Purple Team: drive defense with offense

Purple team exercises are a fast way to improve your security monitoring function. By combining defense and offense in purple team exercises you can measurably improve your security monitoring function faster and less expensively than segregating both functions.

Jacqueline Morrison
is Senior Consultant at KPMG Netherlands.
morrison.jacqueline@kpmg.nl

Jordi van den Breekel
is Manager at KPMG Netherlands.
vandenbreekel.jordi@kpmg.nl

INTRODUCTION

Building an effective security monitoring function is a challenge. The attack surface is becoming more and more complex to manage, understand and even be aware of. However, an effective security monitoring function can be improved faster by utilizing purple team exercises.

Organizations today want to see immediate value as well as longer term strategies and solutions. The type of collaboration described in this article will allow you to see both immediate results and long-term improvements come to fruition, maximizing the value of the internal or external services you pay for.

Whether you have internal teams or utilise external resources for offense and defense functions, if you are not performing any form of purple team exercises it is highly likely you are not getting the most value out of the expertise you are paying for. Want to bolster your security monitoring function fast? Then start with purple team exercises.

WHAT ARE RED, BLUE AND PURPLE TEAMS?

First some background on blue and red teams. The terminology originates from military terms for defense (blue) and offense (red). A blue team in the context of cyber security is responsible for defending against cyberattacks and improving security posture within an organization. This includes implementing preventative and detection controls and responding to security incidents and alerts. This function can be internal, outsourced to a third party, or a hybrid of both.

A red team performs activities to emulate an attacker's behavior during red team exercises. The purpose of a red team exercise is to simulate a realistic attack based on the known techniques of threat actors. The timing and goal of the exercise are not shared with the blue team, to make the simulation more realistic. These exercises are usually performed annually, can take several months to complete, and can be performed by an internal or external team to the organization (some organizations also have a regulatory requirement to complete an external red team exercise).

It is only after the red teaming exercise has finished and the cyberattack simulations have been completed, that the red and blue teams start interacting with each other. Then both teams typically discuss how they experienced the attack simulation, where the blue team will indicate which indicators of compromise they have found, and the red team will provide a detailed story line of all actions performed. Often, the red and blue teams have different reporting structures due to both teams being segregated either internally or with one function being external. This way of working could increase a feeling of competitiveness that moves away from the end goal both teams share – strengthening the security posture of the organization.

To remove the feeling of competitiveness and focus optimally on strengthening the security posture of the organization, you could consider performing a purple teaming exercise instead. A purple team brings the traditionally segregated red and blue teams together for an exercise where they work together.

The format can vary from sitting in a room together and going through attack behaviors, to a red team conducting an exercise with the awareness of the blue team and a red team representative helping and giving tips to the blue team. They are ideally conducted reg-

Figure 1. Combining the strengths of red and blue teams to form a purple team.

	Blue Team	Red Team	Purple Teaming	Penetration Testing
Goal	Detect and mitigate cyber attacks	Test resilience against real attacks	Improve security posture	Gain oversight of vulnerabilities
Scope	Entire organization	Entire organization	Predetermined systems & employees	Predefined system(s)
Test method	N/A	Realistic simulation	Efficient improvement of security posture	Efficient identification of vulnerabilities
Used tools	Security tooling such as Endpoint Detection & Response (EDR) and Security Information & Event Management (SIEM)	Sophisticated tools to remain undetected	Sophisticated tools to remain undetected & detection software	Efficient penetration testing tools (e.g. mass scanning)
Tested controls	N/A	Focus on detective and responsive controls	Focus on detective and preventive controls	Focus on preventive controls
Positioning	Continuous, often 24/7	Periodically	Periodically	Part of development lifecycle

Table 1. An overview of the characteristics of red teaming, purple teaming, and penetration testing.

ularly (once a quarter or every six months) to ensure continuous improvement and to ensure changes to the environment are considered. Collaborating enhances shared learning and maximizes the effectiveness on both sides. For organizations who are not required to carry out a red team exercise or who have a low security monitoring maturity level, purple team exercises can be a standalone option to gain immediate value and long-term action plans.

