Unlocking Cybersecurity Budget with Breach and Attack Simulation

Introduction

One of the biggest challenges for cybersecurity leaders today is determining where to focus their teams' efforts. Astute leaders understand that they cannot address every possible cyber threat, therefore the first step is identifying the most critical risks to their organization, and determining the best solution to address these risks.

Unfortunately, many cybersecurity budgeting decisions are being made without concrete data. With actual data, security teams can demonstrate what's working, what's not, and show security trends over time, which allow teams to show return on investment, and provide the business case for budget increases in the future.

With this in mind, in this paper, we outline ways to unlock cyber security budget using Breach and Attack Simulation. Breach and Attack Simulation lets organizations simulate attacks to really understand their specific security risks -- where security is failing and where it is working. Breach and Attack Simulation platforms can be customized to run types of attacks that are applicable to a particular enterprise (ex: nation state, cybercriminals or script kiddie attacks), including data exfiltration of simulated data that represents the enterprise data at risk.

We will describe how to use Breach and Attack Simulation to unlock your cybersecurity budget. Specifically, we will use simulations to identify key risks, measure current posture, and select the right security solutions to increase your cybersecurity strength.

Who Should Read This WhitePaper?

- CISOs/CSO
- Director of Information Security
- Security practitioner

What You Will Learn:

- Breach and Attack Simulation (BAS) overview
- Using BAS to unlock cybersecurity budget
- SafeBreach technology overview

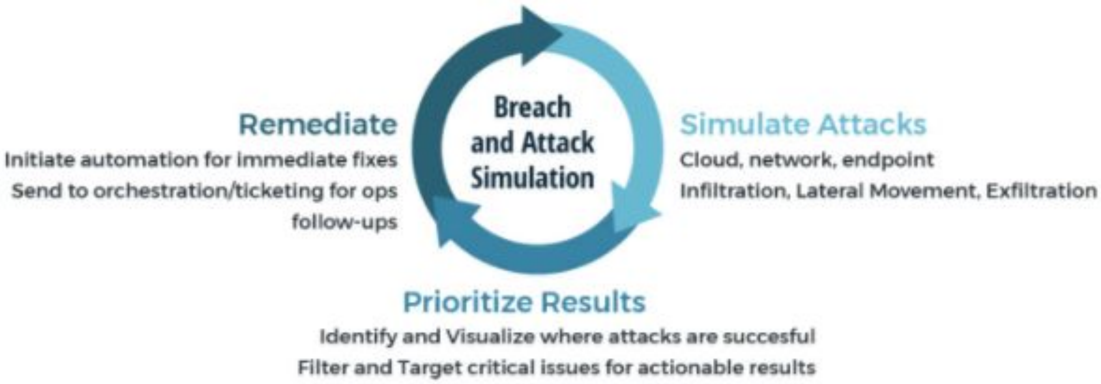
Overview of Breach and Attack Simulation

Worldwide information security spend is expected to be over $86B in 2017. The average CISO deploys between 50-75 different security products, and while these products are designed to thwart attacks, they can do so only if they are configured and deployed optimally. Security teams have limited cycles to spend on manual optimization, testing, and configuration - and thus, even the highest-spending teams end up with blind spots, weaknesses, and simple oversights that can be exploited by hackers.

Breach and Attack Simulation is a unique technology that takes advantage of automation and hacker techniques to validate that security controls that have been deployed correctly, and are working as expected. Gartner, in their Threat-Facing Technologies Hype Cycle in July 2017, said “The ability to provide continuous testing at limited risk is the key advantage of BAS technologies, which are used to alert IT and business stakeholders about existing gaps in the security posture, or validate that security infrastructure, configuration settings and prevention technologies are operating as intended.” In February 2018, Gartner Analysts Anton Chuvakin and Augusto Barros proclaimed that - “Breach and Attack Simulation (“BAS”) and Red Teams Will Kill the Pen Test”.

