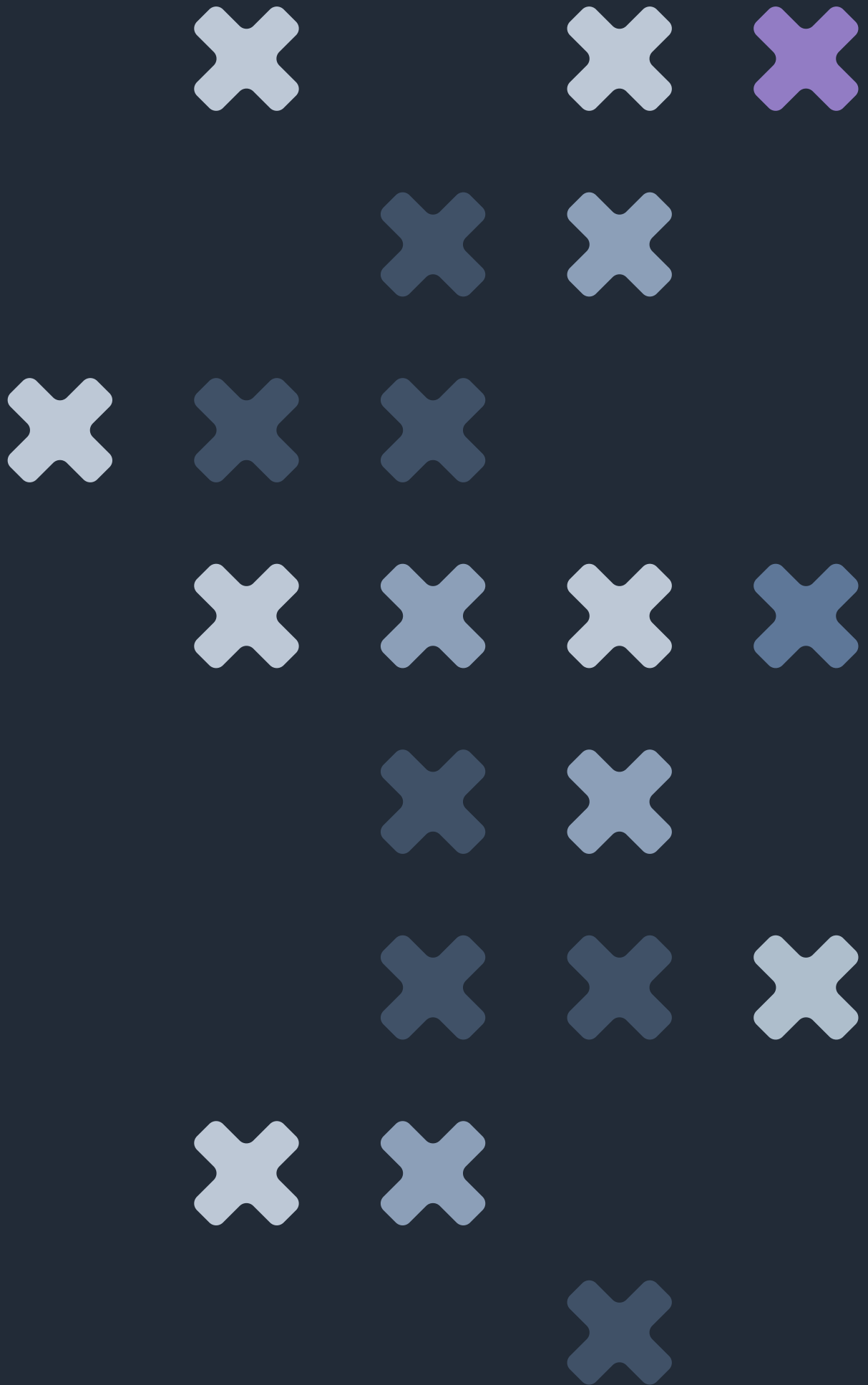




THOUGHT LEADERSHIP

# The CISO's Guide to Powerful Purple Teaming



# Introduction


You have likely seen the way that most common penetration tests go, a business wants to assess their security posture, or maybe even the effectiveness of their defensive teams, so they engage the services of a team of penetration testers. Inevitably some issues are found, a report is generated and the offensive team leaves. This can lead to a situation where the exercise has been completed, the 'box ticked' but the teams struggle to translate technical findings into business impact.

