SNAPATTACK

eBook

Strengthening Security through Collaboration: A Guide to Purple Teaming

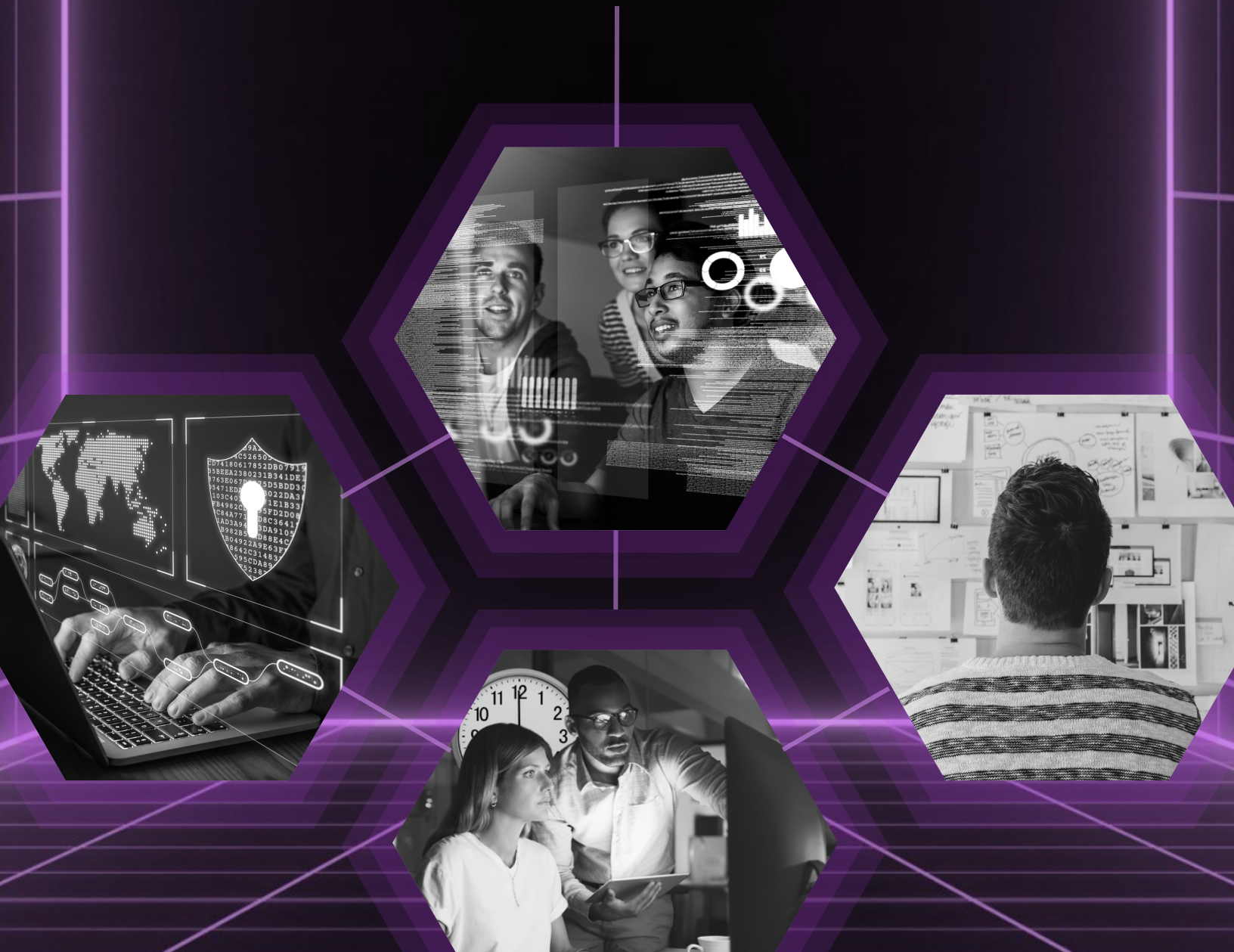

Table of Contents

Introduction

Red and blue teams often work in separate areas. For example, the red team might do offensive drills like pen tests, while the blue team works to strengthen defenses and respond to threats. Because of this divide, red and blue teams have developed a naturally adversarial dynamic - but when the two work together, they can craft a full image of their organization's security posture, rather than two fragmented ones.

