SafeBreach

TEN THINGS TO LOOK FOR IN A BREACH AND ATTACK SIMULATION PLATFORM

A SafeBreach Whitepaper | www.safebreach.com

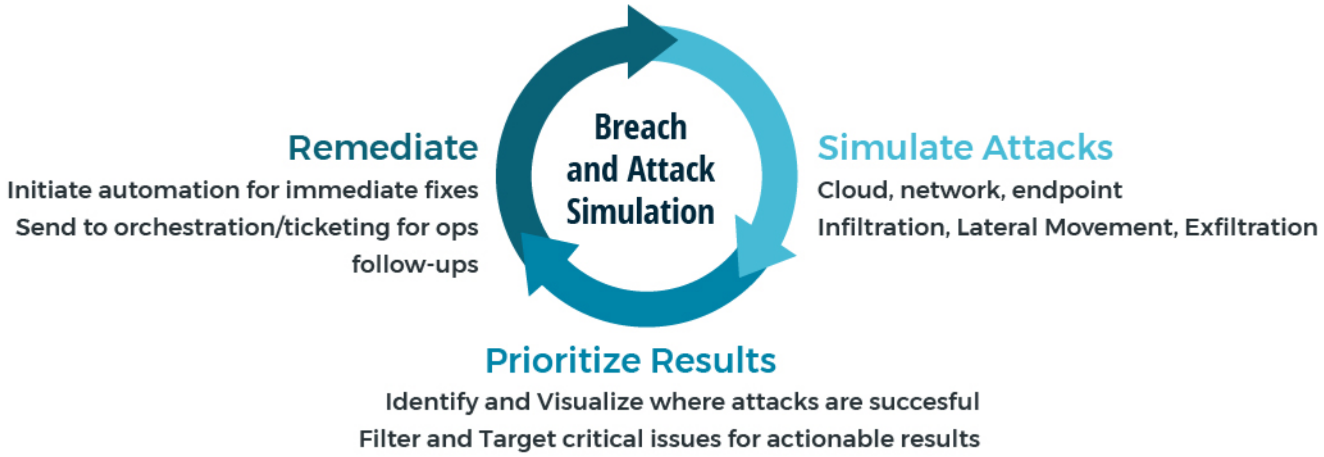
BILLIONS HAVE BEEN INVESTED IN CYBERSECURITY, BUT ATTACKERS STILL HAVE THE UPPER HAND.

Successful breaches are a daily occurrence, and security teams are under ever-increasing pressure to defend against thousands of new and existing attack techniques.

Existing security controllers can thwart attacks, but only if they are configured optimally, and working together to build defense-in-depth. 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.

This paper highlights the top ten features to look for in a Breach and Attack Simulation platform, five key use cases that can help to drive evaluation criteria, and a checklist for executing proof-of-concepts or evaluations.

BREACH AND ATTACK SIMULATION OVERVIEW



Remediate
Initiate automation for immediate fixes
Send to orchestration/ticketing for ops follow-ups

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

Breach and Attack Simulation automates attack techniques to validate the true effectiveness of security controllers. Rather than relying on default configuration, or hoping that policy has been written to address every eventuality, Breach and Attack Simulation allows security teams to:

- **Simulate Attacks:** Unleash real attacks on production environments just like attackers do, but without harm or impact, to identify where defenses are working, and where they are failing.
- **Prioritize Findings:** Quickly identify the right areas to focus on to stop the attacks most critical to your business.
- **Remediate Security Gaps:** Provide a seamless integration with operations teams or automation solutions to update configuration or otherwise block attacks, to incrementally improve overall security posture and effectiveness against threats.

Thanks to automation, Breach and Attack Simulation works continuously, and at incredible scale to simulate attackers and identify weaknesses in real time. This new approach enables data-driven security planning, minimizes exposure, and proactively identifies both where security is working, and where it needs to be bolstered.

Validating and remediating defenses with Breach and Attack Simulation ensures that security is working as intended, and that teams are getting the most out of their investments. However, like anything else, not all solutions offer the same abilities. Read on to see the ten things to look for in a Breach and Attack Simulation platform to best validate your security, prioritize your findings, and guide remediation.

1. SIMULATE ATTACKS ACROSS THE ENTIRE KILL CHAIN

Attacks don't stop once they break through the corporate perimeter. The best solutions safely validate every level of production security, in actual production environments. When investigating and evaluating solutions, ensure that the platform performs network and endpoint breach methods (i.e more than packet captures), across infiltration, lateral movement and exfiltration. And of course, you must be able to visualize blocked and successful attacks based on stage, as well as segment, to easily identify the most effective methods to break the kill chain and stop attacks.