Another common method to improve the security posture is penetration testing. This is something most organizations already are familiar with. It is an essential part of vulnerability management and thus essential to the security of an organization. However, penetration testing is completely different from red vs blue teaming and purple teaming. Penetration testing focusses on finding as many vulnerabilities as efficiently as possible. Typically, this includes the use of very noisy tools, such as mass vulnerability scanners. Remaining undetected is not taken into account during penetration testing, and the focus is purely on the preventive measures. Unfortunately, penetration testing and red, blue and purple teaming are regularly confused with each other, while each serves a very different purpose. Red vs. blue teaming and purple teaming do not focus on finding as many vulnerabilities as possible, penetration testing therefore remains an essential part of the security program, even when organizations have incorporated mature red vs. blue teaming and purple teaming exercises. The characteristics of each of these methods are shown in Table 1.

CHALLENGES

Many organizations lack the internal resources to holistically implement defensive and preventative controls to adequately and robustly respond to the results of red team exercises. The result is oftentimes that the next time a red team exercise is repeated, many of the same or similar findings persist. Some of the challenges we have seen repeatedly at organizations in different industries and sizes are described below, along with the benefits of working together.

Resource and skill constraints

The blue team is traditionally a much-stretched resource and firefighting is commonplace. Ensuring you respond to incidents and alerts in an appropriate timeframe, as well as implementing new use cases, writing and updating playbooks, implementing or championing new preventative controls among many other tasks can be overwhelming. Even in organizations where the budget exists to have separate teams for some of these functions, the skillsets for this type of work are scarce worldwide with an estimated 3.5 million unfulfilled cybersecurity jobs by 2021 according to Cyber Security Ventures ([Morg19]). Onboarding the relevant log sources and adhering to organizational change procedures for implementation can also severely limit the blue team's ability to respond adequately, and often results in quick fixes and priorities focused on what is possible, rather than what should be prioritized.

In a purple team scenario, efforts are focused with precision on the task at hand. The red team is also able to help the blue team prioritize the selection of use cases and even the vulnerabilities or preventative controls to focus on first, based on their experience.

Limited understanding of red team findings

A static report from a red team exercise needs to be interpreted and this can lead to misunderstandings or

assumptions. This could lead the blue team to implement inadequate controls to resolve the identified issue.

When the teams are sitting side by side, it is more interactive. Everything is shared with the blue team at the level required to identify exactly what needs to be accomplished to adequately respond to the finding from the red team.

Unable to test controls implemented

It can be difficult to recreate attack patterns to test implemented controls because the blue team may not have the required skills to do so. The blue team may not have permission to do this on live systems, and the simulators may not be adequate to test everything. This is because they only cover specific behaviors that may not exactly match what was tested in the red team exercise and they may need to be adapted to the environment. Without the ability to simulate the behavior to recreate logs it stunts the blue team's ability to test strengthened defenses and ensure they are adequate. Scarce resources can be an additional hindrance to ensure that new controls are effectively tested both initially and on an ongoing basis, which is also critical.

With the red team working together with the blue team in a purple team exercise, this issue is resolved. As soon as an additional control is implemented the exact same behavior (patterns) can be emulated again, and as many times as needed, until the control adequately prevents or detects it. With regular purple team exercises you can retest your current controls to ensure they still function as expected. Combining the two functions in these purple team exercises also assists with the resource issue, because while they will learn more about it, the blue team does not need to learn the skills and takes the time to recreate attack behaviors themselves.

Tunnel vision

The risk exists that quick fixes are implemented but a holistic approach is not applied. For example, a use case can be built to detect a particular behavior, but was a preventive control also considered? Creating use cases based on single indicators of compromise (IoCs) is common and often not effective in the longer term. This can be due to lack of time to properly consider a solution, lack of skillset and lack of understanding of how an attacker works. It could also be that due to the organizational structure, the SOC (Security Operations Centre) does not have the mandate necessary to change processes or make an organizational change, and so instead does what it can with what is available to it. Quick and dirty solutions are therefore sometimes implemented, which will not sufficiently cover the behavior of the red team or attacker if slightly modified.