This very common engagement flow is an artefact of the way the industry has worked since its inception. Blue teamers, the defensive teams, are well-versed in defence and the tools available to protect their organisation. Similarly red teamers, the offensive teams, will have a range of expertise in penetrating difficult systems.

The problem is as simple as that. Red and blue teams operate on opposite ends of the cyber security spectrum, and the relationship between the two is often adversarial.

Experts in defence are unlikely to have the offensive skillset or even mindset of a hostile attacker looking for every opportunity to find a way into a network. And while an experienced offensive team member may have knowledge of how defensive technologies work, they often lack the deep understanding of the defenders. For the business to be more secure the flaws identified by offensive experts must be mitigated by the defensive team, and thoroughly. This understanding gap can lead to issues being identified but not truly remediating business risk. If only they understood each other better!

The aim of this e-book is to not only show you there is, potentially, a better way to carry out these engagements, but to also give you some tips to help implement a purple team strategy, increase the awareness of any gaps in your current stance and show how the implementation of purple teaming could benefit your business, potentially saving millions in lost revenue due to cyber-attacks.



**The implementation of purple teaming could benefit your business, potentially saving millions in lost revenue due to cyber-attacks.**

# The current state of things

All too often the relationship between red and blue is adversarial, although this is merely a symptom, not the issue itself. To really get to the heart of what is wrong with this relationship it's important to look at, and recognise, the problems with how things are typically organised and incentivised.

One of the biggest issues is that red and blue teams often operate in a vacuum, with the only feedback loop between the two teams being the report generated at the end of the engagement, assuming the blue team ever see the report at all.

Another problem is that both teams are incentivised to outwit the "other side". For the red team, a long report with numerous findings is seen as a job well done, with success often being measured by how many controls the team managed to bypass during the engagement. Meanwhile on the blue team, they're hoping for a report with

few findings, and a lack of alerts during the engagement can be taken to mean all preventative controls worked.

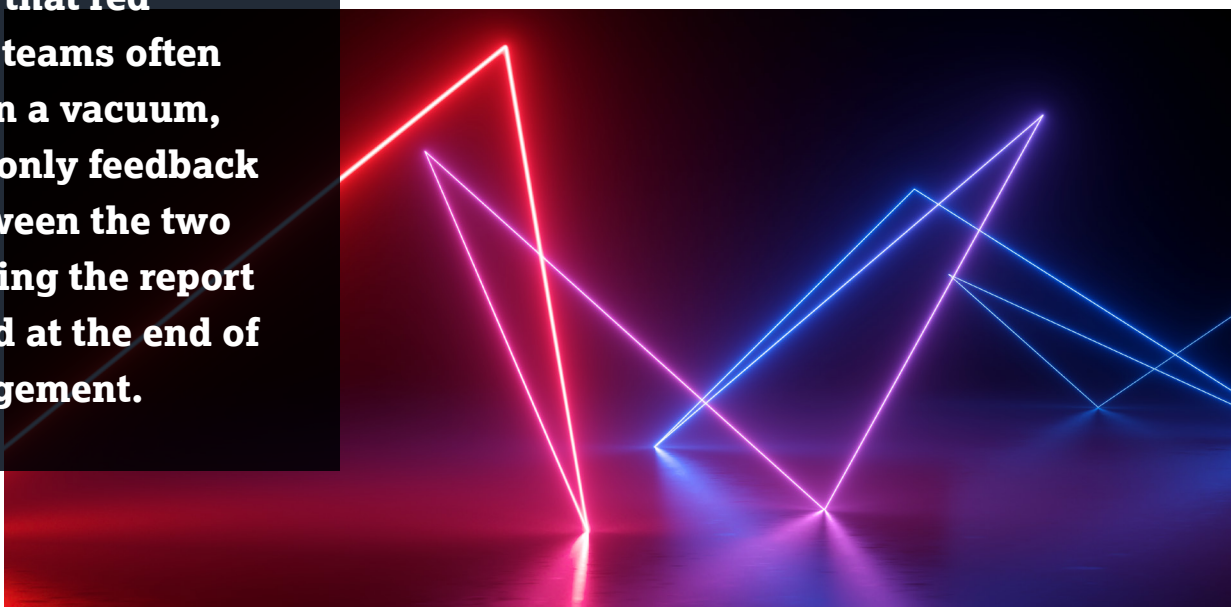
In organisations which regularly conduct security assessments and offensive exercises, another significant problem can develop. The red team often win by virtue of the classic defender vs attacker asymmetry; attackers have to find one flaw in a huge surface area, once. Defenders must protect comprehensively everywhere, all the time. This can lead to offensive exercises where the red team grow stale and do not learn from the times the blue team detected them. A feedback loop benefits not just the blue team in remediation but sharpens the tactics of the red team also.

