Aite PARTNER. ADVISOR. CATALYST.

IMPACT BRIEF

APRIL 2020

Joseph Krull, CISSP, IAM, CISA, CRISC, CIPP
+1.210.421.8233
jkrull@aitegroup.com

Cyber Hygiene in the COVID-19 Era: Breach and Attack Emulation

Effective vulnerability management is a cornerstone of any cyber defense program. A regular cadence of scanning, prioritization, remediation, and validation is the baseline requirement to identify hardware and software weaknesses in today's complex network and cloud environments. In recent years, vulnerability management vendors have added new automation capabilities to reduce the need for human intervention and move toward a near-continuous vulnerability identification process.

Some organizations have gone beyond vulnerability management tools to add basic security control validation via the use of breach and attack simulation (BAS) tools. BAS has evolved since it first entered the security lexicon circa 2015, and it is increasingly being used to evaluate security controls. Aite Group estimates that a somewhat crowded market of BAS vendors has collectively made a total of a few thousand paid deals. BAS allows organizations to perform basic simulations of attack activities primarily by installing agents within the infrastructure and detecting which agents can recognize attack-like signals generated from the BAS tool.

Penetration testing is a widely accepted industry practice to complement vulnerability scanning and evaluate the effectiveness of cyber defenses. Penetration testing uses the tactics, techniques, and procedures (TTPs) used by attackers to probe the network and find vulnerabilities that an actual attacker would use. Unfortunately, penetration testing is quite expensive, as it is labor-intensive and dependent on highly qualified cyber professionals. Fortunately, a new breed of tools—breach and attack emulation (BAE)—is emerging that can be used to automate penetration testing processes and increase testing cycles at significantly reduced cost. This Impact Brief describes the differences between BAS and BAE and includes an example of how an organization is using a BAE product to lower its cyber risk.

BACKGROUND

In an Aite Group November 2019 report, we noted that hardware and software vulnerabilities present significant risks to an organization and allow attackers a path to broader and more damaging actions.[1] The report included examples of how organizations with poor vulnerability management processes suffered debilitating cyber breaches and incurred significant financial and brand damage. Aite Group also identified automation and orchestration opportunities to add additional capabilities to mature vulnerability management programs.

Now, due to the massive expansion of remote work triggered by the COVID-19 pandemic, vulnerability management is even more critical. Organizations must adapt to new challenges associated with vulnerability identification for unmanaged computers, insecure limited-bandwidth home networks, new and expanded attack vectors, and the complexities of remote patching. Members of security teams, often working remotely themselves, look for ways to automate any possible aspect of vulnerability management to be more efficient and support business operations.

In the November 2019 report, Aite Group noted that effective vulnerability management includes five core steps: 1) enhance asset discovery; 2) seek useful sources of vulnerability data; 3) prioritize; 4) scan, validate, and test; and 5) put people into the mix.

In 2015, BAS tools launched. These tools offered capabilities to automate the critical validation component of vulnerability management. Although initial BAS tool capabilities were limited and market adoption was relatively slow, BAS tools are now becoming more common among organizations that want to step up their security validation programs. The BAS market has several players offering various approaches for performing validation and presenting reporting. Deployment generally revolves around sensors or agents installed at various points within the network and the BAS platform using a form of signaling to determine which sensor can be accessed and interrogated. Workflows can be based on playbooks, data derived from a database of known indicators of compromise, or customized queries. The adoption of BAS solutions is one of Aite Group's top cybersecurity trends for 2020.[2] Aite Group noted in January 2020 that organizations are moving toward a test-centric model, adopting BAS to test security controls.

Organizations add penetration testing to their vulnerability management programs for additional validation of security controls. Some compliance requirements, such as the Payment Card Industry (PCI) Data Security Standard and the Electronic Code of Federal Regulations (17 CFR § 39.18 - System Safeguards), make penetration testing mandatory. Although penetration testing is a widely recognized industry practice, it is expensive and relies on manual processes and highly specialized security practitioners. Fortunately, we are now seeing innovation in the penetration testing segment via the introduction of BAE tools. These tools go well beyond the capabilities of BAS and allow organizations to conduct near-continuous penetration testing to assess vulnerabilities and controls that can be breached by an attacker.

