Team's manoeuvres within the context of the attack chain, and devise a response to contain and eradicate the threat effectively.

Keep the Defenders on Their Toes

The Missing Link offers a Red Team as Service (RTaaS) subscription, which will keep the organisation's blue team engaged for an extended period to eliminate complacency. The Red Team will get to know the client's operational environment intimately, and be able to devise increasingly sophisticated attack chains over multiple operations.

This model allows the organisation to benefit from increased efficiency and measure their improvement in detecting and responding to incidents more frequently. Additionally, real adversaries remain in environments for months, or even years, and evolve their tradecraft with the evolving environment. The RTaaS subscription adds additional realism.

At The Missing Link, our dedicated team of operators work with organisations across industries to **tailor Red Team exercises** that will maximise the value and optimise the outcome for our clients.

A Renowned Adversary

We'll use a wide range of adversary tactics to simulate a real attack, demonstrate how real threat actors could breach your defences, and exercise the blue team's capability to detect and respond.

We recognise that Penetration Testing and Red Teaming require different sets of skills and expertise. Our Red Team operators are highly trained in the art and science of adversary tactics and are specially trained to design and execute Red Team operations.

Our Red Team will
test your technology, people and processes

Our Red Team conducts cutting-edge security research and development used throughout the industry, both in Australia and globally. Some of this original work is published on our research blog at Shenanigans Labs.

Ultimately, The Missing Link's Red Team will test your technology, people and processes to uncover any vulnerabilities, helping to ensure you have the level security you need.

If you are ready to challenge your security posture or take it to the next level, schedule a session with our experts to find out which option is right for you.

Contact Us

1300 865 865
sales-tml@themissinglink.com.au
themissinglink.com.au

themissinglink