A CISO'S Guide to Breach and Attack Simulation (BAS) Platforms

ATTACKIQ®

Contents

Notice

AttackIQ® publications are made available solely for general information purposes. The information contained in this publication is provided on an "as is" basis. Any additional developments or research since the date of publication will not be reflected in this report.

What is Breach and Attack Simulation (BAS)?

Breach and Attack Simulation technology allows enterprises to automatically simulate the full attack and expanded kill chain used by cyberattackers against enterprise infrastructure using software agents, virtual machines, and other means. BAS allows you to understand the detailed status and performance of your security controls and processes as well as the personnel that support them.

BAS allows you to find the performance gaps, strengthen your security posture, and improve your incident response capabilities. BAS assesses readiness and validates that your enterprise security systems are performing as originally intended.

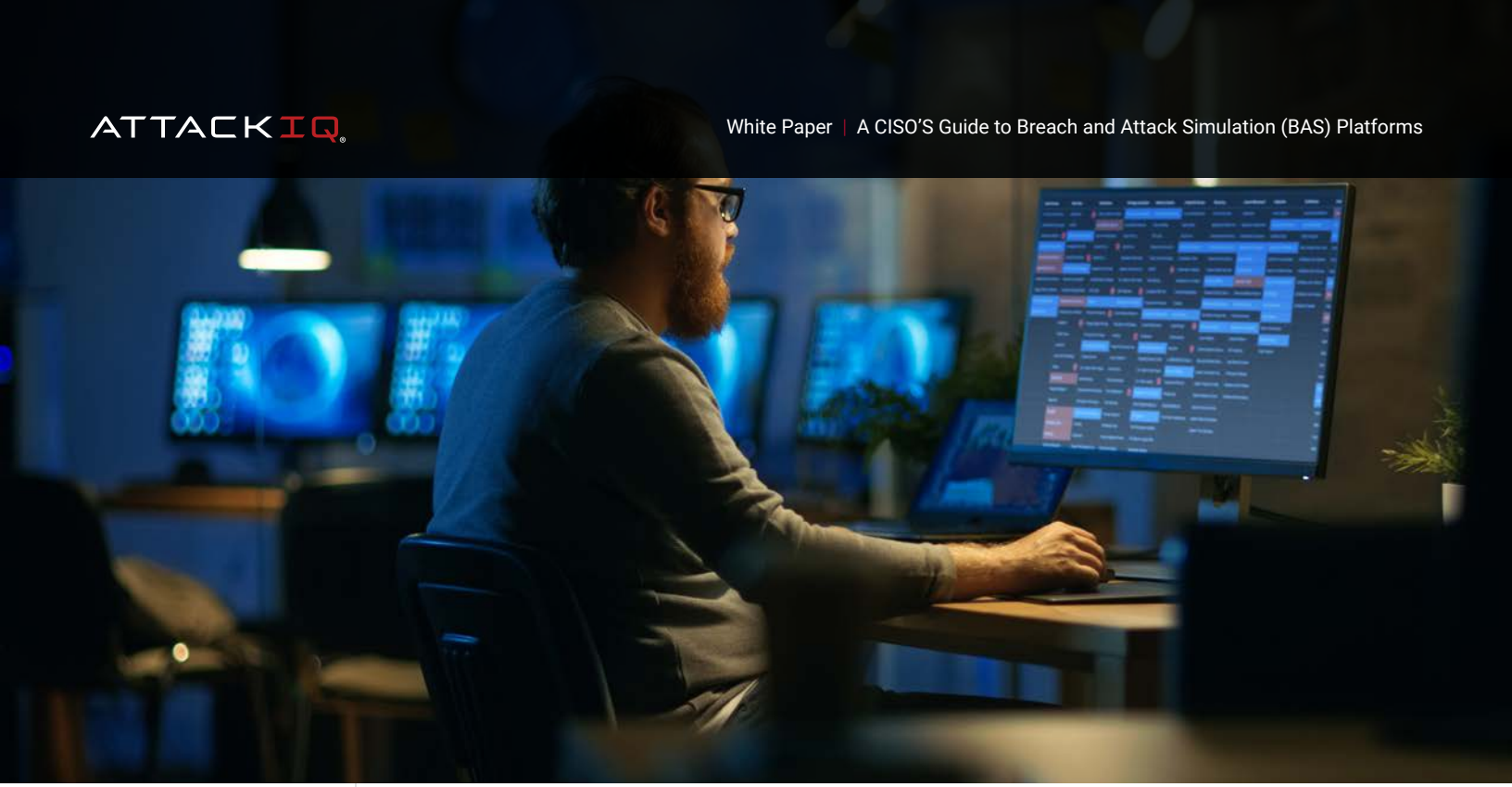
BAS platforms provide automation that enables the platforms to work autonomously and to scale to support the largest global enterprise. Support for live production environments enables you to see in real time how changes to configurations or administration can open new vulnerabilities in your cyberdefense.