1. See Aite Group's report *Vulnerability Management: Take Your Program to the Next Level*, November 2019.

2. See Aite Group's report *Top 10 Trends in Cybersecurity, 2020: Ransomware, Evolving Strategies, and New Tools*, January 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

METHODOLOGY

From mid-December 2019 to mid-March 2020, Aite Group conducted 15 telephone and in-person conversations with security professionals, including security leaders, penetration testers, red team members, and security operations center managers. We also met with a sampling of BAS companies at the 2020 RSA Conference and reviewed four BAS products. Our research included a deeper hands-on study of a new BAE tool, followed by an extended interview with a cyber defense manager at a large financial services company that is using the same tool to reduce the company's overall cyber risk.

THE MARKET

The BAS market in 2020 and 2021 will continue to evolve and mature. Key developments will include an expected market consolidation and a focus on additional integration with ticketing and orchestration tools. In 2020 and beyond, BAS solutions will see competition from a new category of validation tools—BAE—which provide advanced validation capabilities beyond BAS and allow security teams and managed security service providers to replicate and automate activities performed by skilled penetration testers.

Trends and market implications can be found in Table A.

Table A: The Market

Market trends	Market implications
BAS and BAE solutions have evolved and matured and now provide concrete benefits to organizations of all sizes.	Organizations should consider BAS and BAE solutions as extensions to their vulnerability management programs, specifically for control validation purposes (BAS) or attack emulation purposes (BAE).
BAS and BAE solutions differ in how they are deployed and how results are presented.	Organizations should look for functionality that closely mirrors their control testing requirements and place special emphasis on the usability of the data provided. Evaluation criteria includes ease of use, extent of automation, ease of deployment, usefulness of reporting, and methods to reduce false positives.
The BAS market is crowded with more than a dozen vendors competing for allocations in cybersecurity budgets. Aite Group believes that there will be consolidation in this market sector in 2020 and 2021 as well as strong competition from emerging BAE vendors.	Organizations should consider the long-term viability of any vendor before selecting a BAS solution. Some organizations may elect to add a BAE capability or bypass BAS in favor of a more capable BAE product.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Market trends	Market implications
Some BAS and BAE solutions provide very detailed remediation recommendations for identified vulnerabilities. A small subset has initial integrations with ticketing and orchestration tools. Aite Group predicts that this will be a focus area for BAS and BAE vendors in 2020.	Orchestration and remediation support are clear market differentiators and can significantly increase the value of a BAS or BAE solution.
Unlike BAS, BAE products closely emulate the TTPs of a sophisticated attacker.	Organizations should look for BAE solutions that subject their infrastructures to realistic attack scenarios to include how attackers navigate between systems and escalation of privileges.
BAS and BAE products should closely adhere to the MITRE ATT&CK framework for categorizing their simulations. ATT&CK is a knowledge base of adversary tactics and techniques.	The framework offers a consistent language for attack categories and normalized attack definitions. Organizations can use this framework to synchronize and standardize human-led penetration testing efforts with control testing using BAS or automated penetration testing using BAE.
Product pricing is not yet consistent across either BAS or BAE solutions. Vendors price their products based on number of test points, number of assets, annual enterprise license, or assessment vectors.	Chief information security officers should carefully assess the total cost of the solution prior to procurement.
BAS products cannot emulate the activities of an experienced penetration tester or red team. BAE solutions automate key functions of penetration testing but cannot completely replace all human-driven penetration testing activities.	BAE tools should be considered as a force multiplier to complement traditional penetration testing activities. BAE tools free up penetration testers to focus on more complex attack scenarios.

Source: Aite Group

THE BAS AND BAE VALUE PROPOSITION

Prior to the introduction of BAS and later BAE products, vulnerability management fundamentally relied on cycles of scanning, remediation, rescanning, and verification. Organizations applied vendor patches, changed configuration settings, wrote new firewall rules, updated firmware, or closed ports based on the results of scans or vendor recommendations until rescans did not reveal continued vulnerabilities. Threat intelligence also provided input on certain vulnerabilities based on known attack profiles. These vulnerability management cycles are slow, and depending on how quickly remediation activities can be completed, vulnerabilities persist for weeks, months, or even longer. To close this gap, vulnerability management vendors introduced automation and orchestration in their products to help minimize the elapsed time and need for human interaction between scans, remediation, and rescans.

