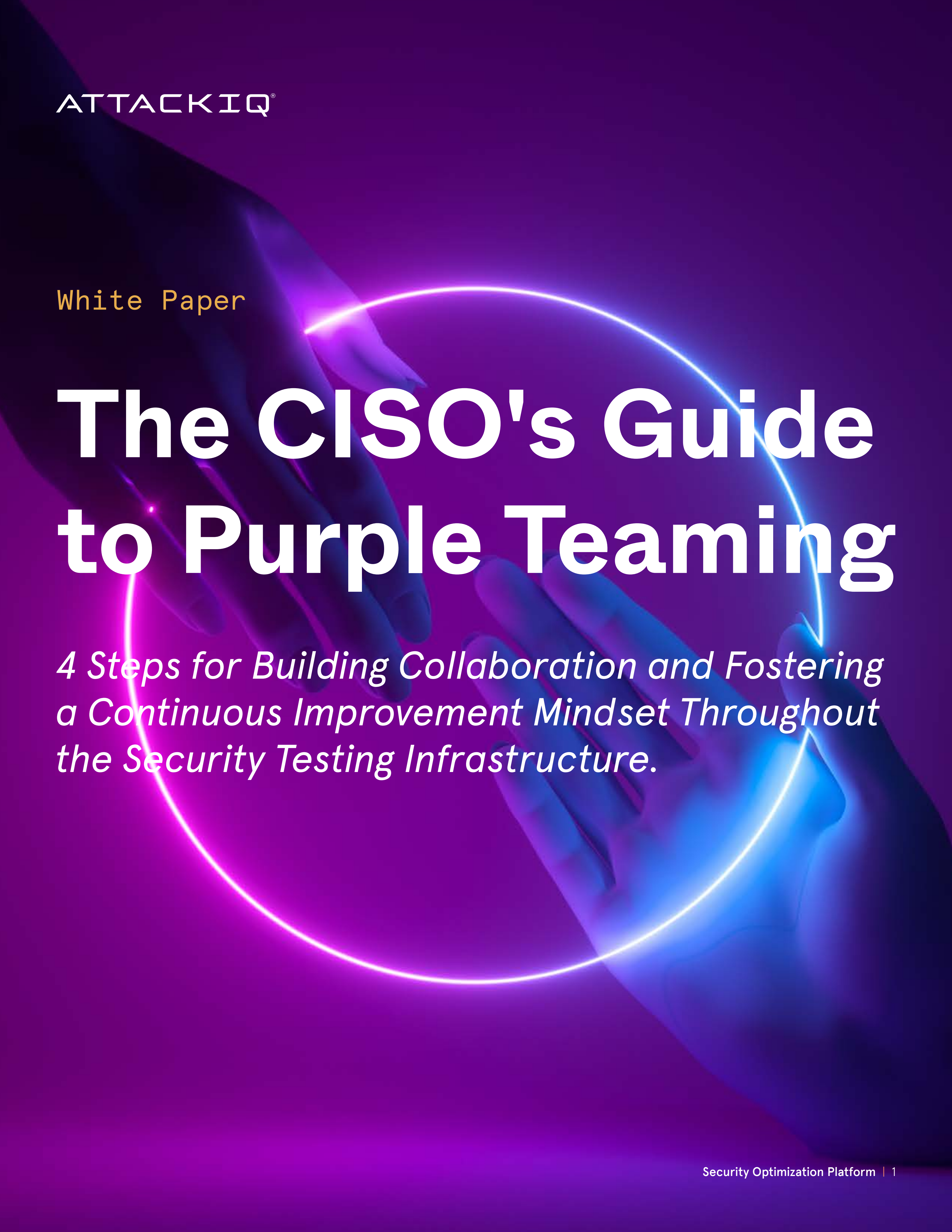
ATTACKIQ®



White Paper

# The CISO's Guide to Purple Teaming

*4 Steps for Building Collaboration and Fostering a Continuous Improvement Mindset Throughout the Security Testing Infrastructure.*

# Notice

AttackIQ® publications are made available solely for general information purposes. The information contained in this publication is provided on an "as is" basis. Any additional developments or research since the date of publication will not be reflected in this report.

# Executive Summary

## Moving Toward the Color Purple

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 are 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."[1] 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, it is understandable that many organizations' blue and red teams keep their distance from one another. Still, an emerging security best practice involves bringing them closer. "Purple teaming" is a relatively new security team structure in which members of 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.