Why is BAS Important and Compelling for CISOs?

BAS can help CISOs answer the most difficult questions they face today with objective data that is otherwise virtually impossible to find. By the time you complete reading this white paper, you will understand how BAS will help you answer these questions. Most CISOs cannot answer the majority of these questions today.

Let us look at some of the most difficult questions that CISOs face:

- Are my security controls working as expected at this moment on my production systems?
- Are my security controls configured properly to do what I expect them to do?
- Threat intelligence has identified several threats that are likely in our industry - do my security controls protect against these new threats? If not, where are the gaps?
- One of the members of our board of directors has asked if our cyberdefense protects against APT23. How do I know? If it doesn't, where are the gaps?
- I am looking at acquiring several new security controls - how will my chosen security controls fare against our current expected threat environment?
- How can I objectively defend my budget requests for specific security controls and the personnel to support them?
- What is the return on investment of our cybersecurity investments and how do I objectively justify it?
- How do I objectively assess the risk in our cyberdefense?
- How can I easily repeat red team testing to see if our remediation worked?
- How can my blue team understand exactly what my red team did, step by step?
- How can my purple team make sure that the vulnerabilities and gaps discovered by the red team are, in fact, remediated properly by the blue team?



What are the Key Features of BAS Platforms?

The key features generally include:

- Administrative console
- Automation software
- Test point agents for production and test environments
- An underlying security framework
- Scenarios for testing which use the framework
- Risk analysis reporting
- SIEM integration
- SOAR integration
- An extensible API or API-1st
- Ticketing system and a case management system
- Direct security technology integration

Administrative Console

The administrative console is where all testing scenarios are set up. All reporting is available through the administrative console.

Automation

Automation gives your red team the ability to run exercises and validation scenarios on your enterprise controls and incident response workflows. Your red team is able to identify how each individual security control responds to the many thousands of possible common attack scenarios, allowing your red team to generate comprehensive reporting on each test result and to clearly communicate the impact of the threat to management. Automation gives your blue team the ability to continuously validate that security controls are configured properly and that it can meet (and defeat) the red team attacks as well as deter actual cyberattackers. Automation also delivers daily reports, such that security management can rapidly and easily identify critical problems for remediation. These regular reports also help document how existing security investments are achieving the desired return on investment (ROI).

Test Point Agents for Production and Test Environments

Test point agents are a key part of the testing harness that includes both attack scenarios that chain the entire Kill Chain together and necessary configuration checks. They are deployed by automation to set up your environment for emulation and testing. Test point agents are enabled to receive and execute your assessments to allow for live testing of your security controls in test systems or in your live production environments. The test point agents used should be lightweight and inactive except during the small testing window, making it feasible to deploy agents on live systems.