The red team can articulate and demonstrate why implementing a tunnel vision control is less valuable. Working together promotes a better understanding of how attacks work, and how they can best be prevented or detected.

Visibility of red team footprints

When the red team report is issued, the first thing the blue team wants to do is to look at each scenario and determine where preventative and detective measures were insufficient, and which measures could be put in place based on feedback. Most often you need to look at any footprints generated by the activity of the red team in your environment to formulate a plan on how to prevent or detect the activity. However, these may no longer be available once the report actually reaches the blue team. Red team exercises are not interactive while being conducted and a report is issued after the exercise. Event logs will usually have already rolled off, and even if you had the logs you are required going to your SIEM (Security Information and Events Manager), retention periods can often be short and therefore no longer available.

Working side by side together at the same time resolves this issue entirely.

Success is incorrectly measured

When the two functions work independently, it can foster a culture of competitiveness. This does not encourage a mentality of working together and instead feeds a rivalry between the two teams. Both teams can potentially be reluctant to share their techniques with each other, to ensure they "win" next time. What does this mean? Potentially the expertise paid for is not being leveraged in the most efficient way.

The end goal and incentive for both teams must be how much they have strengthened the security posture of the organization. Make this measurable. For example, use MITRE's ATT&CK framework ([MITR19]) and create a heat map to show the strength of your techniques used by threat actors targeting your industry. Once the purple team exercise is complete, update the heat map to demonstrate improvements. In addition, leverage a use case framework such as MaGMa ([Os17]) which will calculate a percentage of detection coverage which can then be used to measure improvements of detection mechanisms.

Penetration testing and red, blue and purple teaming are regularly confused, while each serves a very different purpose

HOW TO GET STARTED – UTILIZING PURPLE TEAMING ON YOUR TRANSFORMATION JOURNEY

Many organizations are adopting more "Agile" ways of working, and as such have a desire to see immediate results and benefits. This method focusses on immediate and clear value as well as actionable implementation plans at each stage of the transformative process.

Who should be part of a purple team?

To get the most value out of these – usually – time-boxed exercises, you should ensure that representatives from each aspect of the blue team are involved; including incident response, security tooling engineering, network engineers and vulnerability management. You will also need representatives from the IT operations team, i.e. Windows/Active Directory teams, or at the very least they should be aware of the exercise and be able to make changes as needed. Furthermore, make sure that other stakeholders such as decision makers, change management and risk departments are aware and support the purple teaming exercise. This can help to get things implemented during the actual exercise and allow changes to be expedited if required. Generally, it will be a more blue team exercise due to the workload for the blue team generated by the red team.

Working together

A purple team exercise is a joint mission between the red and blue team to improve the security monitoring function of the company through direct collaboration. The format of a purple team exercise can vary. One very effective format is both the red and blue team sitting together in the same room and going through attack behaviors (this can be based on many scenarios, for example threat intelligence based, a previous red team exercise or replaying an actual attack the organization experienced in the past). Once the red team completes an action, the blue team checks if it detected or prevented it. If not, together they work out why, and either fix the issue on the spot and retest or work out an actionable plan to implement the required controls. This method offers direct collaboration.

What to focus on

The most effective areas to focus on are post-exploitation activities. Assume breach and identify the attacker's actions in your environment. It generally takes too long to focus on initial access in a purple team format, which includes crafting phishing emails or doing extensive reconnaissance on the external network to identify exploitable vulnerabilities.

There should be some level of research completed up front by the purple team, so that the exercise is based on threat-based intelligence specific to your industry.

The red team will work through the selected attack scenario, at each stage of the simulated attack stopping to ask the blue team "Did you see that?" If the answer is no, then they work together to identify why. Are the logs on-boarded, is there a detection control in place, and so on? The same part of an attack can be replayed to test new controls, and also performed in different ways to ensure the detection or prevention mechanism is wide enough to catch slightly modified behavior but also maintains an acceptable false-positive: false-negative ratio.