So what is Breach and Attack Simulation? It is simulation of actual hacker techniques, performed automatically and continuously, but in a safe way. This is accomplished via network and endpoint simulators that are deployed in critical segments to ”test” network and endpoint security controls. Both detection and prevention-based controls can be tested to ensure they are configured, optimized and working effectively for the best security.

Breach and Attack Simulation incorporates a continuous framework -- simulate, prioritize, remediate -- to test security controls in a dynamic enterprise environment.


Breach and Attack Simulation
Simulate Attacks
Cloud, network, endpoint
Infiltration, Lateral Movement, Exfiltration
Prioritize Results
Identify and Visualize where attacks are succesful
Filter and Target critical issues for actionable results
Remediate
Initiate automation for immediate fixes
Send to orchestration/ticketing for ops follow-ups

- **Simulate Attacks:** The first step for customers is to baseline their security controls and exposure. Breach and attack simulation executes thousands of attack simulations, to trigger security controls and alerting. Results show whether simulations are allowed/blocked (testing prevention controls) and pulls SIEM log data to validate detection controls.

- **Prioritize Results:** SOC teams review simulation results, and filter them based on built-in kill chain visualization, and simple clickable filtering based on attack type, size, risk, method, and much more.

- **Remediate Issues:** Once findings are prioritized per the above, results are automatically sent to ticketing systems or automation/orchestration platforms for remediation. Many teams send the findings to their SIEM as well. Once remediation occurs, the SOC team can rerun simulations, or the fixes will be automatically validated in the next simulation cycle.

Unlocking Budget with Breach and Attack Simulation

Despite breaches in the headlines, many organizations still struggle with prioritizing cyber security efforts against other business investments. The following are ways to take advantage of Breach and Attack Simulation to unlock and allocate security budget.

Use Cyber Kill Chain Information To Determine Efforts

It's important that you allocate new funds where they will bring your organization the most benefit. Breach and attack simulation will provide specific details on the methodology and the totality of the impact of a potential successful attack -- from infiltration, through lateral movement, to the data that can be exfiltrated.

The simulation results allow the security team to actually visualize the cyber kill chain. Depending on the results, organizations can choose to allocate cybersecurity budget towards the most effective solutions to "break the kill chain" with the least effort. This can often simply be adjusting configuration on existing controllers, or adding segmentation between parts of the network.

Audit Current Security Solutions

Before deploying additional solutions, security teams should audit the current security controls that they have in place. Having too many security solutions add complexity, and may lead to lack of visibility into what is actually needed to protect businesses. Additionally, some legacy security controls may not properly protect or detect advanced threats.

Before spending a penny on new security controls, Breach and Attack Simulation can be used to test the efficacy of current security solutions. In recent SafeBreach deployments (check out the SafeBreach Hacker's Playbook Report and Getting the Most from Your Next-Generation Firewall), organizations used Breach and Attack Simulation to validate segmentation policies and next-generation firewall deployments. By simply optimizing the configuration of security controls, retiring legacy or ineffective security controls, or consolidating those with overlapping capabilities, security teams can eliminate the need for further investment, reallocating budget to fill in any gaps that may still exist.

Measure ROI Over Time

An incredibly challenging metric for security teams is measuring ROI and trends over time. Are things getting better or worse? Are new investments living up to their expectations over time? Because Breach and Attack Simulation continuously and automatically executes attacks, and security controls are adjusted based on the results, over time, there should be improvements with the security posture of the company. These risk trends over time enables teams to continue to evaluate where they are improving and where they need to improve, and serves as the business case for new investments.

Security PoC and Cyber Shooting Range

One of the more interesting ways Breach and Attack Simulation is used to enable more cyber security budget is by proving a new technology actually works. Teams cannot just depend on a vendor's word; they need to actually run through testing. Breach and attack simulation enables teams to set up a cyber shooting range of sorts to run several vendors through a proof of concept testing. While this Breach and Attack Simulation use case doesn't follow the philosophy of "continuous validation", it can provide sufficient evidence to support a cybersecurity request to purchase vendor A over vendor B.