MITRE ATT&CK™

The Underlying Cybersecurity Framework - MITRE ATT&CK

AttackIQ uses the MITRE ATT&CK framework, the most authoritative, comprehensive, and complete set of up-to-date attack techniques and supporting tactics in the world. MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world data. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. MITRE's stature in the cyber community and the independence of its intellectual property in the ATT&CK matrix make it the ideal platform from which security operations management, executive staff, and boards of directors can objectively evaluate and measure cybersecurity controls' performance, risk, and capability.

MITRE ATT&CK has brought a well-matured taxonomy of the tactics and techniques that may be leveraged by any prospective attacker. This provides, for the first time, a common lexicon that enables stakeholders, cyber defenders, and vendors to clearly communicate on the exact nature of a threat and the objective assessment of the cyberdefense plan that can defeat it. This common lexicon brings a universal language that can be used to describe the procedures of an attacker or attack tools and exactly the techniques which they deploy. The precise lexicon of MITRE ATT&CK enables more precise assessment of threats and a faster, better-targeted response.

MITRE ATT&CK enterprise matrix provides a tabular view to all attacker tactics and techniques that might leverage Windows, Mac, and Linux environments. Across the top are headings listing the 12 tactics defined by MITRE ATT&CK. Listed below each of the 12 tactics is a column that shows between nine and 67 techniques that might be used to implement a particular tactic. It is often that case that several techniques are used in one or more tactics.

Scenarios for Testing Which Use MITRE ATT&CK

Scenarios are used to test your technology controls, validate your security posture, and instrument your environment. Scenarios will mimic malware and attack vectors so you can confirm that your security controls are working as expected.

The fast path to productivity is to test your existing security controls to validate they are performing as you expect. If you decide to test by threat, it is to be absolutely sure that your Breach and Attack Simulation platform shows exactly where the failure happened by security control. Search is an important component of Breach and Attack Simulation.

For example, you can search for the relatively new threat "APT28" and immediately find a scenario and customizable template to meet your needs in MITRE ATT&CK.

Risk Analysis Reporting

SIEM integration is an essential requirement for your Breach and Attack Simulation system. Automation delivers real-time alerts and summary reporting to applications such as your SIEM, email, Slack®, Jira®, and other applications so that you can evaluate the risk for attacks quickly. This rapid assessment of results enables you to make fast and accurate decisions on how to best address vulnerabilities and validate the effectiveness of your security controls. Many security operations teams must manage redundant products and deal with massive volumes of alerts that don't provide meaningful information. Breach and Attack Simulation helps you determine the core security products required to secure your enterprise adequately. Breach and Attack Simulation allows your team to develop a smart strategy and to build the resilient architecture needed to make it work.

Breach and Attack Simulation platform test results add high value towards building out a complete and objective risk analysis. Risk assessment is a cornerstone of most compliance regulations and provides your board of directors, perhaps for the first time, with the objective measurement of cyberdefense effectiveness and enterprise risk. This helps in supporting budget requests, as you can objectively delineate risk areas and the exposure they bring.

BAS Lets You Think Like an Attacker

It is critical to take on the mindset of the attacker. Imagine that one or more cyberattackers are working full time, with no other goal in mind than to break, enter, and compromise your intellectual property, damaging or destroying your information technology infrastructure. Sophisticated attackers are not set back by a few counter defenses - instead, they continue to probe and try to work through these defenses.

Your Breach and Attack Simulation platform must allow you to similarly change the plan, giving you every opportunity to probe and find vulnerabilities. Your BAS platform must provide the flexibility and capability to allow your red team to structure and execute these tests to meet the likely threats in your environment.

Most important is the need to assemble the events that constitute the likely kill chain variations your organization may face and to understand how your security controls perform from the assumed point-of-breach and forward. There are many goals you can now set and measure. These include identifying and stopping the attacker before they can exfiltrate data. Stopping attacker breakout is job one - measuring your organization's ability to detect or block breakout before breach is of paramount importance.