The focus should be on continuous improvement rather than a one-time exercise. Some examples of themes for purple team exercises are as follows:

- Emulation of a real attack experienced by the organization
- Walk through of past red team exercise
- A tiered exercise, getting more complex with each iteration
  - Tier 1 – Noisy e.g. Common tooling, Brute force, Scanning
  - Tier 2 – More evasive tactics e.g. in memory, privilege escalation
  - Tier 3 – Stealthy: Red team compiling own tools
- Cloud environment (AWS, Azure, etc.)
- Test of existing security monitoring detection and preventive controls to determine effectiveness

Measuring success

At the end of the exercise you should be able to measure how your security posture has improved, and also have a plan with actionable items to resolve any issues that prevented implementation during the exercise. As already discussed, having a well-maintained use case framework that maps back to MITRE's ATT&CK framework ([MITR19]) or a heat map of MITRE's ATT&CK framework is a good start to measure before and after to demonstrate improvement to management. An example of how such a heat map can look like is shown in Table 2.

It is recommended to repeat the exercise, ideally on a quarterly basis, to maintain momentum, ensure continued improvement and keep up with the constant changes happening in your environment and threat actors.

Our security monitoring maturity level is low, can we benefit from purple teaming?

If you are still building up your security monitoring function and closing detection and prevention gaps, purple team exercises can be very helpful. For example you can start by having the red team show you the most realistic path to your crown jewels and focus on remediating those gaps. Or you can begin emulating behaviors that create more noise and are easy to detect. The quickest way to improving your maturity level is working closely together with the red team.

Table 2. Example to measure security posture based on MITRE ATT&CK framework (green actions are fully detectable by the blue team, orange actions are detectable under certain circumstances, and red actions are not detectable).

Before purple teaming		
Execution	**Persistence**	**Lateral Movement**
Hardware additions	AppCert DLLs	Logon scripts
Valid accounts	Logon Scripts	Pass the ticket
Supply chain compromise	Application shimming	Remote file copy
		Remote services

After purple teaming		
Execution	**Persistence**	**Lateral Movement**
Hardware additions	AppCert DLLs	Logon scripts
Valid accounts	Logon Scripts	Pass the ticket
Supply chain compromise	Application shimming	Remote file copy
		Remote services

IS THERE STILL VALUE IN A RED TEAM EXERCISE WHEN CONDUCTING REGULAR PURPLE TEAM EXERCISES?

The answer is yes. The goal of a red team exercise is to give a true indication of how your defenses hold up against an attack with no prior warning. While a purple team exercise is not intended as a replacement to traditional red team exercises, it complements them as an extension of this, either in combination with (pre or post red team exercise) or even independently if you do not conduct red team exercises.

CONCLUSION

Purple teaming is a very powerful method to improve the security posture of an organization. It promotes collaboration between red and blue teams and increases the learning experience of both teams and of the organization being tested. It is a natural next step when an organization has incorporated vulnerability management processes and wants to simultaneously measure and improve the capability to detect cyber incidents and attacks. Purple teaming is a very worthwhile addition to identifying vulnerabilities (by penetration testing) and to measuring responsive capabilities (by red teaming). Whatever your budget and maturity level may be, you can benefit from leveraging purple team exercises to complement the existing red and blue aspects of your security monitoring function. Both offense and defense have the same end goal – to strengthen the security posture of the organization. So … why aren't blue and red working together more?

Offense and defense have the same goal to strengthen the organization's security posture

References

[MITR19] MITRE (2019). Enterprise Matrix. Retrieved from: https://attack.mitre.org/matrices/enterprise/

[Morg19] Morgan, S. (2019). Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021. *Cyber Security Ventures*. Retrieved from: https://cybersecurityventures.com/jobs/

[Os17] Os, R. van, et al. (2017). MaGMa: Use Case Framework. FI-ISAC. Retrieved from: https://www.betaalvereniging.nl/wp-content/uploads/FI-ISAC-Use-Case-Framework-Full-Documentation.pdf

About the authors

Jacqueline Morrison is Senior Consultant at KPMG Netherlands with over 10 years of experience in cyber defense.

Jordi van den Breekel is Manager and the Red Team Lead at KPMG Netherlands.