PICUS

ACHIEVING A THREAT-CENTRIC APPROACH WITH BAS

How Breach and Attack Simulation strengthens cyber resilience by answering important questions about the risks organizations face

A Whitepaper by Picus Security

Executive Summary

Traditional security assessments and methods of leveraging threat intelligence are failing to answer the fundamental questions organizations have when assessing their security posture. This means that many organizations instead rely on assumptions about the threats they face and are potentially leaving themselves exposed.

This whitepaper explains how Breach and Attack Simulation (BAS), by supplying continuous data-driven insights about organizations' readiness to defend against the latest threats, empowers security teams to make smarter decisions and become more threat-centric. It also outlines why Security Control Validation is the primary use case of BAS, delivering the most valuable outcomes to help security teams measure and enhance threat readiness as well as become more proactive.

Why Assumptions are a Threat to Organizations' Security

Against an ever-expanding attack surface and increasingly sophisticated attackers, security professionals must make critical security decisions at a moment's notice. Working in such fast-paced and dynamic environments—often without a holistic view to contextualize and prioritize action—it's unsurprising that many are forced to fall back on assumptions and intuition rather than quantitative evidence when making judgment calls.

The result? Inadequate responses to present and future cyber attacks and poor allocation of time, effort and resources.

Organizations are facing 'unknown unknowns'

$3.6 M	the average estimated cost of a cyber-attack to organizations in 2021. *Source: World Economic Forum*
25%	of organizations can quantify in financial terms the effectiveness of their cybersecurity spending. *Source: Gartner*
55%	of security experts lack confidence that cyber spending is aligned to the most significant risks that their organization faces. *Source: PWC*

A Threat-Centric Approach is Vital to Enhance Resilience

By basing decisions on perceived rather than actual risks, security teams can never confidently answer questions about the state of their organization's security posture. Nor can they be sure of focusing on the areas that will have the greatest impact. Limited situational awareness can also lead to bad investments and an inability to achieve optimal protection from them.

To become more cyber resilient, organizations of all sizes must improve their understanding of the risks they face by being more threat-centric. But how is this shift in mindset achievable without placing an even greater strain on already stretched operations teams and budgets?

Manual security assessments such as penetration testing and red teaming deliver valuable insights. However, they are slow to perform, costly and don't provide a comprehensive view. Threat intelligence from a wide range of sources helps organizations keep up with emerging threats but without adequate resources and expertise, the sheer volume of information can easily overwhelm security teams, making it hard to operationalize.

For organizations to obtain the high level of insight required to put threats firmly at the heart of decision making, a holistic, automated and continuous solution is needed: **Breach and Attack Simulation.**

Key Questions for Security and Risk Leaders

- Which threats pose the greatest risk to the organization?
- Do we know our most critical exposures and how to mitigate them?
- How could an attacker take advantage of any security gaps or vulnerabilities?
- What would the likely consequences be of a breach?
- How effective are the security controls we use at preventing and detecting attacks?
- Are we getting the best return from our security spend?

Without the ability to answer critical questions about an organization's security posture, security teams will struggle to prioritize where to focus their attention and resources

Traditional Approaches Don't Provide A Complete Picture

To help obtain answers to fundamental questions about the state of their security posture, organizations have traditionally been forced to rely on human-led security assessments such as penetration testing, vulnerability scanning and red teaming. However, these approaches come up short in several aspects.

Manual Assessments are Slow and Narrow in Scope

Due to the length of time that they take to perform, pen tests are usually restricted to a designated network, system, or application and tend to involve just a narrow range of attack techniques – those which can be replicated by a tester. Being vulnerability-focused, engagements are also of limited value to Security Operations Center (SOC) teams that are more concerned with detection and response.

Vulnerability scanning can provide broader visibility of known security exposures but the results can be challenging to interpret, making it hard to determine which gaps to prioritize. Red teaming is more focused on the emulation of attack scenarios, but these engagements are costly and neither scalable nor feasible to run on a continuous basis.

