TAG CYBER

LEVERAGING OFFENSE TO IMPROVE CYBER DEFENSE USING SAFEBREACH

DR. EDWARD AMOROSO, TAG CYBER

SafeBreach

TAG CYBER

LEVERAGING OFFENSE TO IMPROVE CYBER DEFENSE USING SAFEBREACH

DR. EDWARD AMOROSO

To address modern cyberthreats to enterprises, organizations need a new paradigm of continuous security validation based on the simulation of offensive attacks to optimize cyber defensive posture. The SafeBreach platform exemplifies this breach and attack simulation approach to protect digital assets.

INTRODUCTION

Enterprise security teams today must address multiple dimensions of cyberthreats and must deal with an ever-changing and constantly expanding assortment of attack techniques. Frameworks such as MITRE ATT&CK help with this challenge, but even these models have trouble keeping up. Ongoing and active monitoring and analysis of attack methods represent good strategies for solving this problem.

In addition, security teams must deal with constant shifts in how they use enterprise technology. Most companies are experiencing a digital transformation, so how deployed security controls are configured and function will change frequently. Security teams must, therefore, continually probe and test the effectiveness of their controls to ensure that shifts in digital strategy do not undermine protection architectures.

In this article, we outline strategies for using cyberoffensive tactics to address these defensive challenges. In particular, we explain how a continuous security validation program powered by an automated breach and attack simulation (BAS) can provide increased visibility, risk reduction, remediation and resilience for cyber defense. We use the commercial SafeBreach platform to illustrate this practical cybersecurity approach in enterprise environments.

HOW IS SECURITY POSTURE MEASURED?

Board members, executives and other stakeholders in an organization frequently demand information about security posture. They often assume that the CISO and enterprise security teams will have mechanisms in place to provide both a qualitative and quantitative answer to this question. The good news is that metrics can be put in place to determine whether the posture is improving or degrading.

The industry has moved toward implementing BAS methods for continuous and automated measurement of security posture. The goal is to first provide visibility into the effectiveness of security controls so that immediate mitigation can be put in place to prevent negative consequences. The simulations must be done responsibly to ensure safety and security, which is a key tenant of BAS solutions.

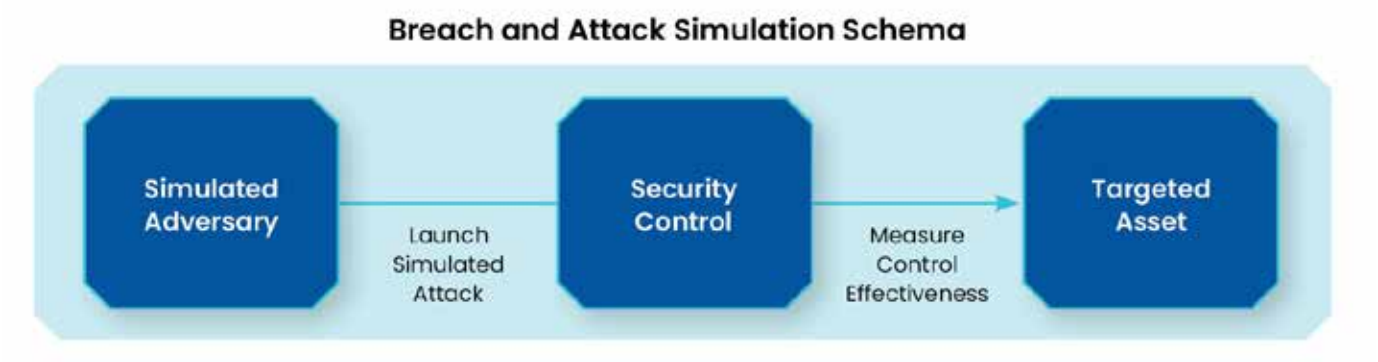

Figure 1. Breach and Attack Simulation Schema

Several advantages emerge for such BAS functionality, including continuous validation of how well certain security controls are functioning. Generally, BAS is integrated into the enterprise network infrastructure, but nothing would preclude a next-generation attack simulation from operating across organizational boundaries and perimeters in a zero-trust network environment.

HOW CAN OFFENSE BE LEVERAGED TO IMPROVE DEFENSE?

The cybersecurity community has come to recognize the necessity of continuous security validation, with the Cybersecurity and Infrastructure Security Agency (CISA) recently calling for organizations to enact a more automated, continuous approach to threat testing. This includes the ability to emulate and automate attacks based on a detailed understanding of common and emerging techniques used by malicious actors.

