

RED, PURPLE & BLUE TEAM TESTING:

Understanding the Difference, Purpose and When to Use Each Approach

This paper explores the differences between Red, Blue and Purple Team testing, how they complement traditional penetration testing, and how organisations can use them to build a more resilient security programme.

A CUSTOMER FOCUSED APPROACH TO PENTESTING

Whether it's a one off or 300 tests a year, you, the customer, are at the heart of our approach to pentesting. iSTORM® offer a fully managed service, real time reporting and a dedicated team of specialist testers so you can focus on the day job.

OUR MISSION IS SIMPLE

To combine the best possible customer experience, with market leading delivery for every client, every time.

Overview

It's no secret that data breaches are growing more sophisticated and extensive by the day, and cybersecurity testing has had to evolve significantly. Penetration testing is an important way to identify vulnerabilities and compliance gaps within your organisation's security posture, and many companies are adding to this by adopting a more practical approach. This is where Red, Blue and Purple Team testing can play an important role.

Although these terms are sometimes used interchangeably, they represent distinctly different approaches to testing an organisation's security. Each has a different objective, methodology and outcome.

Understanding these differences is important. Choosing the wrong type of exercise can mean spending significant time and resources testing the wrong thing, or identifying weaknesses without gaining a clear understanding of how effectively your organisation could detect, respond to and contain a real-world attack.



This paper explores the differences between Red, Blue and Purple Team testing, how they complement traditional penetration testing, and how organisations can use them to build a more resilient security programme.

1. At a Glance

Team	Primary Focus	Main Objective
 Red Team	Attack	Can we compromise the organisation?
 Blue Team	Defence	Can we detect, investigate and respond to an attack?
 Purple Team	Collaboration	Can we improve our ability to detect and stop an attack?

These are not necessarily competing approaches. In a mature security programme, they can form part of a continuous cycle of attack, detection, learning and improvement.

2. Testing Types



Red Team

A Red Team test takes the role of a real-world attacker.

Rather than simply looking for known vulnerabilities, a Red Team exercise attempts to replicate how a determined threat actor might target an organisation. The objective is generally to achieve a defined goal, such as gaining access to sensitive systems, obtaining access to privileged accounts, accessing sensitive information, or reaching a critical business asset.

Red Team engagements are typically team-based exercises and can involve multiple testers working across different areas of an organisation's security. Depending on the objectives, scope and complexity of the engagement, testing can take place over an extended period rather than within a traditional short penetration testing window.

A Red Team may use a combination of technical vulnerabilities, misconfigurations, phishing emails, exposed services, social engineering, credential attacks, physical access testing and other techniques within the agreed rules of engagement.

The important distinction is that the focus is not simply on finding vulnerabilities. Red Team testing can demonstrate how individual weaknesses can be chained together to create a much larger security risk. A vulnerability that appears relatively minor when viewed independently can become significant when combined with other weaknesses.

Red Teaming is not just about finding weaknesses; it is about understanding what an attacker could do with them.



Blue Team

The Blue Team represents the organisation's defensive capability.

While the Red Team attempts to compromise the organisation, the Blue Team is responsible for detecting, investigating and responding to threats.

Blue Team testing focuses on the organisation's ability to:

Detect → Investigate → Respond → Contain → Recover

Blue teams are responsible for standard security tasks like checking security alerts, deploying patches and fixing vulnerabilities, and reporting to company stakeholders and executives.

Red teaming exercises provide vulnerabilities for the blue team, however the most valuable knowledge is what techniques were detected, which were missed, and specifically why the missed techniques were not surfaced by existing detections.



Purple Team

Purple Teaming brings the Red and Blue Teams together.

Rather than a specific team, Purple Team testing is a collaborative exercise format which brings together offensive and defensive practices.

Rather than keeping the attacking and defensive functions separate, Purple Team exercises encourage collaboration and real-time learning. The Red Team demonstrates an attack technique. The Blue Team attempts to detect it. Purple teaming then takes the learning based on the findings from the red team and makes recommendations based on insights gained during the testing process.

The process can be repeated after changes have been made, allowing organisations to validate whether their improvements have had the desired effect. This makes Purple Teaming particularly useful for organisations looking to continuously improve their detection, response and overall defensive capability.

3. Red vs Blue vs Purple

The key difference between each team is the intended outcome.

Red Team demonstrates what a realistic attacker could achieve and how they could potentially reach a defined objective.

Blue Team demonstrates how effectively an organisation can detect, investigate and respond to malicious activity.

Purple Team brings offensive and defensive perspectives together to identify gaps, share knowledge and improve security capabilities.

