Brought to you by:

ATTACKIQ

Purple Teaming

for dummies®

A Wiley Brand

Execute effective purple team operations

Elevate your cybersecurity performance

Optimize your total cybersecurity program

Jonathan Reiber
Ben Opel
Carl Wright

AttackIQ Special Edition

About AttackIQ

AttackIQ, the leading independent vendor of breach and attack simulation (BAS) solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with the MITRE Center for Threat-Informed Defense.

Purple Teaming

AttackIQ Special Edition

by Jonathan Reiber, Ben Opel, and Carl Wright

for dummies®
A Wiley Brand

Purple Teaming For Dummies®, AttackIQ Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-82936-2 (pbk); ISBN: 978-1-119-82897-6 (ebk) Some blank pages in the print version may not be included in the ePDF version.

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager and Development Editor: Carrie Burchfield-Leighton
Acquisitions Editor: Ashley Coffey
Sr. Managing Editor: Rev Mengle
Business Development Representative: Molly Daugherty

Table of Contents

Foreword

I first learned about purple team operations when I was Chief Strategy Officer for Cyber Policy in the United States (U.S.) Department of Defense, designing the United States' first and second cyberdefense strategies to guide U.S. military forces in the conduct of cyberspace operations. At that time in U.S. history, the country was just beginning to invest in the "Cyber Mission Force," a team of 6,200 elite cyberspace operators whose job was to defend the U.S. against hostile nation-state and non-state actors in cyberspace. It was then that I learned of the singular importance of understanding adversary tradecraft in effective cyberdefense operations.

In 2015, Russian government hackers broke into the Pentagon's networks to try and access national security information. The team that helped repel those attackers came from the Cyber Mission Force team that was focused on defending the whole country against Russian government hostility. When I spoke to that team's commander at the time about the operation, then-Major General (U.S. Army) Paul Nakasone (now the four-star commander of U.S. Cyber Command) told me that the reason why they were able to repel the intruders from the Pentagon so quickly was because they were focused intensely on understanding the adversary and how to counter them.

That's why purple teaming is so important for security teams around the world, whether in public or private organizations. In a purple team construct, security teams constantly exercise their defenses against known adversaries' tactics and techniques to ensure that the defenses work as they should. Because they're focused on understanding prospective adversaries, they're ready if and when an intrusion actually happens. They're called *purple* because they combine the best of blue and red teams. When they work in close alignment, they conduct continuous assessments to ensure that security programs work as they should to stop advanced threats. Absent continuous, adversary-focused testing, there's no way to ensure that a security program will perform in the way that it must at the right time.

I hope you enjoy this book, designed to help you build effective purple teams. It explains the foundations of purple teaming

and a threat-informed defense, from using the MITRE ATT&CK framework of known threat behaviors to building collaborative teams to designing an automated testing strategy. The insights within it are drawn from decades of experience running cybersecurity operations for the private and public sectors. Co-authored by Ben Opel, a retired U.S. Marine Corps captain who guided the U.S. Marine Corps operational doctrine in purple team operations, Ben now teaches purple team operations to security leaders all over the world through AttackIQ Academy, a free online academy of courses for leading cybersecurity professionals. Ben and his colleagues teach courses on purple team operations, operationalizing MITRE ATT&CK, and uniting threat and risk management, among others. In addition to Ben's writing, this book includes insights of the third co-author, Carl Wright, Chief Commercial Officer at AttackIQ and former Chief Information Security Officer of the U.S. Marine Corps, a technologist and security leader who has advised the world's leading companies and public organizations on cybersecurity effectiveness. Finally, it reflects on the research of the MITRE Engenuity™ Center for Threat-Informed Defense, a research institution that builds on the MITRE ATT&CK framework to improve cyberdefense and advance the state-of-the-art and the-state-of-the-practice in threat-informed defense. AttackIQ is proud to be a founding research partner of the Center for Threat-Informed Defense, and the insights in this book stem from that work.

The cybersecurity community has learned an incredible amount over the last decade in operations, technology, and management, and purple team operations help improve collective cybersecurity effectiveness. I hope this book is helpful to you, and please reach out if you want to learn more about any of the concepts in this book. You can find me on Twitter at `@jonathanreiber`.

Jonathan Reiber

Senior Director for Cybersecurity Policy and Strategy, AttackIQ

Former Speechwriter and Chief Strategy Officer for Cyber Policy, Office of the U.S. Secretary of Defense

Introduction

Leading global organizations — from the United States military to global banks to energy providers — have been investing in cybersecurity for decades. Even after decades of investment in people, processes, and technology, however, intruders continue to break past organizational defenses. With the publication of the MITRE ATT&CK framework of adversary tactics, techniques, and procedures (TTPs), organizations for the first time have a single repository of threat behavior that they can use to test and validate that their cybersecurity controls work as intended. But what's the good of threat intelligence and automated testing if your security team isn't testing your defenses continuously and making adjustments to improve your security performance?