Such BAS-oriented visibility into enterprise security control effectiveness can be leveraged to support the following types of management initiatives:

- *Security Control Optimization*: This is one of the most powerful outcomes of an effective BAS program in an enterprise. Controls can be optimized by security teams based on outcomes observed during continuous testing and validation to close gaps or address misconfigurations to help with both security protection and framework compliance.
- *Vendor Accountability*: The use of BAS in an enterprise helps maintain accountability for commercial vendors. This not only reduces costs but also maximizes the value of deployed products and platforms, which when done properly, also minimizes the potential for "tool sprawl."

- *Rapid Response*: The ability to respond to threats more rapidly comes with a deeper understanding of and insight into security control effectiveness. Incident response teams can focus on weak spots highlighted by the BAS platform to determine lateral movements and attack paths. Vendors such as SafeBreach also provide service-level agreements to add attack coverage into the BAS platform based on new vulnerabilities.

- *Strategy Planning*: The overall security strategy and planning activities are influenced by the insights from continuous security validation with BAS. The level of visibility that BAS provides enables stakeholders to formulate long-term security plans and inform resourcing decisions. This can help justify security investments, support additional budgets for security teams and ensure strategic alignment across the organization.

Continuously validating the effectiveness of security controls has emerged as a mandatory action in most enterprise environments. The demand for ongoing insight into threat and risk is driven both by the senior-level executives and management teams, including the board, and the working-level practitioners. In the next section, we highlight the enterprise-level SafeBreach platform, which effectively implements continuous security validation for customers using BAS.

CASE STUDY: SAFEBREACH PLATFORM

Founded in 2014, the cybersecurity company SafeBreach offers a continuous security validation BAS platform. Enterprise teams use the SafeBreach solution to safely run attack scenarios against security controls and analyze results to understand gaps, prioritize remediation efforts and inform stakeholder communications regarding the efficacy of the security architecture, business risk and future needs.

The SafeBreach BAS platform uses a set of more than 25,000 offensive attack methods that collectively comprise its patented Hacker's Playbook™. The goal is to help enterprise customers validate the efficacy of their security controls at all layers of their protection architecture—and to do so independently at each stage of the defense process. The SafeBreach offering emphasizes the following areas:

- *Real-Time Validation*: Control monitoring from SafeBreach is done in real-time through its 24-hour service level agreement on all US CERT and FBI Flash alerts. Such real-time support allows teams to test new vulnerabilities immediately, which for modern enterprise teams is superior to the offline validation exercises that have characterized the security industry for many years.

- *Identifying and Prioritizing Risk*: Detecting gaps in coverage is also an important feature of SafeBreach. These gaps might involve localized gaps in functionality or policy for a given control, or they could involve broader shortcomings in the deployment of some required control. SafeBreach also enables teams to prioritize their remediation efforts.

- *Customized Reporting*: Reporting is one of the primary drivers for enterprise security teams to procure and deploy a commercial solution such as SafeBreach. The flexibility to customize reports to the local environment is an especially useful feature in the SafeBreach reporting implementation.