The last big issue is that in a typical engagement more emphasis is given to the remediation of vulnerabilities rather than the development of prevention and detection tools or techniques.

Addressing these issues is key to unlocking the full potential of both the red and blue teams within your organisation.



**One of the biggest issues is that red and blue teams often operate in a vacuum, with the only feedback loop between the two teams being the report generated at the end of the engagement.**



# Enter the Purple team

On the surface, red and blue may appear to be adversaries, and often they are set up to fall into that way of working, but in reality, they should be working together to better prepare against the real adversaries. The true goal of the red team is to get to find flaws and emulate adversaries so that they can show “how the bank would be robbed” before the criminals do it. If their work is not representative of what attackers will do it has little value. If the flaws are found and not addressed so the criminals wander in and rob the bank nonetheless, they were only a cost with no positive impact.

The red and blue team need each other to keep each other honest and to enable them to have the desired business impact. We need to change the way we view the teams if we are ever to improve, red and blue shouldn't be viewed as opposing swords; but instead, a sword and a whetstone, with one working to improve the other.

It is a simple fact that in any engagement, the red team should be working with the blue team to make blue better. Any time the red team fails to do so is a waste of time and money.

The purple team is currently the best and most proven answer to this problem. Whilst the term has been used for a while now, many businesses have yet to adopt it, despite its transformative impact on security teams' value. Purple teaming, in its simplest form just means that we should be creating cross-functional teams consisting of both red and blue, with the goal being to facilitate communication and collaboration between the two teams.

They are no longer adversarial but working in partnership to a common goal, while getting to do the work where their expertise lies.

It's important to note that the solution is not to create a new team to carry out purple team engagements, but to instead fix the interaction dynamic between the red and blue teams. The blue team should be allowed to see how things such as exploitation of vulnerabilities and pivoting through a network work, and similarly the red team should see how monitoring alerts, and the response to them works.

This has the effect of increasing the capabilities of both teams, over time the red team will begin to understand what is being monitored and alerted on and start to think what would happen if another vector was used instead. Similarly, as the blue team see how attacks are carried out, they start to predict red team actions and provide preventative rather than responsive measures, increasing the security of the organisation. In our experience of running purple team engagements to teach teams how to start working together, we have found they also come up with new creative protection and control strategies they would not have on their own and enjoy the exercise of doing so.



## Running Purple team exercises

Setting up and running effective purple team exercises takes time and dedication from both teams involved and the organisation itself. It is not a quick fix, but the results speak for themselves. What follows is a rough roadmap for the creation of a true purple team, though it should be tailored to your organisation's team size, maturity, and risk goals.

Initially the red and blue teams should be introduced (pizza can be helpful), and the goal clearly communicated, the red team should walk through common attack techniques they deploy during tests and blue should do the same for protection mechanisms in place. The teams should work together to identify any gaps, and time should be given to implement any needed changes. If you reach a point where the teams are "politely but passionately arguing" over whether they would have succeeded or stopped a specific attack, you are on the right track!

