Quick Answer: What Are the Top Use Cases for Breach and Attack Simulation Technology?

Published 24 February 2021 - ID G00726662 - 5 min read

By Analysts Mitchell Schneider, John Collins, Craig Lawson, Jeremy D'Hoinne

Initiatives: Security Operations

Breach and attack simulations technologies can address a variety of use cases for security and risk management teams; however, buyers focus on a few common use cases. SRM leaders should determine whether these solutions will help their organizations improve their overall security postures.

Quick Answer

What are the top use cases and reasons why organizations procure and leverage breach and attack simulation (BAS) technology?

- Run the attack simulation tools to gain visibility into whether and where there are gaps in their defenses and to figure out how to optimize existing security technology deployments.

- Use attack simulation to achieve a more automated and scalable attacker's view of their environment.

- Use BAS as a toolkit for red teams by running attack simulations, replicating the approach and methods of real threats in a safe manner, automating repeatable tasks, then allowing organizations to focus on more-sophisticated campaigns.

- Identify and prioritize remediation activity for the riskiest assets in the environment, what vulnerabilities organizations have and how (and whether) that can be leveraged by threat actors to penetrate the IT environment.

- Deploy BAS in an acquisition target's environment to obtain visibility as to how secure the organization is as part of due diligence activities or planning for Day 1 activities or soon after acquisition.

This list of use cases is not exhaustive. As the market is maturing, vendors add new features expanding the scope they cover, and including more aspects of the cyber kill chain.

More Detail
When engaging the BAS market, security and risk management (SRM) leaders should think about questions such as, “What would it look like if threat actor ‘X’ breached our environment?” and “How would an attacker take advantage of any security gaps and/or risks (e.g., high-risk vulnerabilities)?” Understand that remediation could be relatively extensive packages/projects in terms of time and execution. Knowing is not enough, and the wisdom comes from making the recommended improvements in the areas described below.

- **Security control validation/efficacy:** This is the core function for BAS tools. Gaps may be due to poorly configured security controls or a lack of security controls, or inadequate processes and procedures. These simulations also assist teams trying and to figure out how to optimize existing security technology deployments. The simulation approach is designed to show whether current security technologies are configured properly to:
  - Detect active threats
  - Provide detailed and often prescriptive guidance on where existing security controls have issues
  - Provide assessment of the activities that security operations teams can do prior to a breach to better prevent, detect and respond to threats of that nature in the future
  - Test any configuration or updates to products to ensure that there has been no configuration creep that would highlight new or unforeseen gaps in security controls having been introduced

- **Security posture assessment:** Organizations use attack simulation to get more automated and scalable attackers’ views of their environments. For example, a blue team could use the BAS tool to emulate a specific threat actor without having to engage with a red team. They would be able to see the results from the simulation and react accordingly. Depending on the vendor, the organizations can get a detailed attack path, highlighting lateral movement and attack steps to a key target that were able to be successfully executed (or not). Alternatively, many BAS vendors leverage the MITRE ATT&CK framework to build dashboards that enable them to categorize the findings and facilitate a discussion about gap reduction.

- **Penetration testing:** Penetration testing is often performed at a point in time, as well as having a specific scope that covers only a small portion of an environment. Although it is not a replacement for this type of expert testing, BAS lets an organization drastically increase the scope and frequency of this type of active testing. It operates in ways similar to how vulnerability assessment (VA) tools do, so simulations (e.g., VA scans) can be configured to run at a point in time or, ideally, at regular intervals to ensure that organizations always have a more up-to-date picture of their posture to detect/repel cyber exposure.

- **Support red team activities:** BAS can be leveraged as a toolkit for red teams. Organizations can run attack simulations, replicating the approach and methods of real threats in a safe manner, as well as automating repeatable tasks. This enables organizations to focus on more-sophisticated campaigns.
- **Risk-based vulnerability management**: BAS technology offers functionality to identify and prioritize remediation activity for the riskiest assets in the environment, what vulnerabilities organizations have and how (and whether) that can be leveraged by threat actors to penetrate the IT environment. Because BAS is focused on giving visibility to the organization's cyber risks, some Gartner clients have asked if BAS will replace VA technology. However, BAS and VA tools are complementary technologies that provide overlap with traditional vulnerability management tooling.

- **Mergers and acquisitions (M&A)**: An emerging use case for leveraging BAS technology is to deploy BAS in an acquisition target's environment to obtain visibility around the target's security. However, it should be noted that most organizations typically use BAS solutions right after the M&A to spot discrepancies and to get a first assessment, because organizations do not typically have access to the environment before Day 1 for any sort of technology implementation. The process can provide visibility of any security tools already being used, then assist with decisions on which tools to keep and replace after the M&A.

When selecting a BAS solution, SRM leaders should avoid confusion around the different types of security testing products. BAS tools will run simulations in a continuous, consistent and automated manner. In addition, they assess things, such as whether or not the network segmentation is working, and ensure that the security tools are blocking what they are supposed to and detecting what they should be detecting. At the same time, they cover multiple, if not all, stages of the cyber kill chain (see Figure 1). They can also be used from a "threat or threat actor" perspective, where you may want to answer a question such as, "How would APT29 (Cozy Bear) breach my environment?" BAS can be used as a supplement to table-top exercises for this exact use case.
Figure 1: BAS Defining Features

BAS Defining Features

- Automated
- Consistent
- Continuous
- Cyber Kill Chain

Source: Gartner
725662_C

Recommended by the Authors

- Hype Cycle for Security Operations, 2020
- Utilizing Breach and Attack Simulation Tools to Test and Improve Security
- Using Penetration Testing and Red Teams to Assess and Improve Security
- Implement a Risk-Based Approach to Vulnerability Management
- Cool Vendors in Security Operations and Threat Intelligence, 2H20