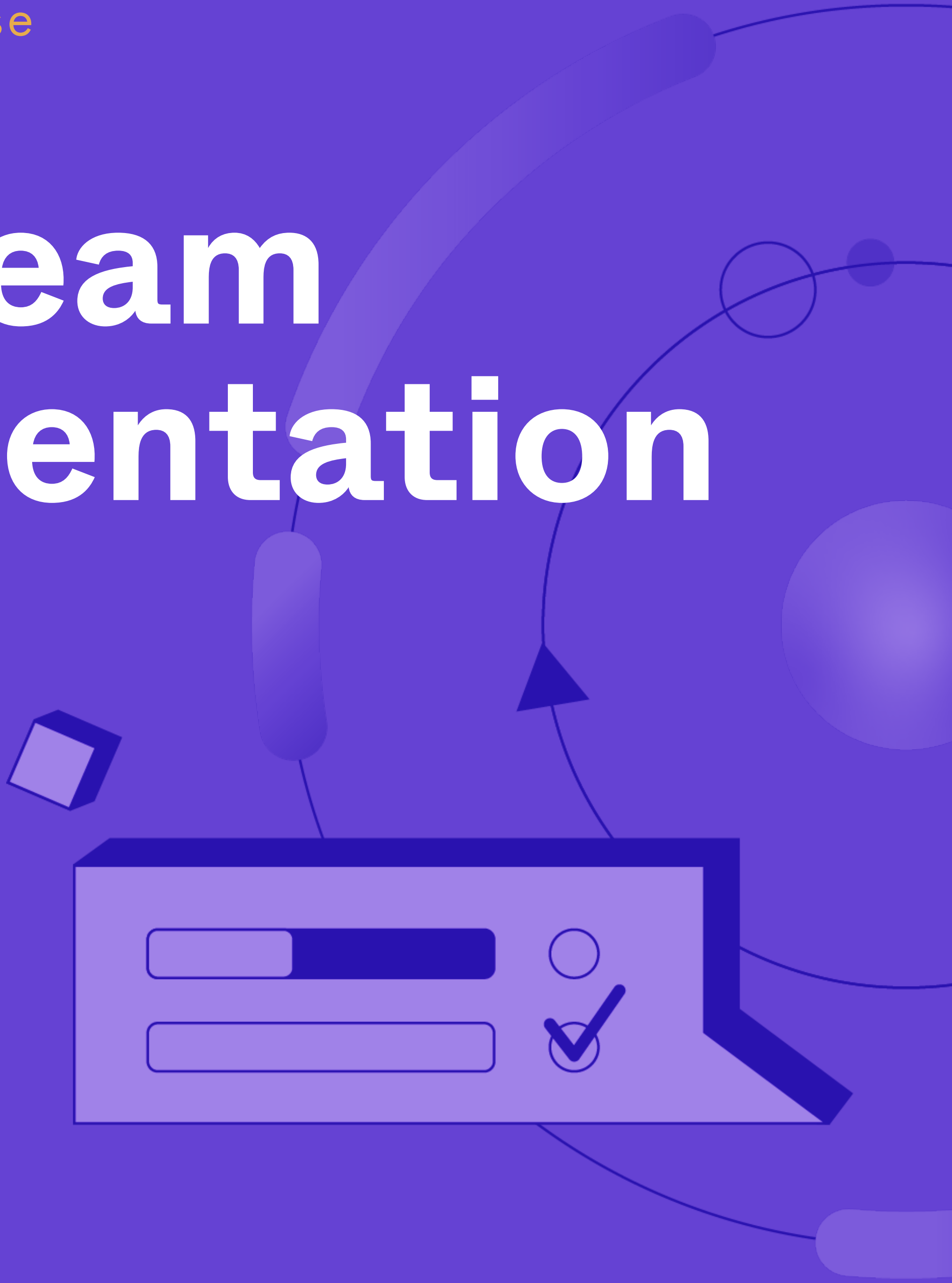
ATTACKIQ

Breach and Attack Simulation Use Case

Red Team Augmentation



Red Team Augmentation

Introduction: The Limits of Manual Red Team Testing

Effective cybersecurity requires coordinated teamwork. The goal of any cybersecurity program is to assure the confidentiality, integrity, and availability of the organization's data. In a traditional cyberdefense team in a mature organization, "blue team" network defenders focus their defensive operations on meeting baseline cybersecurity best-practices: correcting misconfigurations, administering patches, and deploying best-in-class commercial products.

Such traditional methods by no means guarantee success. If cyberdefenses are not oriented toward the most important threats, those defensive resources are wasted, and if they are not tested actively against probable threats, they are likely to fail when challenged by the adversary, letting the attacker slip past.

Security organizations have turned to "red team" and penetration testing to meet this challenge. Red teaming is the process of testing technologies, policies, systems, and assumptions by adopting an adversary's approach. Red team exercises include simulating multi-stage cyberattacks against specific targets on networks to simulate how an adversary might achieve a strategic effect, like stealing financial data, manipulating voter registration data, or destroying data to disrupt critical operations. Red teams pursue these objectives by adopting the tactics, techniques, and procedures (TTPs) of real adversaries.