Enter the concept of *purple teaming.* Purple teaming takes the best of red and blue teams and brings them together around a common threat framework and an automated testing platform to improve cybersecurity effectiveness. Purple teams combine the threat focus of the red team and the defensive focus of the blue team to test an organization's defenses continuously. Purple teams focus on the overarching threat landscape, they understand their security technologies, and they understand their organization and its operational attributes. Purple teams ensure that organizations optimize their cybersecurity readiness continuously. The combination of the MITRE ATT&CK framework, an automated breach and attack simulation platform, and purple teaming as an operational construct delivers a threat-informed defense and cybersecurity effectiveness.

About This Book

Welcome to *Purple Teaming For Dummies,* AttackIQ Special Edition. The purpose of this book is to help you take practical steps for building a purple team to maximize your security effectiveness. Each chapter helps you understand, develop, and deploy purple team operations across your security program. At each point along the way, the lessons in this book have an overarching mission in mind: Make the most of scarce budgetary resources, drive down complexity for your security leaders, and increase security effectiveness.

Icons Used in This Book

Throughout this book we use special icons that alert you to important information. Here's what to expect:

TIP

The Tip icon highlights pieces of information that can help you do things quicker or easier.

REMEMBER

This icon calls out information that's helpful to remember when building your purple team.

WARNING

Information contained here points out struggles you want to avoid in your purple teaming journey.

Beyond the Book

This book can help you discover more about purple teaming, but if you want to find out even more information than we can offer in the 32 pages of this book, check out the following:

- **attack.mitre.org:** See the full MITRE ATT&CK framework.
- **mitre-engenuity.org/ctid:** Visit the Center for Threat-Informed Defense and gather key resources for deploying an effective threat-informed defense through your purple team.
- **academy.attackiq.com:** AttackIQ provides online courses to improve your cybersecurity operations and effectiveness.
- **attack.mitre.org/resources/adversary-emulation-plans:** Discover how your purple teams can use automated adversary emulations to drive effectiveness.
- **attackiq.com/solutions:** See ways your purple teams can deploy an automated breach and attack simulation platform.

IN THIS CHAPTER

- Discovering what is meant by purple teaming
- Integrating purple teaming into your security

Chapter 1
Understanding Purple Teaming and Cybersecurity

In art, mixing mellow blue with aggressive red yields a vibrant purple. What happens, though, when the same palette is combined in the realm of cybersecurity?

Blue and red security teams typically live in separate organizational silos. This is partially a matter of organizational structure and partially a reflection of each group's intent. Blue teams are the guardians of the corporate network; they're focused on defending key terrain, meeting regulatory requirements, and ensuring cybersecurity effectiveness. By contrast, red teams are, essentially, tasked with conflict. Their purpose is to lay the groundwork for a threat-informed defense, which entails developing a deep understanding of attackers' tradecraft and technology. Red teams must get into the mind of the enemy in order to test the company's carefully planned controls in the same ways that an actual attack would.

Because of the stark differences in attitudes and tactics, many organizations' blue and red teams keep their distance from one another. Still, an emerging security best practice — purple teaming — involves bringing them closer.

Introducing Purple Teaming

REMEMBER

Purple teaming is a relatively new security team structure, in which members of your blue and red teams work together collaboratively. They align processes, cycles, and information flows — and, as a result, they overcome the competitive or even adversarial dynamic of the traditional siloed security approach.

Although the name may seem to imply that blue and red teams, as distinct entities, are eliminated, purple teaming doesn't typically involve integrating those groups on the organizational chart. Instead, your red and blue teams continue to operate independently. In many cases, your blue team is a part of your company and the red team is hired from the outside as a consulting team. However, large, well-resourced organizations — like global banks or the United States military — are more likely to have internal red teams. Either way, a shift to purple teaming means that your red and blue teams develop highly communicative, supportive, and cooperative relationships across the functional boundary.

Such a structure is ideal because each group has gaps in capabilities that the other can fill. Purple teaming simultaneously optimizes the skillsets and minimizes the limitations of both red and blue teams, paving the way for a threat-informed defense. Check out Chapter 2 for more on a threat-informed defense.

Tying Purple Teaming to Your Security

Purple team operations lead to an increase in cybersecurity effectiveness by bringing the adversary-focused mindset of the red team together with the defensive knowledge and capabilities of the blue team to focus your defense capabilities on the threats that matter most. Building an effective purple team requires leadership — and it helps to have a clear starting point, like the MITRE ATT&CK framework, to focus your collaborative effort.

This section explores the relationship between MITRE ATT&CK, purple team operations, and the steps required for managing, planning, and changing your organization to deploy effective purple team operations.