## What Even Is a Purple Team?

Although the name implies elimination of blue and red teams as distinct entities, purple teaming does not typically involve integrating those groups on the organizational chart. Instead, the red and blue teams continue to operate independently. For companies that have their own security team (vs. an external managed security service provider), the blue team is in-house, while the red team is in many cases external. Large, well-resourced organizations — like global banks or the U.S. military — are more likely to have internal red teams. Either way, a shift to purple teaming means that the still-distinct 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, paving the way for a threat-informed defense.

### ELEMENTS OF THREAT-INFORMED DEFENSE

What is a "threat-informed defense"? The MITRE Corporation views threat-informed defense as consisting of three elements:

- **Cyberthreat intelligence analysis.** Leverage the MITRE ATT&CK® framework to anticipate your adversary's next move at each stage of an attack. Then, using this knowledge, "harden cyber defenses and improve ways to...prevent, detect, and respond to cyberattacks."[2]
- **Defensive engagement of the threat.** Security personnel proactively look for signs that an attack is in progress, both to mitigate threats detected in real time and to develop a knowledge base of past exploits that can inform response to future threats.
- **Focused sharing and collaboration.** "Among communities of cyber defenders, working in partnership provides a force-multiplier effect. These collaborations can greatly benefit cyber-threat intelligence analysis and strengthen cyber defenses."[3]

[1] "Focal Points: Threat-Informed Defense," The MITRE Corporation, accessed February 17, 2021.

[2] "Threat-Based Defense: Understanding an attacker's tactics and techniques is key to successful cyber defense," The MITRE Corporation, accessed February 16, 2021.

[3] "Threat-Based Defense: Understanding an attacker's tactics and techniques is key to successful cyber defense," The MITRE Corporation, accessed February 16, 2021.

## What Even Is a Purple Team? (cont.)

> ***"Building trust and cooperation in this purple new world requires that security organizations develop a shared understanding of the threats that pose the greatest risk to the organization."***

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

Pairing the thorough and detailed MITRE ATT&CK framework with an automated breach and attack simulation (BAS) platform like the AttackIQ Security Optimization Platform enables a security organization to routinely simulate the attacks that are most likely to threaten them. Red and blue teams can work together to design the testing regimen, jointly identify security control errors and gaps, undertake mitigation measures, and then re-test to validate that their security controls are effective.

First, though, the CISO and other security leaders must begin to shift toward purple. The transition is not simple. It involves building communication channels and fostering consensus and collaboration among groups of professionals who have historically seemed to operate on opposite sides of security testing strategy.

The effort will undoubtedly pose challenges, but the following four steps can help a CISO bring red and blue teams closer until their knowledge and perspectives begin to blend into a unified wall of purple.

# Step 1: Recognize the Strengths and Weaknesses of Each Group

> ***"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, then not conduct another test for a year until the company starts its next testing cycle."***

Red team testing simulates adversary behaviors to validate the effectiveness of specific security controls (composed of people, processes, and technology). Individuals who specialize in red team testing are threat emulation specialists. They cultivate a big-picture perspective of the cyberattack landscape so that they can adapt information from threat intelligence reports into safe, workable simulations that realistically test the controls of a specific organization.

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, then not conduct another test for a year until the company starts its next testing cycle. In this case, the organization's blue team may be responsible for implementing red team recommendations after the red team has already moved on. Even internal red teams cannot possibly cover all the organization's critical controls through manual testing processes. One customer relayed to us that their red team only ever tests 10 percent of the security controls in an organization. This is insufficient to guarantee cybersecurity effectiveness against advanced persistent threat actors that have the time, personnel, and resources to devote to a cyberattack campaign. Even if you have the best defenses on the market, if they are not tested and validated continuously, they will fail in an attack.

## Benefits of Blue

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

The trick is to harness that value. Both blue and red 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 its systems "pass" the red team's specific tests. This approach obfuscates the ultimate goal: to develop defenses that would successfully thwart the real cyberattacks the organization is likely to face.

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 stretched too thin — and the blue team may naturally provide a less-than-enthusiastic commitment to developing tests more likely to penetrate organizational defenses.

The blue team is also less likely than its colleagues in red to have the devious mindset of an attacker. Blue team members may in fact have a fairly shallow understanding of prospective adversaries.