That's where purple teaming comes in. Purple teaming is a dynamic, tailored approach to security that's risen in popularity in recent years. **It's the result of collaboration between red and blue teams, testing defensive capabilities against offensive attacks.**

Purple teams measure and validate an organization's security coverage to ensure that organizations are better prepared to defend against potential threats. There are different methods of purple teaming, each of which has its own advantages and disadvantages.

What is Purple Teaming?

Purple teaming is a collaborative approach to security that combines the skills and techniques of both red and blue teams to evaluate and fortify organizations' standing against potential threats. They are responsible for testing and validating an organization's security systems, processes, and procedures to ensure they are effective when the adversary truly strikes.

Red teams are experts in offensive security who test an organization's security posture through simulated attacks that emulate real-world threat actors. Blue teams, on the other hand, are experts in defensive security and are responsible for defending against external and internal threats. By combining the skills of both teams, purple teams are able to identify weaknesses and opportunities for improvement.

The Challenges to Creating a Purple Team

As valuable as it may be, creating a successful purple team is not without its challenges. While crafting a collaborative strategy, security teams should keep a few potential roadblocks in mind:

Cost:
The most obvious challenge to purple teaming is the cost. Purple teaming requires a significant amount of time and resources, which can be difficult for some organizations to source amid a busy SOC, talent gap, and tight budgets.

Teaming:
Another challenge is finding the right team members. It is important to ensure that the team is composed of experts in both offensive and defensive security, as well as other areas such as compliance, risk management, and incident response. This can be difficult, as purple teams require a unique combination of skills and experience.

Siloed Operations:
Finally, it can be difficult to ensure that all team members are working together effectively. A roadblock many purple teams face is the naturally adversarial dynamic at play between offensive and defensive teams. They have traditionally competing goals, and setting that aside for purple teaming exercises can be challenging. It is important to ensure that all team members are aligned on their roles and responsibilities, as well as their overall objectives. Communication is also essential, as it helps to ensure that all team members are on the same page and working towards the same goal.

The Benefits of Purple Teaming for Strengthening Your Security

Though it presents its fair share of challenges, purple teaming drives collaboration and fortifies security measures - there are many benefits to investing in purple teaming exercises.

Best of Both Worlds:
Purple teaming builds a comprehensive security posture by combining the best of both red and blue teams. It also reduces the workload for both teams because they can share responsibilities and collaborate to identify and mitigate threats.

Communication + Collaboration:
In addition, purple teaming can improve communication between the red and blue teams. By working together, both teams can gain a better understanding of each other's skills and objectives, resulting in a more efficient and effective security posture.

Risk Reduction + Efficiency:
Finally, purple teaming can reduce the risk of a successful attack, which in turn reduces the time and resources required to respond to one.

The benefits of purple teaming can be seen in many real-world examples. One of the most successful purple team approaches was implemented by the US Department of Defense (DoD). The DoD leveraged purple teaming to identify and disclose new malware, resulting in a more comprehensive security posture.

How to Implement a Purple Team Approach

Implementing a purple team approach requires organizations to commit to a collaborative effort. It is important to ensure that both the red and blue teams are working together to identify potential threats and develop strategies to mitigate them.

1

Set Objectives

The first step to implementing a purple team approach is to identify the objectives of each team. It is important to set team expectations of individual responsibilities and overarching goals.

2

Make a Plan

Once the objectives have been established, the next step is to create a plan of action. This should include a timeline for each team, required resources, and clear communication channels between the teams so that they can share information.