Security investments must be evaluated as an integrated defense-in-depth stack - this is necessary to detect and stop malicious adversary breakout and successful exfiltration. When analyzing performance with modeled kill chains, breach is not the endpoint. Detection of breach is the beginning of your successful defense. Your ability to test and manage the unfolding kill chain variations successfully will be the difference between success in stopping the attacker and suffering catastrophic data breaches, operational damage to IT systems, or much worse.

How Do You Get Started with Breach and Attack Simulation?

MITRE ATT&CK helps to present the 1,000-foot view that you need to be most effective. You can now logically organize your defenses against the threats you expect. The best place to start is with an analysis of the security controls you have in your environment today. You can map them back logically to MITRE ATT&CK to assess the coverage they provide against the tactics and techniques they will likely face in your environment. Analytically, you can identify gaps against the threats you expect in your environment, determine the risk these gaps provide, and make prioritized decisions to enhance your defenses.

This gives you clear and objective data to have a better discussion with management over budgets and attendant risk. Most interesting, if you implement the use case with MITRE ATT&CK for Breach and Attack Simulation (BAS) to automate and operationalize MITRE ATT&CK assessment and reporting, you will get a clear and complete picture of the efficacy of your cyberdefenses. For perhaps the first time, you will be able to precisely answer questions such as: "Are my cybersecurity controls working as I expect? Are we protected against APT23?" and many more.

Understanding Breach and Attack Simulation Use Cases

These are just a few of the many use cases supported by BAS. We have highlighted a few for review.

Red Team Performance

Improving red team penetration testing performance is a leading use case for BAS. Red teams can develop and automatically deploy a consistent and highly organized approach to defining the tactics and techniques of specific threats and then logically assess their environments to see if the defenses work as expected. MITRE ATT&CK and a BAS platform make all of this consistent, repeatable, and easily communicated. BAS enables these tests to be deployed at any time, against even the production environments, to ensure that critical resources are protected properly at all times.

Blue Team Performance

Blue teams can use BAS to provide precise reporting on deficiencies discovered by the red team. They can also use it to validate that upgraded and reconfigured security controls are in fact working as expected.

Threat Intelligence

Breach and Attack Simulation and MITRE ATT&CK can be used to more rapidly and effectively integrate your threat intelligence into your cyberdefense operations. All of this can be rapidly operationalized and automated. Threats can be mapped to the specific techniques of the attackers to understand if gaps exist, determine risk, and develop and deploy a plan to address them. This helps you answer specific questions about these new or predicted threats such as: "Do we think we are protected against APT23?"

Security Control Analysis and Selection

BAS platforms enable you to compare and differentiate vendor products against the tactics and techniques you feel you must defend against. Vendor products also differ - you can work with vendors to better understand their performance against the MITRE ATT&CK framework. The BAS platform enables you to test this easily, at almost any time.

Summary

Breach and Attack Simulation technology allows enterprises to automatically simulate the full attack and expanded kill chain used by cyberattackers against enterprise infrastructure. BAS allows you to understand the detailed status and performance of your security controls, processes, and personnel that support them.

BAS allows you to find the performance gaps, strengthen your security posture, and improve your incident response capabilities. BAS platforms provide automation that enables the platform to work autonomously and to scale to support the largest global enterprise.

To find out more about how to participate in a free trial of the industry-leading AttackIQ Breach and Attack Simulation, please reach out to info@attackiq.com or visit us at www.attackiq.com.

ATTACKIQ
U.S. Headquarters
9276 Scranton Road, Suite 100
San Diego, CA 92121
+1 (888) 588-9116
info@attackiq.com

AttackIQ, a leader in the emerging market of breach and attack simulation, built the industry's first platform that enables red and blue teams to test and measure the effectiveness of their security controls and staff. An open platform, AttackIQ® supports the MITRE ATT&CK Matrix, a curated knowledge base and model for cyber adversary behavior used for planning security improvements and verifying that defenses work as expected. AttackIQ's platform is trusted by leading companies around the world. For more information visit **www.attackiq.com**. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.