Building trust and cooperation in this new purple world requires your security organization to develop a shared understanding of the threats that pose the greatest risk to your organization, as well as an agreed-on approach for determining whether defenses are working properly. This is a management-plan-and-change process.

To institute a common language for threat research, many organizations transitioning to purple teaming now turn to the MITRE ATT&CK cybersecurity framework. Developed by the not-for-profit MITRE Corporation, ATT&CK is a knowledge base of adversary tactics, techniques, and procedures (TTPs) that have been observed in real-world cyberattacks. It's a comprehensive and authoritative guide to the global threat landscape, and many red teams have relied on it for years to build their understanding of adversaries' TTPs.

REMEMBER

Pairing the thorough and detailed MITRE ATT&CK framework with an automated breach and attack simulation (BAS) platform enables your security organization to routinely simulate the attacks that are most likely to threaten you. Your red and blue teams can work together to

- Design the testing regimen
- Jointly identify security control errors and gaps
- Undertake mitigation measures
- Retest to validate that their security controls are effective

To achieve these steps, security leaders and the security team first must begin to shift toward purple. The transition isn't simple. It involves building communication channels and fostering consensus and collaboration among groups of professionals who've historically seemed to operate on opposite sides of security testing strategy.

The effort will undoubtedly pose challenges, but, as a security leader, you can bring your red and blue teams closer until their knowledge and perspectives begin to blend into a unified wall of purple. The four steps to achieve this task include

1. Recognizing the strengths and weaknesses of each group
2. Cultivating a continuous improvement attitude

3. Building a testing strategy to implement a threat-informed defense
4. Establishing clear communication among the blue and red teams and management


REMEMBER

By integrating these four steps, which we cover in more detail in Chapter 3, with the MITRE ATT&CK framework and automated testing at the center, your security teams can align red and blue and pivot toward a purple team construct to validate your security controls continuously and at scale to maximize effectiveness.

IN THIS CHAPTER

- Explaining a threat-informed defense
- Having a threat-informed purple team

Chapter 2
Implementing a Threat-Informed Defense

The concept of a threat-informed defense underpins successful purple team operations. This chapter describes the elements of a threat-informed defense strategy as it relates to the MITRE ATT&CK framework, purple team operations, and how teams develop a successful testing strategy to ensure comprehensive security control validation. You discover the key elements of a threat-informed defense strategy, how purple teams incorporate threat knowledge into their operations, and how red and blue teams can improve their collaboration by focusing on known threat behaviors and security program performance.

Recognizing the Elements of a Threat-Informed Defense

Underpinning purple team operations is the concept of a *threat-informed defense.* Put simply, it means to secure yourself; you need to think like the adversary and focus on the adversary's tactics, techniques, and procedures (TTPs) to maximize defense effectiveness. How will adversaries target you? What can you do to defend yourself against their approach?

Taking on a threat-informed approach to security planning, historically speaking, meant network defenders focused on meeting baseline security practices correcting misconfigurations, administering patches, and deploying commercial cybersecurity products. If anyone took on an adversary mindset, companies outsourced the threat-focused part of the equation to red teams that would try to break past their network defenses. The hitch is, absent a threat-informed defense approach, security teams risk strategic drift, prioritizing compliance standards, and fixing network configurations instead of maximizing their effectiveness against known, dangerous threats and behaviors.

REMEMBER

The biggest driver of transitioning to a threat-informed defense is the national security research that codified adversary behavior. The MITRE Corporation pioneered the MITRE ATT&CK framework of known adversary tactics, techniques, and behaviors. ATT&CK places known adversary behavior into one single table of adversary behaviors, tactics, and sub-techniques. From there, a threat-informed defense has three key elements:

- **Cyberthreat intelligence analysis:** Use the MITRE ATT&CK framework to anticipate the adversary's next move at each stage of an attack. Then, they take this knowledge to test their security teams to better respond to known attacks.
- **Defensive engagement:** Security teams use the ATT&CK framework to look for signs that an attack is in progress to mitigate threats in real time and develop a knowledge base of past exploits that can inform response to future threats.
- **Focused sharing and collaboration:** Cyberdefenders work in partnership to share threat information, test their defenses, and improve operational effectiveness

Organizationally, appointing a leader to manage threat-informed defense across the organization is important. This person aligns the purple team around the MITRE ATT&CK framework, overseeing the testing strategy required for effective security control validation, and ensuring that blue and red teams are aligning their controls against known threat behaviors to generate the performance data required for cybersecurity effectiveness. Having one single leader to manage the threat-informed defense strategy helps the organization transition toward a data-driven, management-focused strategy that prioritizes metrics, effectiveness, and collaboration to ensure that the program works as best it can.