The following are just two examples of how attacks are executed across the kill chain. Ensure your Breach and Attack Simulation platform can simulate attacks at this granular level.

RANSOMWARE

Infiltration/Inbound

1. Initial malicious payload downloaded to a host
2. Payload deployed on local disk

Lateral Movement

3. Worm attempts to move laterally within a network
4. Attempts to install to disk on various other hosts

Exfiltration/Outbound

5. Malware attempts to communicate outbound to Command and Control for cipher and "unlock" commands

DATA AND CREDENTIAL THEFT

Infiltration/Inbound

1. Initial dropper payload downloaded via HTTPS to end-user laptop
2. Initial dropper payload executed and install to disk

Exfiltration/Outbound

3. Dropper calls outbound across multiple protocols and ports for further malicious payloads

Infiltration/Inbound Phase 2

4. Payloads are sent internally as malware identifies appropriate LAN traffic to hijack

Lateral Movement/Replication

5. Rogue automated tasks scheduled on local machines via PowerShell

Exfiltration/outbound phase 2

6. Periodic screenshots, and keylogger data sent outbound to rotating command and control
7. Hashed and clear-text credentials scraped and sent to command and control

Some Breach and Attack Simulation tools are little more than automated penetration testing - a small set of attacks, aimed at penetrating the network perimeter. But real attackers work across environments and systems to establish footholds, and find data with the highest value. To best prove defense against real attacks, Breach and Attack Simulation must execute simulations from the outside in, within networks, and even within and between hosts. And of course, at no point should endpoints, applications, or networks be taken down or disrupted for validation.

2. RUN CONTINUOUSLY

Breach and Attack Simulation should run continuously, to not only establish a security baseline, but also to ensure that ongoing maintenance and updates don't introduce new risk. Many solutions claim to be continuous, but are actually simply small tests that must be scheduled individually or by group, and lack scale for both validation as well as prioritization of findings.

RUNNING CONTINUOUSLY SHOULD ENABLE SECURITY TEAMS TO:

1. Measure high-level, and specific, security posture over time
2. Reduce exposure time by identifying issues immediately, and proactively
3. Eliminate human testing biases, and uncover unknown or unexpected security issues

Running continuously is more than just the ability to schedule simulations, or script attacks. The right solution should not need any dedicated headcount, should not require manual creation or running of methods, and should have no production impact. Without real automation, non-continuous solutions are no more effective than one-off penetration testing.

3. SHOW RISK TRENDS OVER TIME

Part of the value of Breach and Attack Simulation is the ability to create and execute real, data-driven security strategy, rather than just a series of reactive tactics. Look for solutions that provide security trending that will prove the effectiveness of security to board members and executives. With the right solution, you should be able to show risk trends over time, and prove that security investment is making a measurable difference. This can help substantiate budgeting, and ensure that security team leaders maintain an executive presence akin to sales, marketing, or any other data-driven function within an organization.

4. HAVE A LARGE, TRUSTED SET OF ATTACKS SUPPORTED BY LEADING RESEARCH

Unlike penetration testing or red team exercises, Breach and Attack Simulation should be able to validate security at scale. This means, of course, that security teams should look for large sets of attacks that they can rely on for simulations. However, it's also critical that the attacks are developed and tested by a reputable, industry-recognized team. Look for solutions with dedicated security research teams, recognized in the industry for advancements in attacks, and trustworthiness. When it comes to unleashing thousands of attacks on your network, crowdsourcing might not be an option you're willing to trust.

5. VALIDATE SECURITY AGAINST KNOWN ATTACKS

With so many breaches making headlines, it's more critical than ever to be able to prove security to board members, executive teams, and other stakeholders. Breach and Attack Simulations should be able to quickly and easily prove whether or not your defenses are ready to withstand headline attacks, or custom attacks that target your industry or vertical.

Ask vendors to prove how well they support new attacks. Look for SLAs around new attack creation, as well as proven public records of updates and new methods. In addition, the best solutions should have SLAs for custom attack creation as well, should your team identify new or emerging threats that need simulating.

6. IDENTIFY SECURITY BLIND SPOTS AND "UNKNOWN UNKNOWNS"

Known attacks must be defended against, but of course, every new attack also poses a threat. Breach and Attack Simulation should allow your teams to validate security against both the known, and the unknown.