Once any changes have been made, the red team can begin to carry out exercises in collaboration with blue. The engagement plan should ideally be drawn up in advance to test specific controls or to emulate a particular attacker, and as attacks are launched or tools used the team should be checking-in to determine if it was detected. Clear communication in both directions is key to the success of this phase. After this first engagement has been carried out, the results should be discussed and any areas for improvement for both red and blue should be identified before running another.

As time passes and more engagements are carried out, the detection and response capabilities of the blue team will improve, as will the understanding of the red team. This will naturally lead to the techniques and tools deployed by both red and blue becoming more advanced. Once you reach this stage every testing cycle will improve the overall security stance of the organisation.

Depending on the nature of your organization and your risk profile, purple teams can conduct specific adversary modelling exercises. You can take known tactics of specific gangs, such as those provided by the [MITRE Att&ck](#) and have the red and blue teamwork through a known scenario of attack to understand how they would sharpen their attack and defence tactics respectively. This can assure the business of the ability to deal with a difficult attacker, but also teach both teams tactics and techniques they would not normally think to use.



**In our experience these exercises can be one of the most powerful tools in developing security capability and reducing risk.**



# The process



## Scoping and planning meeting to set target:

- Is the plan to emulate a specific threat actor?
- What is the end point – time limit or specific objective?
- Communication methods and approach between red and blue established



### Days 2-6

- Red takes an action
- Blue responds
- Red and blue discuss action
- Repeat

## Evaluation Phase:

- Couple of days reviewing notes and what happened:
- What worked, what didn't? What can be tweaked?
- You, or your tools, didn't catch it because...

### Days 8-9:

- Make the tweaks
- Run the exercise again to validate fixes fixed the issues and to identify more weaknesses
- Continue until red team can't win

## Planning and scoping for next engagement

# Outside help

Often an organisation will want to set up purple team exercises but either doesn't have an in-house red team or does have a team but communication between red and blue needs to be developed. This is one of the areas where purple team development can go very wrong, but also a powerful tool in getting it right!

The default setup of these teams is often adversarial, and in many cases a significant portion of the red team are external resources to the business which can weaken the relationship further. Some organisations try to throw together the teams with a common goal, without a 'ringleader' that has conducted the activity before. Without the right supervision and experience this can lead to blame, criticism or an unbalanced activity that does not focus on better prevention and detection. Using a third party to assure the successful development of the purple team (or development of a purple team maturity roadmap) can be critical to a positive exercise.

When engaging outside help you need to pick a way for them to engage the teams, and the two most common and effective models are:

**Third party acts as interface between red and blue** – This method is used to teach organisations, and their teams, how to carry out effective purple team exercises. The third-party acts as a facilitator for the two teams, helping to develop test cases and build communication between the teams.

**Third party acts as red team, with constant contact** – This method is used when the organisation does not have an in-house red team. It is also commonly used for repeated testing of a protection or detection method. The red team takes an action repeatedly and blue tunes their defences, whether that may be prevention or detection of the action.

It allows red to take and emulate a certain attack method and for blue to immediately look at their defence and detection capability, adjusting it accordingly to reduce noise, increase the quality of alerts, or stop the attack all together.



**Using a third party to assure the successful development of the purple team can be critical to a positive exercise.**





# Top 5 tips

## 1. Understand your cyber security maturity – Are you ready?

It's important to make sure that you're ready before starting down the path toward purple teaming. Make sure that your blue team and their tools and techniques are well established. If the team do not have standard processes for dealing with alerts, or your toolset is not configured to a reasonable baseline then it's unlikely you'll see the best results from running a purple team exercise. Work to mature these practices before you start matters, or the team will simply feel like they failed. You may want to get an expert reviewer to validate your readiness before you begin.