Adopting a Threat-Informed Purple Team

Integrating an adversary mindset requires organizational effort but not necessarily new team members. Adopting a threat-informed defense approach is more of a methodology. It does mean, however, that organizations need to shift away from the traditional blue/red paradigm and toward the purple team construct. A blue team becomes purple when it emulates the adversary as a means of self-evaluation. In the process of adopting a threat-informed defense strategy, blue teams should ask whether

- **They understand the most dangerous threats they face, and which are most likely to impact their operations.** What tactics, techniques, and procedures will the adversary deploy? Teams can prepare for known adversary threats by using the MITRE ATT&CK framework.
- **They understand their organizational mission, center of gravity, and critical vulnerabilities.** What will the adversary seek to hold at risk? What are their crown jewel applications? How will the adversary seek to engage those assets, and what defenses work to protect those assets?
- **They understand and trust their security controls architecture and teams.** Have security controls been tested and validated against known threats? Is everyone working together?

To operate as a threat-informed purple team, your teams should be familiar with the overarching threat landscape, their defense capabilities, and your organization. They should be able to self-iterate their security posture. They should be able to clear low-effort attacks, validate security controls, and challenge advanced threats by defending themselves against known adversary TTPs. Finally, by deploying automated adversary emulations against their security controls, purple teams can validate their security control effectiveness.

THE PURPLE OF U.S. CYBER COMMAND

Over the last decade, the U.S. military has been at the forefront in transitioning from a network-defense approach to a threat informed defense. Other organizations can draw real lessons from the experience. Since its founding, U.S. Cyber Command (USCYBERCOM), the U.S. military's cyberspace operations wing, has operated under the direction of the four-star commander who's also the director of the U.S. National Security Agency (NSA). Tight links between USCYBERCOM and NSA create a mutually beneficial intelligence-operations cycle that helps the team find and pursue leads, discover new information, and create opportunities to coordinate.

For example, when staff at NSA and USCYBERCOM formed a Russia-focused small group to defend the country against prospective interference by the Russian government in the 2018 U.S. Congressional elections, intelligence flowed into the defensive planning cycle. USCYBERCOM and NSA remain separate organizations, but the leader can direct them to work together.

Organizations that merge intelligence and operations — red and blue team activities — for their cybersecurity can achieve similar benefits in the purple team's threat intelligence and strategic planning. The head of USCYBERCOM is essentially the military's director of threat-informed defense for purple team operations, and security teams can adopt an similar position. The role doesn't require a new team member, just someone who's dual-hatted to lead purple teams forward in a threat-informed defense.

IN THIS CHAPTER

- Identifying your teams' strengths and weaknesses
- Promoting continuous improvement
- Building your testing strategy
- Maintaining clear communication

Chapter 3
Seeing How Your Organization Can Build a Purple Team

So how do you build a purple team? You follow the four steps laid out in this chapter.

Step 1: Recognize the Strengths and Weaknesses of Each Group

What do red and blue teams bring to the table? As a leader, it helps to take stock of who they are and what each team does. And once you bring them together, you need to realize the effectiveness of purple teaming.

Looking at red teams

Red team testing simulates adversary behaviors to validate the effectiveness of specific security controls (comprised of people, processes, and technology). Individuals who specialize in red

team testing are threat emulation specialists. Their strengths include cultivating a big-picture perspective on the cyberattack landscape so they can adapt information from threat intelligence reports into safe, workable simulations that realistically test the controls of your specific organization.

WARNING

The challenge is that manual red team testing is too resource-intensive to happen continuously. An external red team may run a test, identify weaknesses, and then leave until your company starts its next testing cycle. In this case, your organization's blue team may be responsible for implementing red team recommendations after the red team has moved on. Even internal red teams can't possibly cover all your organization's critical controls through manual testing.

Digging into blue

The blue team is responsible for defending your company's assets and operations in cyberspace. Its members specialize in detecting, investigating, and resolving anomalous behavior and out-of-the-ordinary events in your specific IT infrastructure. Blue teams usually possess a deep understanding of your business, the network, and security architecture. This inherent institutional knowledge is invaluable in guiding decisions about what types of threats pose the greatest risk to your organization and how to mitigate them.

WARNING

Blue team members who see "passing" a red team test as vital to demonstrating their own effectiveness actually have a disincentive to assist with designing rigorous assessments. Add to that the resource shortage that permeates many cybersecurity organizations — leaving everyone overworked — and the blue team may be less likely to penetrate organizational defenses. The blue team members are also less likely than their red colleagues to have the devious mindset of an attacker; in fact, blue teams may have a fairly shallow understanding of prospective adversaries.

Making the case for purple teaming

The trick to building a purple team is to harness the value of both blue and red teams. These teams sometimes develop a "pass/fail" mentality around testing. The red team works to find control gaps, while the blue team focuses on ensuring that their systems "pass" the red team's tests. This approach muddies the ultimate goal: to hone defenses to thwart real cyberattacks your organization is likely to face.