Make sure your solution doesn't require your team to manually assemble every single attack scenario - as doing so not only takes dedicated team members, but also only validates against what your team thinks up. Instead look for solutions that allow for custom attacks, but also automatically validate your defenses against unpredicted, or unexpected attacks, without requiring hours of manual setup and maintenance.

7. WORK LIKE REAL ATTACKERS

Attackers are relentless. While script kiddies might just run scripts from an off-the-shelf exploit kit, even a moderately advanced attacker will pivot and adapt to thwart defenses. Since attackers don't try a few methods and then stop, neither should your Breach and Attack Simulation platform.

Look for simulated attacks that are granular and modular, not simply static PCAP recordings for specific moves. To accurately simulate an attacker, Breach and Attack Simulation must pivot and adapt, automatically running attacks over different ports, protocols, and machines, trying every avenue to find weakness. Look for solutions that are built to evolve to support future attacks, future security solution, and emerging technologies like IoT.

When testing various Breach and Attack Simulation solutions, evaluate the depth of the various attacks. While a small subset may seem easier to manage, it can lead to a false sense of security, or leave blind spots that attackers will exploit.

8. INTEGRATE WITH EXISTING TOOLS AND PROCESSES

Extensibility and integrations to ensure that your team gets the most from any Breach and Attack Simulation solution. Of course any solution should provide value on its own, but taking a platform approach ensures that a solution can grow in value, and effectiveness. When evaluating various solutions, it's important to look at both inbound and outbound integrations for maximum value.

Inbound integrations should include the ability to consume and weaponize Indicators of Compromise (IoCs) from Threat Intelligence providers. This not only increases the scale of simulated attacks, but also ensures validation against new and emerging threats from "the wild."

Outbound integration should include tools that can help your teams both prioritize findings, as well as act upon them. Findings data should easily be passed to visualization tools or business intelligence platforms, to help identify how best to prioritize fixes. Likewise, remediation should be tied closely to existing orchestration platforms or ticketing systems to mesh well with operations teams' processes. Perhaps simplest of all - integration with automation tools can provide true closed-loop security, where Breach and Attack Simulation identifies weaknesses, sends them to an automation platform, and those weaknesses are addressed across controllers automatically. This kind of closed-loop operation ensures that any new findings can be resolved quickly and without the risk of human error - greatly minimizing exposure time.

Additionally, look for integrations with SIEM. These should be both inbound (pulling data that shows what alerts have fired, as well as which controllers did or did not stop an attack), and outbound (pushing findings for content and alerts).

9. PROVIDE ACTIONABLE, PRIORITIZED RESULTS

Perhaps most critically of all, Breach and Attack Simulation should give your team a faster, easier, and more effective way to prioritize ongoing security effort. Breach and Attack Simulation should provide the ability to quickly slice through results to identify the weaknesses that are most critical to your business, and guide teams on how to fix them.

Make sure you can easily identify a prioritized set of actionable results, and work those down in a manageable way. Look for reasonable filters to sort and prioritize, and ensure that you invest in a solution that integrates with operations team workflows (such as ticketing systems) as needed, and can also extend remediation directly to controllers with automation for true closed-loop security.

Breach and Attack Simulation should make security more effective, with less effort - not more. Ensure that findings are actionable, and that you can prove the value of security investment over time.

10. BE SAFE ENOUGH FOR DEPLOYMENT IN PRODUCTION ENVIRONMENTS

Validating security outside of production is useful as a tabletop exercise, or proof-of-concept, but the best Breach and Attack Simulation solutions can be deployed directly into production environments, without risk of data loss, credential leaks, or endpoint destruction. Look for solutions that work within production without caveats, and without risk. Validate where you want to store simulation findings - on premises, or in the cloud. Lastly, ensure any malware testing is performed in a way that doesn't require sequestered machines, quarantine zones, or offline environments, to prevent malware infection.

USE CASES FOR BREACH AND ATTACK SIMULATION

Starting with the right goal in mind can help drive evaluations to ensure the right solution is found. Below are some examples of key benefits that can help guide evaluation.

- **Get more from existing security**
  Security controls are incredibly flexible, but are often deployed with generic "one-size-fits-all" policy recommended by vendors, or configured once and never revisited. Breach and Attack Simulation safely simulates thousands of attacks to see which policies are effective, which need updated, and where holes exist. By optimizing config and ensuring controls work in concert, security teams can get the most from existing security investment.

- **Minimize security exposure**
  Enterprise environments are far from static—constantly updated to meet the needs of the business, and to stop new and emerging attacks. However, all this configuration often leads to simple oversight, or human error, that can introduce risk. Thanks to continuous validation, Breach and Attack Simulation identifies new exposure in hours, so security teams can minimize exposure time and prove the effectiveness of new configuration.