## 2. Create a plan

Your purple team's strategy should reflect the threats that your organisation faces. Ensure that the tools, techniques, and practices of those likely to target you are covered in the exercises. If you are not likely to be the victim of a nation-state attack, then you should model more run of the mill ransomware or web application attacks. As your team matures, they can experiment with more esoteric risks to learn, but start with the likely and high impact.

## 3. Maximise the opportunity as a learning experience.

Remember that purple teaming should not be adversarial, the goal is for all participants to learn how the other team acts and understand how that impacts the work that they do. It should be encouraged that all members of the team absorb and reflect the results of any exercises. Make the time for the team to reflect together and then make the time for both teams to apply findings. Running an exercise, declaring the need for a set of changes and then returning to work (leaving those changes on a nice document somewhere) does not reduce risk.

## 4. Measure the growth of both teams, not just blue

As your purple team carries out more exercises, the effectiveness of both the red and blue components will increase. It's important to ensure that you're measuring improvement across both teams and using the results of engagements to identify any training needs within each team. This is not just about testing blue; this is about both teams growing better together and reducing business risk. Shared metrics measure shared goals.

## 5. Consider external help where needed

There are a number of places where this can add value, but it should be used at the right time and in the right way to avoid needless expense. Occasionally supplementing your red team with external testers will help keep the team fresh with new ideas, and the blue team challenged.

Leveraging experts to run your purple team engagements will keep them positive, and make sure the right learning outcomes are achieved. Expert defenders can also be used to review blue team implementation plans to make the exercises more teachable. The focus of these external resources should always be to train on the job and make the in-house team that will be left there to deal with attacks better, or you aren't really purple teaming – just consulting!



# Next steps

We have helped many organisations improve their security teams and hope that the learnings we have shared herein help you develop a purple team roadmap that significantly strengthens your position against attackers. In our experience these exercises can be one of the most powerful tools in developing security capability and reducing risk, but in a cost effective and positive way for your team. We would also underline the importance of setting out on the journey the right way.

Our team are world-class consultants who can help you decide firstly, if purple teaming is indeed right for you at your current stage. If you need to further develop your blue or red teams before you can engage in purple teaming, we can also help you develop a capability enhancement roadmap.

**Get in touch with our team at [hello@secure-impact.com](mailto:hello@secure-impact.com)**

If you'd like to discuss how purple teaming could benefit your organisation and you believe an external partner could help, do reach out to a cyber security consultancy such as Secure Impact to learn more.



**Giorgia Cacace**  
General Manager



**Tom Fawcus Gibbs**  
VP of Technology



# About us

Secure Impact offers enhanced cyber security consulting services, combining superior technical expertise and an innovative, client-centric approach.

We offer the following offensive and defensive services, and bespoke consultancy aimed at executive-level engagement:



## SI OFFENSIVE

- Penetration testing
- Red team assessment Purple team assessment
- Security assessment
- Cyber due diligence



## SI DEFENSIVE

- Digital forensics
- Incident response planning
- Digital footprint service Blue team assessments



## SI CONSULTING

- CISO for a day
- Simulated incidents
- Tabletop exercises
- Cyber drills
- Bespoke consultancy

**We'll get to know the unique challenges you face before adding our expertise to provide solutions and technologies that will improve your overall security posture, both against threats you may face today, and will face in the future.**

# SECURE IMPACT

Your security team.



## Your security team.

We understand you have real business challenges which likely won't be solved with commoditised scans, tick box exercises or generic reports. Our GIAC-certified team can help create real business outcomes for you and your team through collaborative offensive and defensive engagements.

From penetration testing to defensive and consulting services, we promise engagements which are business-oriented, bespoke to your risk profile, and geared to achieving your security objectives.

We partner with CISOs and security teams from the FTSE 100 to VC-backed scale-ups, creating shared learning outcomes for our clients, and developing a roadmap to improve their cyber security maturity.

### Secure Impact Ltd.

The Old Bull Pens, Sezincote, Moreton-In-Marsh, Gloucestershire, GL56 9AW

© 2022 Secure Impact.

**Want to discuss how we can help your  
business?  
Contact us to learn more.**