Just as the red team should work with its peers in blue to better understand the unique features, high-value assets, and security needs of the overall organization, the blue team should turn to the red team for help in understanding what its organization's defenses face. Blue team members need to continuously work to improve their knowledge of the anatomy of different types of attacks, and interactions with the red team can help speed up the learning.

REMEMBER

Achieving baseline security today requires that your red and blue teams work hand-in-hand — purple teaming. The cyberthreat outstrips any one group's ability to understand and adapt to the threat landscape. Siloed groups don't work; red and blue team members need to share an attitude of mutual respect and appreciation. Lines of communication must be open in every direction.

Your Chief Information Security Officer (CISO) should facilitate purple team collaboration, starting with building consensus on which attacks pose the greatest risks to your company. Together, red and blue team members should review the attack variants and TTPs described in the MITRE ATT&CK framework, jointly developing a most-wanted list of adversary techniques to test against. They can pose such questions as

- What elements of our business are most vulnerable to cyberattack? What might be the ramifications if our defenses were to fail?
- Which threats and TTPs from the MITRE ATT&CK framework do we need to incorporate?
- How frequently should we repeat each type of test?

Participants can mine ATT&CK for a detailed description of each technique and a list of threat actors known to use it. The goal of this exercise is to bring the red and blue team members into alignment on how your company should approach its threat-informed defense strategy.

From there, the CISO can further support the purple team by getting everyone in the same room and running table-top exercises to move through a prospective attack campaign. Dialogue around attack techniques, your organization's security controls, and options for response and mitigation can make the importance of red and blue team collaboration apparent to everyone involved.

AUTOMATED TESTING AND PURPLE TEAM OPERATIONS

The manual red team approach also has significant limits. Given the scope of the attack surface, companies can't routinely test themselves against a full array of TTPs manually. At the same time, a one-off, point-in-time test fails to validate security controls on a continuous basis; if a control gap opens up, the red team may not notice it for a long time. To ensure security effectiveness, companies need to test at scale, appropriate scope, and in a continuous fashion. And that way to do that is through automation — a breach and attack simulation (BAS) platform that can emulate a wide range of attacks as frequently as the organization requires, in an affordable way.

An automated BAS platform that aligns with MITRE ATT&CK can regularly emulate the most probable methods of adversary attack. ATT&CK-aligned automated tests provide visibility into the performance of security controls on an ongoing basis, quickly alerting staff to any control gaps that may arise, and the blue team uses test results to improve the overall effectiveness of the organization's defenses.

A BAS solution also provides on-demand reporting. If a new threat emerges or something changes within the corporate network, a new automated test can generate a report that validates the effectiveness of organizational controls. Red teams can leverage a BAS platform to augment manual testing. Blue teams can use it to supplement red team testing, especially if the red team is external. Either way, automated testing should be a central feature of your purple team operations.

Step 2: Cultivate a Continuous Improvement Attitude

Success in the purple team venture requires building an attitude of continuous improvement across your teams. Some organizations' cybersecurity cultures unintentionally pit the blue team against the red team, with blue teamers worrying that a hard red team test may break key components of their security infrastructures. A good BAS platform can test organizations safely and in a production environment; more importantly, automated adversary

emulations test not only the technology but also people and processes. Such an assessment can be understandably uncomfortable for the people under the microscope.

Many blue teams respond by preparing staff and systems for the specific test they're going to face. They expect to receive a warning so they can bulk up the relevant defenses. Needless to say, attacks in the real world occur without notice.

It's time to flip this calculus. If in the future, teams feared assessments, going forward both red and blue teams should look forward to attack simulations to drive up effectiveness. Assessments are an opportunity for blue team members to learn how to improve their security and to do so in a scenario where consequences are limited. Far better to learn of control gaps through automated testing than as a result of an actual data breach or ransomware event.

But before blue teams can shift away from seeing tests as something to fear and pass, they need confidence that management will adopt the continuous improvement mindset and avoid hammering them for control failures. Security leaders need to set a consistent and supportive tone. Security is difficult. Threats are dynamic. It is critical to validate security control prevention and detection capabilities and to find gaps in an organization's defenses. Across the red team, blue team, and security leadership, everyone needs to view each assessment as a chance to improve their understanding of threats and defense effectiveness.

Such a continuous improvement attitude needs to underpin an organization's overall approach to adversary emulations. A company can fend off actual attacks only if all teams are committed to perpetual learning.

Step 3: Build a Testing Strategy for a Threat-Informed Defense

After the CISO has established that a collaborative purple team needs to pursue security assessments as a means of continuous improvement, the next step is to design and build a continuous testing strategy. As a starting point, the purple team should perform an audit of the current security infrastructure. They should

document controls, as well as their understanding of the strengths and weaknesses in the organization's cyberdefenses. Then, they should begin planning to test those assumptions.