- **Prepare for audits**
  Annual penetration test and compliance audits bring stress and risk for CISOs and security teams. These tests often result in a list of findings that's too long for operations to address, and is only representative of a small window of time before changes to the environment make it obsolete. Breach and Attack Simulation runs continuously, to find risks well before audits, and smooth the process of maintaining compliance.

- **Test alerting and action plans**
  Every security team knows that defenses are build from people, processes, and technology, but often the technology receives all the focus. By simulating attacks, SOC and MSSP teams can perform breach scenario training before a real attack occurs, to validate action and alerting plans. Provide business rationalization Security investment is too often a "gut feel" based measure, and too often executive teams only start deep security investment after breach has occurred. Breach and Attack Simulation can provide real security data, to justify further security investment, or to address the growing issue of proving security against headline attacks.

- **Provide Business Rationalization**
  With Breach and Attack Simulation working continuously, security teams will have the data they need to improve and maintain security, without guesswork, or reliance on vendor claims. Start with the right goals in mind, and you'll be able to leverage the power of automation to get ahead of attackers.

CHECKLIST: ASSESSING BREACH AND ATTACK SIMULATION

1. SIMULATE ATTACKS ACROSS THE ENTIRE KILL CHAIN

□ Does the solution validate more than simple network moves (i.e more than packet captures)?

□ Can you see all attacks, visualized by kill chain, to prioritize remediation easily and quickly?

□ Can the system actually simulate attacks across the entire kill chain, all the way down to host-level disk, without risk?

□ What data is moved between nodes/simulators?

2. RUN CONTINUOUSLY

□ How much effort is required to run continuously?

□ How easily can findings from continuous validation be prioritized, and acted upon?

□ What integrations exist for automating remediation to minimize exposure windows?

3. SHOW RISK TRENDS OVER TIME

□ The platform should show risk trending across the kill chain.

□ How easily can you identify newly introduced risks, and correlate them to specific attacks?

□ Can you prove the value of security controllers to executive staff, board, finance, etc by showing effectiveness, and improvement over time?

4. HAVE A LARGE AND TRUSTED SET OF ATTACKS

□ How many attacks exist?

□ How often are they updated?

□ Who creates and updates the attacks, and how are they guaranteed to be safe for production deployment? Are they crowdsourced, or built in-house?

5. VALIDATE SECURITY AGAINST KNOWN ATTACKS

□ How well does the vendor support new attacks?

□ Is there an SLA for custom or requested attack creation?

□ What's the published record for new attack updates and additions?

6. IDENTIFY SECURITY BLIND SPOTS AND “UNKNOWN UNKNOWNS”

□ Do attacks have to be manually created for every scenario?

□ How easily can you validate defenses against unpredicted attacks, or find unexpected weaknesses in your defenses?

7. BE MODULAR, AND WORK LIKE REAL ATTACKERS

□ Are simulated attacks granular and modular - i.e. are they simply static recordings for specific moves, or will they pivot and adapt like a real attackers do?

□ Will the platform automatically run iterations of all various attack scenarios, or does that require manual intervention?

□ Does the platform scale to support both emerging attacks, as well as emerging hosts/technologies like IoT?

8. PROVIDE ACTIONABLE, PRIORITIZED RESULTS

□ How easily can you identify a prioritized set of actionable results?

□ Do filters exist for sorting and prioritizing?

□ What integrations exist for external processing/analytics/visualization?

□ Do integrations exist for automated remediation?

□ Can you prioritize by phase of kill chain, ease of remediation, sophistication of attack, rate of leak, etc?

9. INTEGRATE WITH EXISTING TOOLS AND PROCESSES

□ Can the platform consume and weaponize Indicators of Compromise (IoCs) from Threat Intelligence providers?

□ Can findings data be easily be passed to visualization tools or business intelligence platforms?

□ Can findings data be tied closely to existing orchestration platforms or ticketing systems to integrate with operations teams’ processes?

□ Does the platform integrate with SIEM both inbound (pulling data that shows what alerts have fired, as well as which controllers did or did not stop an attack), and outbound (pushing findings for content and alerts)?

10. BE SAFE ENOUGH FOR DEPLOYMENT IN PRODUCTION ENVIORMENTS

□ Are endpoint tests destructive and/or do they risk infecting your network with real malware?

□ Is any real data, including host user credentials, ever compromised, moved, or sent to the cloud?