Effective testing is thus a central part of the cybersecurity process. Red teams perform an important cybersecurity function by discovering faults in cyberdefense programs. The challenge is that red team testing is often episodic and the coverage delivered is therefore limited by personnel hours; the result is that coverage is unfortunately smaller than the scale of the security team's defenses. The delta between limited red team personnel and the scale of the blue team's defenses often leads to gaps in security control validation, resulting in decreased cyberdefense effectiveness.

For the U.S. government, this presents a risk given the nature and scale of the cyberthreat to sensitive government data. According to the U.S. government's General Accounting Office, the federal government faces many tens of thousands of security incidents annually, and increasing cyberthreats place continuous pressure on government security teams. Risks to critical government IT systems include insider threats as well as escalating nation-state threats from the governments of Russia, China, Iran, and North Korea, among others; they seek to destroy, manipulate, and disrupt data to achieve their national strategic goals. Developments in artificial intelligence, the widespread use of internet of thing (IoT) devices, and ubiquitous connectivity increase the potential risk.

In the face of an escalating threat, red teams can improve the efficacy and efficiency of their overall security control testing process with an automated breach and attack simulation platform that operates safely, at scale, and in production. The practice of using a breach and attack simulation platform to test defensive capabilities in concert with a red team is called red team augmentation. Red teams can methodically simulate the TTPs of an attacker using the MITRE ATT&CK framework, operationalized by AttackIQ's Security Optimization Platform. Successful red team augmentation helps the entire cybersecurity operations organization rapidly and efficiently improve cyberdefenses.

Case Study: A U.S. Federal Government Agency

In an important case study of red team augmentation, AttackIQ was approached by a federal government agency that already employed a highly skilled contractor to perform red team services against its core infrastructure, but wanted to improve their red team testing and security control validation process. It was essential to this federal agency that the red team help them identify and assure their network, system-level, and application-level security controls rapidly.

The red team's goals were to regularly present any identified defensive gaps to the blue team so that the techniques used in an attack could be rapidly assessed and mitigated. The blue team would seek to validate the success of this mitigation as quickly as possible. The red team would run test scenarios to determine if adversaries could exploit previously mitigated vulnerabilities. The agency was already implementing the MITRE ATT&CK framework, which was well-suited to enhanced red team operations, but not in a comprehensive and automated manner.

Understanding the Use Case

The Challenge

Because red teaming is predominantly a manual process, it is difficult to scale red team operations through spreadsheets and other shared documents about red team tactics. With this agency, there was some homegrown use of scripting tools, but the vast majority of the testing was driven from document-based lists and manual execution. It made the red team process slow and labor-intensive.

Red teams such as this one also face the challenge of the lack of a common lexicon; in the absence of a shared lexicon, red teams struggle to communicate across the security team about the threats and defensive capabilities required to mitigate them. Problems over the use of language and a shared understanding of the adversary's approach often contribute a loss of efficiency in red teaming. Security teams need to understand the red team's actions and understand, step-by-step, how the red team compromised the team's defenses using adversary tactics.

Scaling the Solution

By using MITRE ATT&CK in combination with AttackIQ's Security Optimization Platform, the federal agency's red team could deploy a common lexicon of adversary techniques through a single platform to improve cyberdefense effectiveness at scale. With AttackIQ's Security Optimization Platform, the red team was able to automate adversary attacks and generate real data about the team's performance. The red team maps its planned attacks directly from MITRE ATT&CK and AttackIQ's scenario library. The agency is now using MITRE ATT&CK in a mature, scaled manner as its single lexicon. With ATT&CK, the entire organization can qualify and discuss vulnerabilities and threat actors based on their activity. All of the red team's planswmincluding detailed attack scenarios, assessments, and objective reporting based on MITRE ATT&CK—are now automated within the AttackIQ Security Optimization Platform.

The red team can now execute tests and communicate the results and defensive recommendations through automated, detailed reporting across the organization. Security control performance data flows to the leadership team, the blue team, the security operations center (SOC), the intelligence team, and the incident response teams, giving everyone a single picture of cyberdefense effectiveness.

Conclusion

With the AttackIQ Security Optimization Platform, this federal agency has now augmented its red team testing operations through automation, driving down demands on the red team and freeing up highly skilled professionals to focus on complex problems. The agency can test and measure its security controls in a live production environment. With a strong foundation of data, the red team can tune its testing over time to make informed investment decisions about people, processes, and technologies. The cyberdefense team can rapidly analyze results to improve existing controls and identify where new controls are needed. Ultimately, AttackIQ's Security Optimization Platform allows red team personnel to focus on harder security problems across the organization that demand human attention.

By implementing red team augmentation using MITRE ATT&CK and the AttackIQ Security Optimization Platform, this federal agency saved its red team time and resources. The Security Optimization Platform supports comprehensive improvements to the red team's execution and reporting, and has materially improved communications between the red team and other cyberdefense team members. The net result: AttackIQ has improved the team's security effectiveness and reduced the agency's overall risk.

ATTACKIQ

U.S. Headquarters
2901 Tasman Dr. Suite 112
Santa Clara, CA 95054
+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 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 of Threat Informed Defense.

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