3

Monitor + Measure

The final step is to monitor and measure the performance of the purple team. This should include tracking the progress of each team, as well as evaluating the effectiveness of their strategies. This will confirm whether the purple team is meeting its objectives and can identify any areas for improvement.

Tools like MITRE ATT&CK & the SnapAttack Validations report can guide teams as they measure and adjust the effectiveness of purple team exercises.

How to Monitor and Measure Purple Team Performance

Monitoring and measuring the performance of the purple team is essential for ensuring that it is meeting its objectives. There are several key metrics that organizations should keep in mind when evaluating the performance of the purple team.

1. **Threats Identified**
   The first metric purple teams should track is the number of threats identified to determine whether the team is doing its job effectively.

2. **Mean time to Detect/Respond (MTTD/MTTR)**
   Organizations should also monitor the detection and response time for each threat, as this can help to identify areas of improvement.

3. **Mitigation**
   Risks identified during the engagement should be mitigated in a timely fashion. Tracking this metric drives accountability and efficiency into the vulnerability management program.

4. **Efficiency**
   By tracking threats identified and response time, security teams can evaluate the efficiency of existing security controls and strategies. Once they know how effective their current defenses are, they can strengthen or pivot those strategies according to their purple team findings.

5. **Team Progress**
   Finally, organizations should measure the team's overall effectiveness. This can be done by tracking the amount and efficiency of threat identification and response over time as the teams test and develop various security strategies. In doing so, organizations can identify any areas where the purple team is falling short and make the necessary changes to improve their security posture.

The Different Types of Purple Teaming

Each organization conducts purple teaming differently, and each method has its own advantages and disadvantages.

Traditional Purple Teaming

The most common purple teaming framework is the traditional approach, which is a simple back-and-forth exercise wherein the red team fires an attack at the network, and the blue team attempts to identify and prevent the attack.

Traditional approaches do have merit. A skilled red teamer can bring a level of creativity and technical capability to the table that automation cannot replace. Mature organizations with internal red teams will benefit the most from this approach, but it requires a significant amount of time and resources to implement. One of the primary challenges here is not every business has a resident red team, nor the resources to contract one on an ongoing basis to test implemented security controls even once or twice per year.

Automated Purple Teaming

For companies looking for a more cost-effective approach to purple teaming, automated purple teaming may be a viable option. This type of purple teaming uses automated pen testing and breach and attack simulation tools to identify potential threats and develop strategies to mitigate them.

Utilizing automated tools lends itself to a faster, more efficient approach - machines can run more tests in a shorter period of time, processing much higher quantities of data than a manual team could alone. Additionally, in a widening talent gap, hiring and training for the skills required to implement an advanced purple team program is a tall and expensive task - automated tools can pick up some of the labor and free up time for thinly-stretched security teams. Automated tools can streamline tasks like attack simulation as well to give teams direction and context without the same level of effort that they would need to manually conduct such exercises.

Many automated purple teaming tools automatically generate reports for the exercises they complete - this gives teams context, direction, and a clear picture of their coverage before moving forward with other security tests and activities. Not only do teams benefit from greater coverage and bandwidth, but leadership also gains visibility into their security standing.

While automated purple teaming is easier to implement from both a cost and resource standpoint, it still has limitations. A fully automated approach lacks the context and dynamic nature that the human element brings to purple teaming. Automated purple teaming tends to have higher false positive rates due to gaps in what the tools are able to accomplish; it is up to the person manning the tool to validate alerts, identify which threats are truly endangering their organization, and tune the tool as needed. In a constantly changing, evolving threat landscape, red and blue teams bring the touch of a true threat actor in a realistic environment to purple teaming that can't be accomplished by technology alone.

Organizations that lack an internal red team often see the biggest benefits through this approach, as the barrier to entry is significantly lower than building an in-house red team and aligning around a purple team approach. That said, many large organizations with internal red teams do utilize attack simulation tools to automate some of the more tedious tasks.