## The Case for Purple

> *"For an organization to deliver effective cybersecurity, individuals with these diverse skill sets need to work hand in hand."*

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, blue teamers should turn to the red team for help in understanding what the 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 are a great learning opportunity.

For an organization to deliver effective cybersecurity, individuals with these diverse skill sets need to work hand in hand. The demands of guarding against rapidly evolving attacks have outstripped the ability of just one group to understand and adapt to the complete threat landscape. Siloed security functions 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.

Chief information security officers and security leaders should facilitate purple team collaboration, starting with building consensus on which attacks pose the greatest risk to the 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. As they do so, they can address 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 does our red team testing need to incorporate?
- How frequently should we repeat each type of test?

Participants can mine MITRE 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 both red and blue team members into alignment on how the company should approach threat-informed defense.

From there, the CISO can further support a burgeoning purple team by getting everyone in the same room and running table-top exercises to talk through a prospective breach or attack. Dialogue around attacker techniques, the 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 scope of threats that companies face is so broad that a red team relying on manual testing will necessarily have coverage gaps; it cannot routinely test the full panoply of TTPs the organization is likely to face. At the same time, one-off point-in-time tests fail to validate security controls on a continuous basis, so if a control gap opens up inadvertently, the red team may not notice for a considerable time.

## Automated Testing and Purple Team Operations (cont.)

Red team tests should focus the blue team on ensuring that its defenses perform as intended. But a testing regime will not achieve this objective if the tests do not operate at scale against enterprise security controls (to ensure sufficient coverage) and do not operate continuously (to ensure controls continue to work over time). Solving these problems requires automation — an automated security control validation solution that can simulate a wide range of attacks as frequently as the organization needs it to, without requiring extensive staff resources every time it runs.

> ***"An automated security validation platform that aligns with MITRE ATT&CK can simulate, on a regular basis, the most probable methods of adversary attack."***

An automated security validation platform that aligns with MITRE ATT&CK can simulate, on a regular basis, the most probable methods of adversary attack. These automated tests provide visibility into the performance of security controls on an ongoing basis, quickly alerting staff to any control gaps that arise. The blue team can use these test results to improve the overall effectiveness of the organization's defenses.

An automated platform 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 at that moment in time. Red teams may leverage an automated security validation platform to augment their manual testing. Blue teams may use it to supplement red team testing, especially if the red team is an external organization. Either way, automated testing should be a central feature of purple team operations.

# Step 2: Cultivate a Continuous Improvement Attitude

Some organizations' cybersecurity culture unintentionally pits the blue team against the red team. Blue teamers worry that a hard red team test might break key components of their security infrastructure. In fact, red team tests that adequately simulate real-world threats need to evaluate the effectiveness of not just technology, but also people and processes. Such an assessment is, 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 that they can bulk up the relevant defenses. Needless to say, attacks in the real world do not give advance notice, so alerting the blue team of an impending red team test is counterproductive.

Nobody wants to see their defenses breached. Nevertheless, both red and blue teams should look forward to attack simulations. They are not just a demonstration of the effectiveness of the organization's defenses. They are an opportunity for blue team members to learn where and how security should be improved, in a scenario where consequences are limited even if the attack succeeds. Far better to learn of control gaps through red team testing than as a result of an actual data breach or ransomware event.

## Step 2: Cultivate a Continuous Improvement Attitude (cont.)

*“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 required defenses.”*

But before blue teams can shift away from seeing tests as an activity to prepare for, with something to prove, they need confidence that management will not hammer them if the test reveals a control gap. CISOs and other leaders must set a consistent and supportive tone throughout the testing environment: security is difficult, and threats are dynamic. Validation of a control's ability to detect and prevent attacks — or discovery of a control gap — is critical to maintaining effective protection of the organization's infrastructure. 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 required defenses.

Moreover, that continuous improvement attitude needs to underlie the organization's overarching approach to attack simulations. A company will be able to fend off actual attacks only if all teams are committed to perpetual learning about strategies and tactics for strengthening the security infrastructure.

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

Once 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 an infrastructure that supports such assessments. As a starting point, the purple team should perform an audit of the current security infrastructure. It should document controls, as well as its understanding of the strengths and weaknesses in the organization's cyberdefenses. Then, the team should begin planning to test those assumptions.