Every organization needs a process for systematically identifying and mitigating security gaps. However, the security team can't defend against every possibility. Attempting to protect everything equally results in inadequate protection across the board. Security strategies should focus on the subset of pertinent threats that are most likely to do the most damage. As your organization develops its security assessment strategy, the CISO should ensure that the testing process focuses on the threats the purple team has identified as most critical.

The CISO should also ensure that assessments are viewed as a program, not a project. Semi-annual or bi-annual testing is inadequate for a number of reasons:

- The threat landscape is constantly changing as attackers refine their methods.
- The organization's defenses are in perpetual motion.
- Changes undertaken for an entirely different purpose may open a new control gap that's invisible in day-to-day IT operations.
- Infrequent point-in-time tests may allow an attacker to dwell within a network for weeks, or even months, before the breach is detected.

TIP

Instead of discrete testing periods, deploy an ongoing program to operationalize testing. Dovetail with the purple team's continuous improvement mentality and result in frequent, incremental improvement. If testing reveals a control gap, the blue team can make investments to fill the gap. An immediate retest can determine whether the changes closed the gap and can identify opportunities for further improvement.

Such a testing strategy is difficult to deploy when control assessments are performed manually. Instead, a purple team needs to leverage automated testing through a BAS solution like the AttackIQ Security Optimization Platform. This approach operationalizes simulations, enabling either red or blue teams to perform as frequently as needed. In addition, AttackIQ improves

assessment efficiency, freeing up resources for more analysis and mitigation activities.

A good BAS platform should maintain a tight integration with MITRE ATT&CK, running scenarios aligned to specific TTPs identified in the ATT&CK framework to facilitate a threat-informed defense.

Step 4: Establish Clear Communication Flows

Throughout the development, implementation, and operation of a threat-informed testing regime, all security resources — both internal and external — must work closely together. They need to share unique perspectives and insights while learning from their colleagues. That is the point of the purple team. But it doesn't happen without intentional process changes.

Establishing clear communication flows among red and blue team and management is vital. The CISO has many roles, which we cover in this section.

Having built-in feedback loops

The CISO ensures that linkages among red team and blue team members are built into a formal, structured feedback loop. Each test should conclude with a joint debriefing session, where purple team members reflect on which controls worked as expected and which attack techniques found defensive gaps. Remediation reports from an automated security control validation platform provide the CISO with clear visibility into your organization's performance.

The purple team discussion after an automated test should address mitigation, but it should also reflect on the effectiveness of the assessment itself, evaluating the following:

- What you learned from the assessment
- How well your detection capabilities worked
- Any present indications that you need to refine specific aspects of your testing program

Turning the continuous improvement mindset toward the assessments enables your company to build and execute ever-more-difficult scenarios that provide a real view into your ability to defend itself against the most dangerous threats.

Ensuring security testing policies are in place

The CISO should ensure that the organization has a well-defined, clearly articulated security testing policy. Documentation that's accessible to everyone involved in security should outline how frequently your organization tests controls, who conducts the tests, and what objectives or milestones the assessment process should produce.

Establishing communication processes

The CISO also needs to establish a process for communicating the security testing policy to the red team. If the red team is external, its statement of work should address expectations for collaboration and information sharing, as well as expectations about which areas of the security program the red team will manage.

Cycling testing and remediation

Another part of building purple synergies is aligning the blue team's update-and-installation cycles with red team testing schedules. The CISO's end goal should be to ensure that the purple team operates in a cohesive cycle of testing and remediation that complements the timelines of all groups affected by the security assessment program.

IN THIS CHAPTER

- Seeing the role of purple teaming in healthcare
- Managing people with purple teaming
- Revealing risk in regulatory policies

Chapter 4
Looking at Purple Team Use Cases

Developing and managing a threat-informed defense strategy and implementing purple team operations may feel abstract for you until you gain a tangible sense of how purple team operations work in practice. In this chapter, you see how certain teams develop and deploy purple team operations, a threat-informed defense strategy, and a breach and attack simulation (BAS) platform to validate security controls and elevate the entire cybersecurity effectiveness.

Placing Purple Teams in the Healthcare Sector

The head of red teaming at a major global healthcare organization uses a purple team construct to validate his security controls and elevate his cybersecurity program's effectiveness. The board of directors holds its team responsible for answering three key questions:

- Is our security infrastructure good at resisting attacks from the outside?

- Are we good at stopping data (medical information, patient records, and so on) from leaving the company in an unintended way?
- Is the company getting a good return on security investments?

Many things can go wrong in security — so many types of technologies, so many different scenarios. This puts a premium on cybersecurity effectiveness, the healthcare cybersecurity expert says. How does he ensure that his program works as well as it can? Purple teaming is vital to the process.