Many organizations supplemented their vulnerability management programs with cyber control audits or manual penetration testing to prioritize exploitable vulnerabilities that could not be identified as such by vulnerability scanners, as well as to identify network, credentials, and control weaknesses in operational cyber defenses. In some cases, penetration testing is a

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

mandatory component of compliance frameworks; otherwise, it is widely considered a sound business practice. To date, penetration testing is a human-centric endeavor. Organizations create internal red teams or engage professional services firms to conduct penetration tests against their networks and applications. Dedicated red teams give organizations the ability to perform security testing when needed. Still, salaries and benefits for team members constitute a substantial line-item in security human resources budgets. Experienced red team members are difficult to recruit and retain in most markets due to an extremely limited pool of qualified penetration testers.

The cost of penetration testing by professional services firms is not trivial. It can range into the low six figures for a time-boxed annual internal and external penetration test engagement for a large enterprise network. Some organizations engage specialty boutique firms to control costs, but these smaller firms have limited resources to support multiple clients with comprehensive testing geared to a client's preferred testing schedule and specific needs. The high cost of penetration testing results in organizations limiting test frequency to quarterly, semi-annual, or even annual tests. In many cases, prompt retesting after remediation of exploitable vulnerabilities becomes a "nice-to-have" rather than a "must-have" requirement.

Penetration testing, particularly when conducted annually or even semi-annually, does not match the urgent need to rapidly identify and remediate exploitable vulnerabilities. Every configuration change, application update, introduction of new equipment, or firewall rule change can inadvertently introduce new attack vectors and unacceptable risk to an organization. It is often possible to detect these vulnerabilities through scanning and network audits. Still, only penetration testing assesses whether these vulnerabilities can be exploited by an attacker to get closer to an organization's crown jewels.

BAS products came into the marketplace to help organizations augment their vulnerability management programs and provide a means to conduct tools-based validation of cyber controls. BAS can help bridge the gap between vulnerability management tools and manual penetration testing. They reduce the reliance on costly manual penetration testing to find weaknesses in cyber controls, particularly when penetration testing is only performed periodically. BAS tools have configuration screens that allow users to schedule and run configurable tests, and the most advanced BAS tools support the creation of custom testing scenarios. After viewing a subset of BAS products, Aite Group assesses that even a relatively junior security professional with basic network and control testing skills can effectively schedule and manage BAS-based testing. The primary advantage of a BAS tool is that control testing can be automated, and tests performed quickly and near continuously if needed.

BAE products now entering the market offer the capability to more closely link vulnerability management and penetration testing programs. BAE tools automate the activities of penetration testers and give organizations the ability to conduct frequent testing of the infrastructure using emulated attacks based on attacker TTPs—even daily if desired. It's possible to mimic attacks using either a shotgun or rifle approach, testing entire subnets or just specific IP addresses.

On-demand BAE solutions have additional benefits. The tool can be used to validate the effectiveness of security products or the ability of a cyber operations team to detect and respond to attack activities. The capability to perform tool-based penetration testing with a few keystrokes can allow security professionals to conduct pre-production testing of configuration

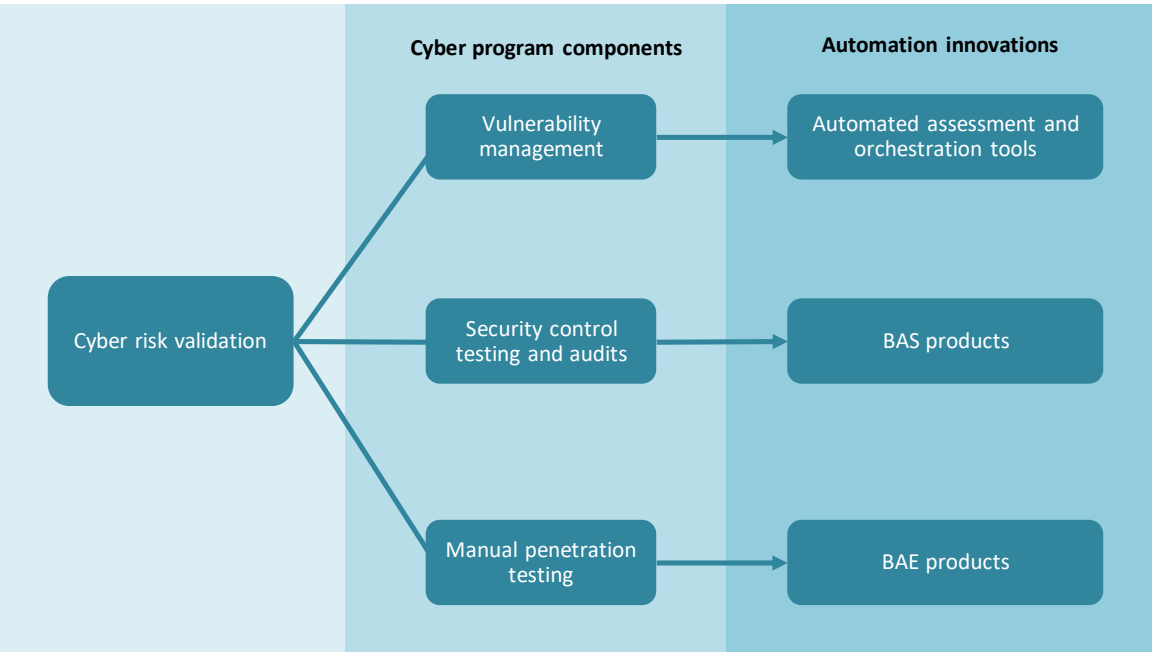
101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