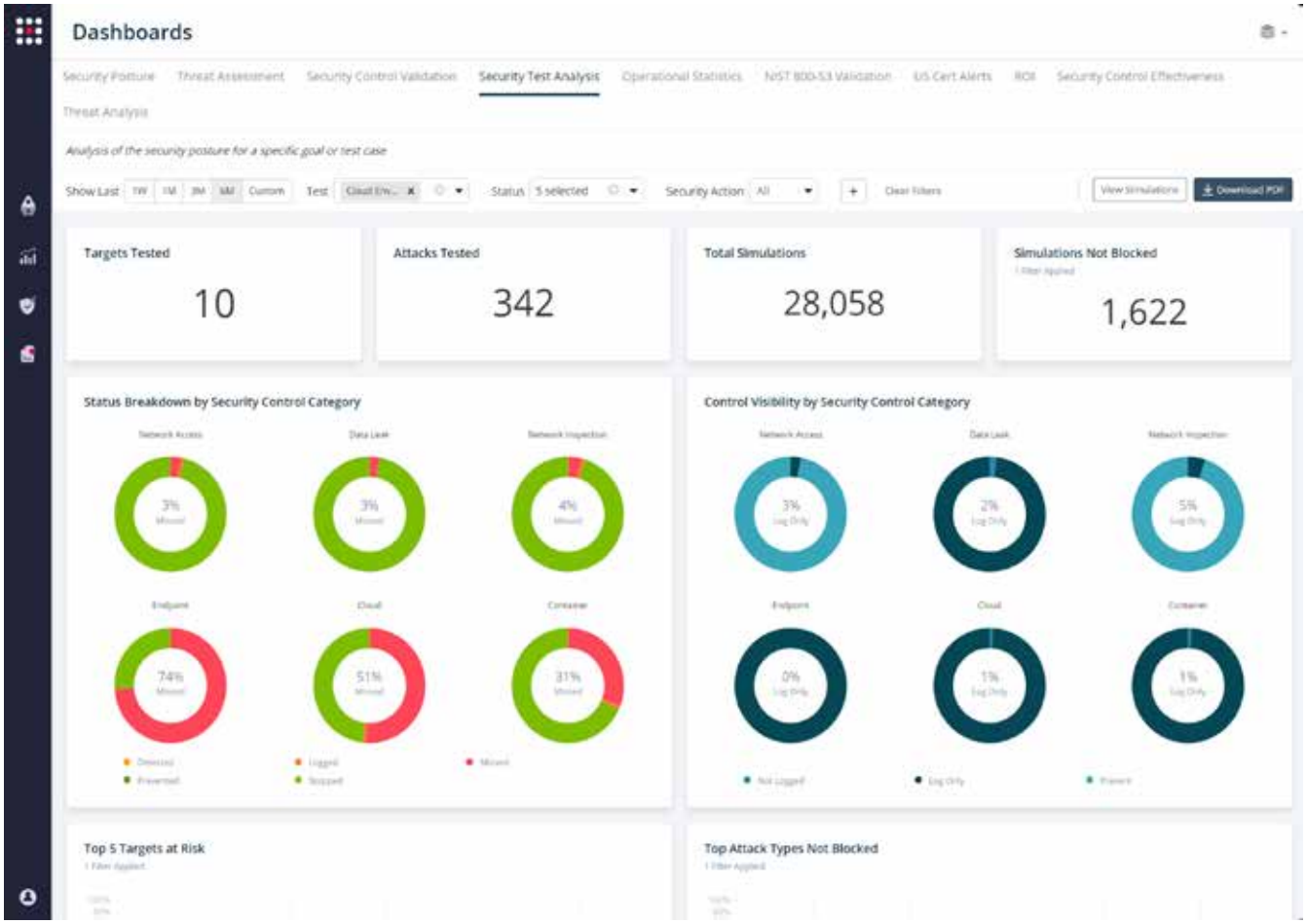

Figure 2. Sample SafeBreach Reporting Dashboard

The industry has clearly moved from viewing BAS as optional to viewing BAS as a mandatory tool to identify weaknesses in security controls. As a result, integration with other security solutions and platforms is an important feature. SafeBreach supports this evolution by including integrations with many major security vendors including Palo Alto Networks (Cortex SOAR) and Microsoft Advanced Threat Protection (ATP).

ACTION PLAN

Enterprise teams are advised to engage an action plan today to ensure they leverage this critical technology properly. While each organization will have a unique set of local management and technical approaches, every group will benefit by addressing the following list of tasks that collectively form an action plan that can lead to the effective deployment of BAS into the security architecture.

Step 1: Security Control Validation Inventory
Before BAS can be deployed, the security team must first identify how controls are currently validated, including control validation approaches such as penetration testing, enterprise security scanning and attack surface management. BAS solutions can complement or even reduce the need for these approaches, but action plans should always start with an understanding and documentation of what is presently deployed.

Step 2: BAS Solution Review

Next, the security team should select a BAS vendor. As discussed above, SafeBreach offers an effective platform for enterprise organizations that covers all major requirements, but buyers do have options. TAG Cyber's Research as a Service (RaaS) can support enterprise teams requiring detailed information on BAS vendors to ensure that the selected vendor properly integrates with their existing security infrastructure.

Step 3: Stepwise Deployment

Experience dictates that BAS deployments can be done in a stepwise manner, starting with a proof-of-concept implementation, and moving across the enterprise to cover additional portions of the network and additional controls. This is helpful because, unlike more complex platforms, BAS is relatively easy to deploy quickly and can begin deriving value immediately. TAG Cyber analysts are always available to assist enterprise teams with their planning.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and nonclients alike—all from a former practitioner perspective.