The head of red teaming says that performing tests a few times a year isn't sufficient. But you can significantly enhance the benefit you get out of purple teaming and automation to measure the things you're doing to determine what's good and what's bad. You want to get to a place where, if an adversary appears, you know that your weapons are working.

Purple Team Testing to Manage People

Sometimes, weaknesses have nothing to do with technology; purple team testing can reveal problems in security program performance across operations. If the purple team finds that a security control is failing, that leads the team to wonder why. Here's an example.

One company is underpaying its key staff, and the staff is leaving. The human operations capability is downgraded, and the board may not know about it until a red team operation is performed. By knowing what the company needs to test for, and deliver against, it's crucial to justify increases in salary for its teams.

If you run an automated purple test, it may show a security control failure. After further investigation, you learn that teams are failing to perform because of staff turnover, but that the turnover is driven not by technology but by problems in salary. Only through a security outcome driven test do you learn that there's a performance problem within the team. Only by investing the problem further do you discover that security personnel are leaving because of problems in their salary. The human resource

department wouldn't discover this on its own necessarily, but, by discovering security program degradations and investigating how and why it's happening, you learn something and make change happen.

A purple team construct can find problems in internal processes, but it can also reveal problems in external managed security service providers (MSSPs). When you red team an MSSP, you may find out that the business was relying on a third party that, in fact, wasn't performing. What could a purple team test reveal? Say, for the MSSP, the salesperson has the invoice for the renewal of a certain license of that service that you need for your security. Your organization hasn't signed the contract. It just shut it off. It might be like the oxygen of your operation, but no one has told you where it is. It's stuck in procurement somewhere, stuck in receivables. So the person who is dependent on it at your home organization doesn't know that the purchasing department hasn't paid the invoice.

From there comes the real work of improving the team. That the red team found the deficiency isn't the question. The question you want to answer with an automated testing platform and purple teaming is extremely potent. You're talking about a process of continuous controls assurance. To do so requires continuous testing.


TIP

Each team needs to make decisions about prioritization and testing frequency. Prioritize controls based on granularity. Some you may run infrequently, like once a week. Others are key and may be run every 24 hours.

Purple Teaming in A Global Regulatory Environment

For a large multinational organization, purple team operations can also reveal risks presented by different countries' regulatory policies. Some countries allow for firms to take on a robust security approach, while others have strong privacy protections that prevent firms from being able to scan certain kinds of traffic.

Every global organization has to operate under the national laws in which it conducts operations. Some countries, like the United

Kingdom and Australia, allow companies to inspect traffic that leaves their networks; other countries like Germany and Poland don't. The business is prevented from scanning outgoing traffic in those countries.

How does this increase organizational risk? And what does that mean for a purple team tasked with protecting the organization? An attacker wants to find your most relaxed part of your organization. If an attacker breaks into an organization in one country, that could impact the security of the company in another country given the globally networked nature of the organization. This is particularly the case for global services like Active Directory. The attacker could try to find a way into the organization through the least well-defended part of the organization; from there, once they gain access, the question is if they then move laterally to exfiltrate that data.

REMEMBER

But purple teaming provides a solution. You can answer all questions consistently, repeatedly, and at scale. If you run a red team today and have two different people running the same test, yet the organizations you're using are different, you need to take subjectivity and politics out of the equation. You need a non-subjective test that's repeatable, consistent, and scalable.

With purple teaming, uncertainty is managed. Ultimately, the expert sees purple teaming and automated testing as a revolutionary approach to transforming security. Your assurance effectiveness is going to go way up. Your board is going to be robust with auditors, and you're going to be confident that you're doing the right thing. And with quantified evidence, you can measure real-world attacks against your controls. You drive toward success by integrating red and blue teams and executing a strategy of continuous testing.

IN THIS CHAPTER

- Shifting organizational culture
- Recognizing your assets and defenses
- Testing more than technology
- Centralizing performance data

Chapter 5
Ten Lessons for Purple Team Operations

What are some of the key lessons to transition security teams to a purple team construct? Leading corporate security functions are transitioning from a siloed fortress mentality of network defense to an approach that combines a purple team mindset with a threat-informed defense. This chapter gives you ten lessons on how to effectively build a purple team construct and improve your cyberdefense posture.

Lead An Organizational Culture Shift

Building a purple team construct isn't like plugging in a new technology; change requires leadership and direction. Purple teaming brings tremendous benefits to security teams and increases cybersecurity effectiveness, but it requires security leaders to manage and plan for change.

Recognize Your Teams' Strengths

Your red and blue teams bring unique insights to security operations. The red team understands the adversary, and its tactics and techniques may have a historical sense of how the adversary has behaved in the past and often likes the challenge of testing a blue team's defenses. Blue teams understand the missions that matter most to the organization, understand its security capabilities, and know personalities of the security team players. By bringing the teams together in strength, you increase the chance of success. For more about recognizing your teams' strengths and weaknesses, check out Chapter 3.