changes, integrate penetration testing into change control programs, and evaluate the continued viability of aging security devices and controls. BAE tools can add realism to cyber defense and incident management exercises as well as team training. BAE tools can also help organizations reduce costs associated with compliance-based penetration testing, including the PCI requirement for annual penetration testing.

A word of caution: BAE products should not be regarded as a wholesale replacement for experienced penetration testers or red team members. Planning and executing attacks using the tactics of a sophisticated adversary requires special skills, intuition, and often social engineering that cannot yet be effectively conducted by a BAE tool. On the other hand, penetration testers and red team members can use BAE tools to augment their efforts and reserve their time for more sophisticated tasks. BAE tools also offer opportunities for managed security service providers to offer penetration testing as a value-added service.

Figure 1 depicts the relationship between cyber risk validation, cyber program components, and automation innovations.

Figure 1: Cyber Risk Validation—Automation Innovations



Source: Aite Group

DIFFERENCES BETWEEN BAE AND BAS

The fundamental difference between simulation and emulation products is that BAS is designed to perform representative control testing based on a sampling of components, while BAE provides a networkwide emulation of actual attacker behavior based on TTPs.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Key differences between BAS and BAE products can be found in Table B.

Table B: Differences Between BAS and BAE Products

BAS	BAE
Nearly all BAS products rely on agents or sensors that must be deployed to various areas of the infrastructure prior to use. BAS necessitates setting a path to the agent/sensor and the BAS product sticking to that path based on a playbook approach.	BAE products are agent-less. This means that any subnet or IP can be subjected to automated penetration testing without pre-configuration. BAE products function like a black-box penetration test that automatically and dynamically adjusts its attack vector as it obtains new information or accesses specific files.
BAS products track paths through the network based on successful signaling between the tool and the deployed sensor/agent. The product's primary output is a report based on representative paths.	BAE products can test the entire network and every resource, to generate a report on actual vulnerabilities found on any network-connected resource. Some BAE vendors offer a cloud delivery option as well as an on-premises deployment option.
BAS tools do not test password strength or complexity, nor can these tools perform privilege escalation.	BAE tools exploit vulnerabilities, perform automated password cracking, and conduct man-in-the-middle attacks as would be expected during an ethical penetration test of the network.
BAS products do not test for data hygiene (e.g., credentials in shared folders).	BAE tools leverage accessible data and sniffed traffic to perform lateral movement and privilege escalation.

Source: Aite Group

CASE STUDY

The cybersecurity team at one of the world's largest investment firms with more than US$500 billion in assets under management operates the company's vulnerability management program and contracts for third-party penetration testing from multiple providers. The cyber team is only able to budget for, schedule, and manage external penetration testing by professional services firms a few times a year. These limited-duration engagements do not provide complete coverage for the company's large and widely distributed network.