Validate MSSP or SOC Team SLAs

There have been many managed service provider horror stories where enterprises assumed their security was being monitored, but realized after an incident that it wasn't done properly. The same may be true of internal operations teams that may miss a particular issue for various reasons. Breach and Attack Simulation enables companies to ensure people, process and associated technologies that they depend on are working as expected by executing several attack scenarios and testing response. Any gaps that exist can then be identified and cybersecurity budget set aside to enable improvements.

Align to a Compliance Framework

Many businesses need to adhere to some type of risk and compliance framework like GDPR, PCI, or HIPAA. These risk and compliance requirements are typically tied to actual fines or financial implications. GDPR non-compliance can result in a fine of up to 4% of the company revenue. Security teams can utilize Breach and Attack Simulation to show how far away they are from complying to a specific framework. For example, Breach and Attack Simulation can prepare security teams for GDPR impact assessments by validating the efficacy of the security controls protecting personal data.

Check out the SafeBreach whitepapers on GDPR and PCI for more information about how Breach and Attack Simulation can help ease compliance and eliminate surprises in audits.

How Breach and Attack Simulation Works

A Breach and Attack Simulation software platform consists of a management console and software simulators that play the role of "virtual hackers". Simulators are deployed in segments across the network, endpoint and cloud, and execute a variety of breach methods -- brute force, exploits, malware, exfiltration. Because simulations occur only between simulators, there is no impact to users or the environment. At the same time, simulations will validate that security controls that should prevent or detect against these breach methods are working.

Here are things to look for in a breach and attack simulation platform:

1. Simulations that can be executed continuously and automatically every day without requiring "red team" expertise
2. Simulators supported for network, endpoint and cloud to provide the entire cyber kill chain perspective
3. Simulations should be executed at the actual atomic breach method level (i.e. not PCAPs) to reflect not only breaches in the headlines, but also variants chosen by future attackers
4. A comprehensive breach method playbook supported and continuously updated by offensive security experts
5. A true platform architecture that integrates with existing security ecosystem - threat intelligence, SIEMs, ticketing systems.

Unlocking Budget With Breach and Attack Simulation

Major Breach Risks

Boards and executives exposed to breaches in the headlines often want to understand whether current security controls will protect against attacks like Meltdown, Spectre, Hidden Cobra, Apache Struts, and SamSam. Instead of waiting for a data breach to be the first indication that security controls have failed, security teams can instead simulate high-profile attacks in the headlines using Breach and Attack Simulation to identify key challenges and ultimately determine budget that is needed to be proactive.

Takeaways

Cybersecurity investment is too often a “gut feel” based decision. Breach and Attack Simulation transforms security into a measurable business function. It enables blue teams, red teams, boards and executives to baseline their current security posture, decide where they want the program to be in a year, and mesure/track the progress and investment over time. Instead of just selecting security products that may fill a perceived gap, Breach and Attack Simulation quantifies with actual data which ones are working and where the gaps truly are. Additionally, by tracking trends over time, teams can show a clear return-on-investment to the board and executives, and justify their budgets in the future.

SafeBreach Breach and Attack Simulation

Simulate attacks across the kill chain including infiltration, lateral movement, and exfiltration

Initiate immediate remediation with SIEM, orchestration and ticketing systems

Find unknown exfiltration routes for data such as PII, credit cards, and source code

Bolster your offensive security with a playbook of thousands of attack and breach methods

Execute new and evolving attacks from a dedicated internal threat research team

SafeBreach

SafeBreach is a pioneer in the emerging category of breach and attack simulation. The company's groundbreaking platform provides a "hacker's view" of an enterprise's security posture to proactively predict attacks, validate security controls and improve SOC analyst response.

SafeBreach automatically executes thousands of breach methods from an extensive and growing Hacker's Playbook™ of research and real-world investigative data.

Headquartered in Sunnyvale, California, the company is funded by Sequoia Capital, Deutsche Telekom Capital, Hewlett Packard Pathfinder and investor Shlomo Kramer.

For more information, visit www.safebreach.com or follow on Twitter @SafeBreach.

111 W. Evelyn Avenue
Suite 117
Sunnyvale, CA 94086
408-743-5279