Adopt Continuous Improvement

You can set the tone for success by helping teams adopt an attitude of continuous improvement. Success doesn't come by breaking past blue's defenses or mean you defend against the adversary correctly every time. Continuous learning is at the center of a purple team construct. Red teams learn to test blue repeatably, at scale, to validate your organization's defenses. Blue teams learn the thrill of elevating their cyberdefense capabilities against the adversary over time, and see the benefits of continuous testing as they run emulations in partnership with the red team, reveal gaps in defenses, and improve their defense performance. Cultivating an attitude of continuous learning sets the conditions for cybersecurity effectiveness. For more info, check out Chapter 3.

Identify Key Assets and Defenses

A purple team construct should drive blue and red teams to work together to identify and test the defense assets that matter most. Are those assets working as they should? Are they geared toward defending the data that matters most? Are they effective, or are other capabilities (people, processes, and technologies) required? By working together in a continuous testing process, red and blue teams can conform their defenses protect key assets.

Adopt a Continuous Testing Strategy

The purple team construct is built on the notion that one-off testing is insufficient to guarantee cybersecurity effectiveness. Teams can come together and rally around the concept of a continuous testing strategy that identifies the most important defense assets, tests them continuously, and uses performance data in a feedback look to validate defense effectiveness. This process requires a strategy that can guide the team forward.

Test People, Process, and Tech

While a purple team construct can reveal failures in security control prevention and detection, what matters most are the questions and mitigations that follow. If a security control failed, it could be due to misconfiguration, which is easy to solve, or it could be due to personnel or process problem that demands investigation (check out the healthcare case study in Chapter 4).

REMEMBER

You're testing all three aspects of security: people, process, and technology.

Use ATT&CK to Unite the Team

Purple teams can use the MITRE ATT&CK framework to organize their testing. ATT&CK provides a clear, user-friendly threat intelligence framework that teams can use to prioritize assessments, investments, and future planning. The MITRE ATT&CK framework gives teams a starting point to work off the same sheet of music, think like an adversary, and run continuous tests to drive up effectiveness.

TIP

For additional insight into MITRE ATT&CK, download a copy of *MITRE ATT&CK For Dummies*, AttackIQ Special Edition, at `attackiq.com/lp/mitre-attack-for-dummies`.

Augment ATT&CK with Automation

Purple team operations are inefficient if they're limited to manual tests. The combination of MITRE ATT&CK and purple team operations enable a comprehensive threat-informed defense. Even if you have a small security team, you can leverage the MITRE ATT&CK framework by deploying an automated testing platform in your environment and use the automated platform to augment your red team — even if it's just one person whose job is to think like an adversary. Automated platforms can drive down annual red team testing costs, maximize returns on investment for security controls, and improve personnel performance.

Build Communication

If you can't build clear communications between the red team, blue team, and management, most other subjects in this chapter don't matter. Everyone should work together to measure and test security controls and to elevate security program effectiveness. The management team should understand the purple team construct and the goals of the team (continuous testing and validation), and the red and blue team should have open lines of communication between them as they work to get ahead of real-world attacks. Flip back to Chapter 3 for more info.

Centralize Performance Data

A purple team construct focuses security teams on preparing for the threats that matter most and on running a continuous testing strategy to gain granular visibility into their security program's effectiveness. Today, private organizations lack visibility into their security teams' performances against known threats. A threat-informed defense strategy solves that problem by focusing the organization on known threats, and then testing the organization against known threat behaviors to generate real data about its security program's performance and maximize security effectiveness. Performance data is what gives security teams the visibility they need to succeed.

Execute effective purple team operations

How can you ensure that your cybersecurity program works as well as it should? As cyberattacks increase in velocity and impact, this question haunts security leaders every day. Intruders break through defenses, controls falter, and organizations pay hefty ransoms (or worse). What is the way forward? The era of siloed red and blue security teams is over. Red and blue can blend together in a purple team construct to deepen collaboration, implement a threat-informed defense, and elevate cybersecurity effectiveness.

Inside...

- Put MITRE ATT&CK into practice
- Incorporate a threat-informed defense
- Lead organizational change
- Deepen collaboration between teams
- Develop an automated testing strategy
- Test people and process, not just tech
- Learn from a big multinational company

ATTACKIQ

Jonathan Reiber is Sr. Director for Cybersecurity Strategy at AttackIQ and former Chief Strategy Officer for Cyber Policy in the U.S. Defense Department. **Ben Opel** is Sr. Director for Customer Success at AttackIQ and a former Marine. **Carl Wright** is CCO at AttackIQ and prior CISO of the U.S. Marine Corps.

ISBN: 978-1-119-82936-2
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.