To supplement the vulnerability management program and third-party penetration testing, the cyber team introduced a BAS tool three years ago. In the second quarter of 2019, the team decided to add a more advanced BAE product to its program. The team selected the PenTera product from Pcysys to integrate into its penetration testing program to complement the activities of the professional services firms and go beyond the control testing capabilities of its exiting BAS tool. Aite Group spoke with the cybersecurity professional that manages the company's cyber testing program. He has many years of experience as a penetration tester, and he has used multiple BAS products. During our discussion, he commended the advanced capabilities of PenTera as a BAE tool. He specifically called out the breach-and-attack emulation capabilities as opposed to the simulation capabilities of the company's original investment. He based this opinion on PenTera's ability to safely test against live production environments using an agent-less solution and the product's capabilities to emulate a broad range of advanced attack scenarios. Using PenTera, his team is now able to actively test the security of network file

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

shares, a standing concern for the organization. He also indicated that he was impressed with the graphical user interface, easy-to-configure reporting templates, and integral, wiki-like remediation aids.

The security team had a specific use case ideally matched to PenTera's capabilities. The company has several offices in different international locations. Sending penetration testers to these locations or engaging multiple international firms made internal penetration testing unmanageable and prohibitively expensive. Now, using an instance of PenTera on a laptop, the cybersecurity manager can securely ship the computer to the remote location and have a local resource plug the machine into the local network. Once the tests are complete, the local office repacks the laptop and sends it on to the next designated location. This allows the security team to perform tool-based penetration testing on a periodic schedule, even at locations that could not be effectively tested in the past.

The security team has integrated PenTera into its daily activities and uses the tool to test the effectiveness of various controls. The team generally spins up a virtual machine instance for PenTera and then conducts a series of attacks against designated parts of the infrastructure. In the future, the security team plans to develop an advanced governance model around the use of the emulation tool that will include policies to make testing mandatory for certain types of infrastructure changes.

The cybersecurity professional noted that he was pleased with PenTera's ease of use, which has contributed to its extensive utilization by members of the team. He indicated that testing is currently being performed by a single team member who devotes 20% to 30% of his time to testing using PenTera. Low-impact attacks are scheduled and run automatically. PenTera allows more substantial attacks to be entered into a workflow that requires a manager's approval to release attacks. The cybersecurity professional noted that in the last nine months his team has been using PenTera, there have been no adverse impacts on normal network use.

The cybersecurity professional indicated that use of PenTera has reduced the organization's overall level of cyber risk, as the tool can be used frequently with minimal involvement by members of the team. PenTera allows the team to rapidly confirm that remediation activities have been completed and are effective.

RECOMMENDATIONS

Aite Group recommends that organizations take the following actions regarding their testing efforts:

- Now is the time to embrace automation. Add a BAS or BAE solution to your overall cybersecurity strategy. Obtain a BAS solution if your goal is simple control validation. Select a BAE tool or replace an existing BAS product to go beyond control testing. BAE can supplement current penetration testing activities to reduce costs, allow more frequent testing, and support better utilization of cybersecurity staff.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- Carefully evaluate the range of BAS products before procurement. Products with similar features crowd the BAS market. Product deployment, control test scheduling and execution, and test result presentation are key differentiators. A proof of concept with a subset of BAS providers may be warranted for larger organizations.
- There is potential for market consolidation in 2020 and 2021. Carefully consider the long-term viability of the various BAS vendors.
- For BAE, look for products with advanced features and capabilities such as agent-less deployment, a diverse range of sophisticated attacks, and the ability to subject live production environments to TTPs that could be encountered in future threat environments.
- As pricing models are inconsistent across vendors, carefully consider the total cost of ownership for any BAS or BAE product.
- Managed security services providers should evaluate how BAE can be offered as a value-added service. Agent-less deployments can facilitate frictionless penetration testing as a service offering.

CONCLUSION

- BAS tools are now viable tools for organizations that want to augment their vulnerability management programs with automated cyber controls testing.
- The BAS market is crowded with similar products; the market is subject to likely consolidation in 2020 and 2021. Organizations should carefully evaluate BAS solutions prior to procurement.
- BAE solutions will challenge BAS in the marketplace. These attack-emulation products enable organizations to subject their infrastructures to activities that very closely mirror what they would face from a sophisticated adversary.
- Both BAS and BAE solutions can help an organization reduce its cyber risk through more frequent—or even continual—testing of its controls and cyber defenses.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

RELATED AITE GROUP RESEARCH

Top 10 Trends in Cybersecurity, 2020: More Ransomware, Evolving Strategies, and New Tools, January 2020.

Vulnerability Management: Take Your Program to the Next Level, November 2019.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com