Hybrid Purple Teaming

Finally, there is the hybrid approach that we call continuous purple teaming, which combines elements of both the traditional and automated approaches. Hybrid purple teaming is often the most effective, as it allows organizations to leverage the strengths of both approaches while minimizing their weaknesses.

A hybrid approach to purple team combines the tools and efficiency of purple teaming tools or platforms with the manual operation and interpretation of team members. Using tools to automate components such as vulnerability scanning or certain attack simulations leaves red and blue teams more time to invest in the more manual aspects of purple teaming. Team members provide the perspective of a human attacker while the tools can streamline some processes leading up to the exercise itself, reducing the time between research, discovery, and remediation of threats.

Continuous Purple Teaming: A Hybrid Approach

Continuous purple teaming is an enhanced method within hybrid purple teaming. Continuous purple teaming is the fusion of threat-informed defense and collective defense, where red data (attacks) and blue data (detection analytics), and the people who produce that data, coexist and inform one another. This results in a continuous loop of enhanced security and an improved understanding of their own environment.

This integrated process leads to a robust, repeatable, and collaborative workflow that provides each team with the context necessary to leverage purple team findings. And best of all, a continuous workflow keeps teams up-to-date with the ever-evolving threat landscape.

Benefits to Continuous Purple Teaming

1. Saves time
2. More cost-effective than traditional purple teaming
3. More comprehensive than automated purple teaming
4. Mitigates human error
5. Reduction in red and blue team workload
6. Improved communication + collaboration

SnapAttack is the world's first continuous purple teaming platform, built to remove barriers to proactive cybersecurity and threat-informed defense. SnapAttack's threat intelligence library offers information that both red teams and blue teams can instantly equip in their exercises. Blue teams can define no-code, high-confidence behavioral detections directly from emulation data while red teams use SnapAttack's emulated threat library and high-quality threat intelligence to simulate attack behaviors and record attacks as data. Additionally, the work of both teams can be immediately compared to one another to define and measure an organization's coverage.

To achieve proactive, threat-informed defense, SnapAttack simplifies the process for validating security controls and closing detection gaps. Customers can employ SnapAttack's vendor-neutral, validated detections for proactive hunting and detection to take instant action on curated intelligence.

Users can monitor their threat coverage or build high-confidence, high-quality threat detection and hunt packages in reaction to gaps revealed by ongoing security validation by integrating high-quality threat intelligence into SnapAttack.

Achieving proactive, threat-informed security no longer requires multiple teams and tools but rather a single multidisciplinary team and one centralized platform.

Utilizing the SnapAttack Continuous Purple Teaming Platform, you can integrate purple teaming as a best practice in your enterprise, rather than waiting for a yearly or semi-annual review to find out whether you're protected.

Conclusion

In conclusion, purple teaming is an effective approach to security that brings together the best of both red and blue teaming.

By fusing the skills and responsibilities of both teams, not only are they empowered to collaborate - they break down the barriers holding them back from achieving robust, threat-informed security coverage.

Finally, purple teaming can reduce the risk of a successful attack, as well as the time and resources required to respond to one.

By combining the benefits of both offensive and defensive security, security teams can collaboratively and sustainably work toward a more comprehensive and effective security posture. If your organization is looking to leverage threat-informed defense towards more robust security, purple teaming is an effective solution to consider.

SNAPATTACK

SnapAttack was built ***by*** CISOs, SOC leaders, and threat hunters ***for*** CISOs, SOC leaders, and threat hunters.

By rolling cyber intel, adversary emulation, detection engineering, threat hunting, and ***purple teaming*** into a single, easy-to-use product with a no-code interface, SnapAttack enables you to get more from your technologies, more from your teams, and makes staying ahead of the threat not only possible but also achievable.

Schedule a demo today to see how you can finally answer the question, “Are we protected?” with confidence.