One of the most important considerations when planning any security testing exercise is understanding what you are trying to achieve. The organisation should first define the question it wants answered, then objective should then drive the methodology.

4. How Do They Differ from Traditional Penetration Tests?

A traditional penetration test usually focuses on identifying and validating vulnerabilities within a defined scope. The objective is generally to identify vulnerabilities and provide evidence of their impact, allowing the organisation to remediate them.

A Red Team exercise goes further by considering the attack path. This is objective based compared to a penetration test which is defined by a scope. A penetration test is limited to a scope, however Red Teaming is about achieving a goal, and the path to get there remains undefined. So instead of asking: "Is this system vulnerable?" the question becomes: "could an attacker use this weakness to achieve a meaningful objective?"

Purple Teaming takes this further again by asking: "Could we detect this attack, and if not, how can we improve our ability to do so?" These approaches therefore answer different questions and provide different types of insight.

5. When Should You Use Each Approach

There is no single testing approach that is appropriate for every organisation. The right choice depends on the organisation's objectives, threat profile and existing security controls.

Penetration Testing

Penetration testing can be appropriate when an organisation needs to:

- 🔗 Identify vulnerabilities and validate security controls
- 🔗 Meet compliance requirements
- 🔗 Test a new application or infrastructure
- 🔗 Assess a specific technology
- 🔗 Understand the security of a defined environment

It is often the foundation of a broader security testing programme and can support both compliance requirements and security best practice.

Red Team

Red Teaming may be appropriate when an organisation wants to:

- 🔗 Test its resilience against a realistic attack
- 🔗 Understand attack paths to critical assets
- 🔗 Test preventative security controls and assess effectiveness of security architecture
- 🔗 Evaluate exposure to realistic threats
- 🔗 Test whether an attacker could achieve a specific business objective

Red Team exercises are particularly valuable for organisations with established security controls that wants to test how its defences perform under realistic conditions.

Blue Team

Blue Team exercises can be useful when an organisation wants to understand:

- 🔗 Whether attacks are being detected and whether security alerts are meaningful
- 🔗 Whether monitoring provides sufficient visibility
- 🔗 How effectively incidents are investigated
- 🔗 How quickly the organisation can respond
- 🔗 Whether incident response procedures work in practice

This approach can help organisations identify gaps in their defensive capability and improve their ability to detect and respond to threats.

Purple Team

Purple Teaming can be particularly valuable when the organisation wants to actively improve its defensive capability. It can help organisations

- 🔗 Improve detection rules and identify monitoring gaps
- 🔗 Validate security controls and improve incident response
- 🔗 Test security tooling
- 🔗 Develop threat detection use cases
- 🔗 Measure progress over time

The collaborative nature means that lessons can be shared between offensive and defensive teams rather than remaining isolated within separate security functions.

6. Choosing The Right Approach

The terminology can sometimes make security testing appear more complicated than it needs to be. The important question is:

What do you need to learn about your security?

If you need to understand your vulnerabilities, a penetration test may be appropriate. If you need to understand how far a realistic attacker could get, consider Red Teaming. If you want your offensive and defensive teams to work together to improve detection and response, Purple Teaming can provide a valuable framework.

For many organisations, the most effective security programme will use a combination of approaches over time.

Conclusion

Cyber security testing is no longer simply about finding vulnerabilities.

Modern organisations need to understand not only where they are vulnerable, but also how those vulnerabilities could be exploited, whether an attack would be detected and how effectively the organisation could respond.

Penetration Testing, Red Teaming, Blue Teaming and Purple Teaming each provide a different perspective.

Used appropriately, these approaches can provide organisations with a much clearer picture of their real-world security resilience.

Ultimately, the goal isn't simply to prove that an organisation can be attacked. It is to understand what could happen, learn from it and make the organisation harder to compromise next time.

**Better insights. Stronger defences.
More resilience.**

iSTORM's approach

At iSTORM, we believe security testing should be about more than producing a report.

Our approach combines technical expertise with a focus on understanding the organisation, its objectives and the risks that matter to its business.

From penetration testing and vulnerability assessments through to more advanced attack simulation and security consultancy, we work with organisations to identify weaknesses, understand their impact and support meaningful remediation.

Want to understand where your organisation is exposed?

iSTORM can help you assess, validate and prioritise your security risks through CREST-accredited penetration testing, Red and Purple Teaming and expert security consultancy.

Talk to the iSTORM team to find out how we can support you.

Contact us directly:

info@istormsolutions.co.uk or call +44 (0) 1789 608708