Every organization needs a process for regularly and systematically identifying and mitigating security control gaps. However, the security team cannot defend against every possibility. Attempting to protect everything equally results in inadequate protection across the board. Thus, security strategy needs to focus on the subset of pertinent threats that are most likely to do the most damage.

As the organization develops its approach to controls assessment, the CISO must make sure the process focuses on those issues that expose the organization to the threats that the purple team previously identified as most critical.

## Security Assessments: A Program, not a Project

> *"The CISO should also ensure that assessments are viewed as a program, not a project."*

The CISO should also ensure that assessments are viewed as a program, not a project. Semi-annual or bi-annual testing is not adequate for a number of reasons. For one thing, the threat landscape is constantly changing as attackers refine their methods and experiment with new techniques. For another, the organization's defenses are likewise in perpetual motion. Configuration changes undertaken for an entirely different purpose might open a new control gap that is invisible in day-to-day IT operations. Infrequent point-in-time tests may allow a successful attacker to navigate around the network for weeks, or even months, before the breach is detected.

Instead of discrete testing periods, organizations need to roll out an ongoing program that operationalizes security testing; dovetails with the purple team's continuous improvement mentality; and results in frequent, incremental improvements to the effectiveness of controls. Whenever testing reveals a control gap, the blue team can make changes to strengthen the control. An immediate re-test 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 an automated testing platform like the AttackIQ Security Optimization Platform. It operationalizes attack simulations, enabling either red or blue teams to perform them as frequently as needed. In addition, AttackIQ improves the efficiency of assessments, freeing up valuable resources for more analysis and mitigation activities.

The Security Optimization Platform offers the added benefit of tight integration with MITRE ATT&CK. Its prebuilt templates streamline scenario testing of specific TTPs identified in the ATT&CK framework. And its integration of up-to-date threat intelligence about adversary TTPs facilitates threat-informed defense companywide.

# Step 4: Establish Clear Communication Flows Among Red Team, Blue Team, and Management

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

First, the CISO should ensure that linkages among red team and blue team members are built into a formal, structured feedback loop. Each test should conclude with a joint debrief, where purple team members reflect on which controls worked as expected and which attack techniques found gaps in organizational defenses. Remediation reports from an automated security control validation platform provide the CISO with clear visibility into the performance of the organization's security infrastructure.

# Step 4: Establish Clear Communication Flows Among Red Team, Blue Team,and Management (cont.)

> *"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."*

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

- What did we learn from this assessment?
- How well did our detection capabilities work?
- Are there any indications that we need to refine specific aspects of our testing program?

Turning the continuous improvement mindset toward the assessments themselves enables the organization to build and execute ever-more-difficult scenarios that provide a true view into the company's ability to defend against the most significant threats. Automation is key to bringing this vision of purple team optimization to fruition for any organization that faces staffing constraints.

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

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 take ownership of.

Another step in building purple synergies is aligning blue team 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.

# Conclusion

> *"And by taking a continuous improvement approach to optimizing the testing effectiveness, purple teams are providing their organizations the best possible defense against the ever-changing threat landscape."*

Leading corporate security functions are transitioning from a siloed fortress mentality of network defense to an approach that combines a purple team mindset with threat-informed defense. Everyone involved in the security assessment process — across traditionally blue teams, red teams, and management — is operating collaboratively, with full knowledge of one another's activities and capabilities. The teams are combining expertise to determine, together, which individuals or groups are most likely to strike their organization, what approach these attackers might take, whether the organization's current controls would be effective in preventing such an attack, and how to emulate and test those expectations.

Newly formed purple teams are using the AttackIQ Security Optimization Platform to incorporate automated breach and attack simulations, built on the MITRE ATT&CK framework and real-time threat intelligence, as a standard element of their day-to-day security operations. These routine assessments validate that security controls are effective. And by taking a continuous improvement approach to optimizing the testing effectiveness, purple teams are providing their organizations the best possible defense against the ever-changing threat landscape.

Learn more by taking one of the several AttackIQ Academy classes that focus on purple teaming.

ATTACKIQ®

U.S. Headquarters
171 Main Street Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com

**About AttackIQ**
AttackIQ, the leading independent vendor of breach and attack simulation 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 identify 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 MITRE Engenuity's Center for Threat Informed Defense.

For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.

© 2021 AttackIQ, Inc. All rights reserved. Confidential and proprietary. Do not distribute.