Threat Intelligence is Hard to Operationalize

Threat intelligence is another highly valuable source of insights to inform decision-making. However, few security teams possess the level of resources and expertise required to aggregate data streams from a wide range of sources—or analyze them in sufficient time and detail to obtain immediately actionable outcomes.

The complexity of threat intelligence information can also lead to data fatigue and mean that crucial details can be missed or overlooked.

56% **of security professionals believe that threat data is too voluminous and complex to offer timely and actionable intelligence.**

Source: Ponemon Institute

A Lack of Awareness Means Being Reactive

The challenge of obtaining holistic, measurable and actionable security insights from traditional assessment methods and threat intelligence is a key factor holding security teams back from being threat-centric. It is also a reason why many remain too reactive; jumping from one threat, alert or vulnerability to the next without an ability to determine which should be treated as a high priority.

More Technology Does Not Guarantee Better Outcomes

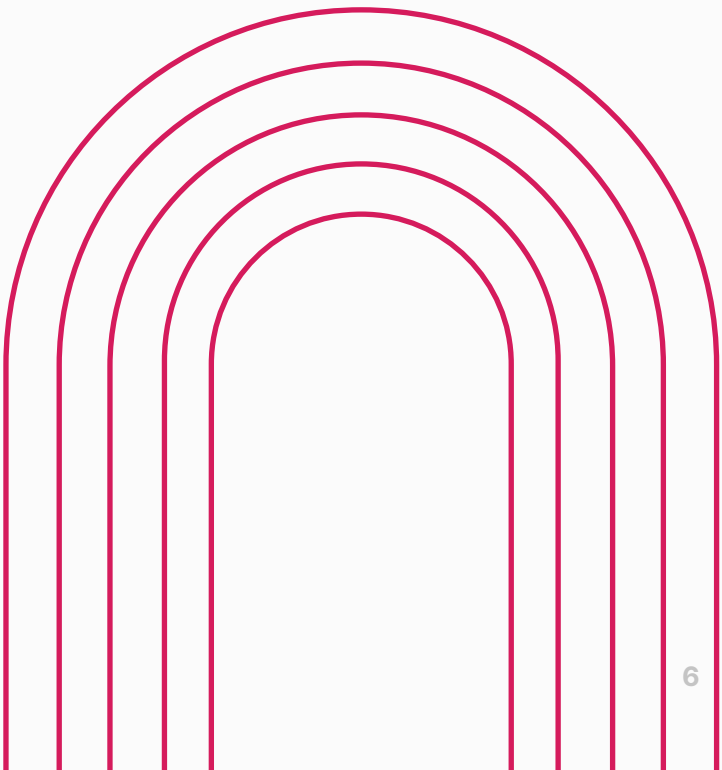
Perhaps unsurprisingly, many organizations view the answer to becoming more proactive as a need to invest in more and more technology. However, more dollars spent does not equal better protection.

Investments in security technologies without an understanding of which threats pose the greatest risk can lead to bad choices. Without the visibility a threat-centric approach enables, investments could be made in the wrong areas, leading to overlaps in coverage, or worse still, a failure to address gaps.

More security controls also cannot alleviate cyber risk if their effectiveness is not evaluated on an ongoing basis. They can instead add to a security teams' problems rather than address them by being another source of alerts to manage and monitor.

22% **of organizations surveyed are highly confident that their security controls work as they are supposed to.**

Source: Ponemon Institute



How Breach and Attack Simulation Facilitates A Threat-Centric Approach

Breach and Attack Simulation (BAS) offers organizations a swifter and less resource-intensive path to becoming threat-centric. Via automated, consistent and continuous simulation of real-world threats, BAS equips organizations to achieve a more holistic view of their security posture and mitigate threats as soon as they emerge.

Here's how BAS compares to traditional assessments

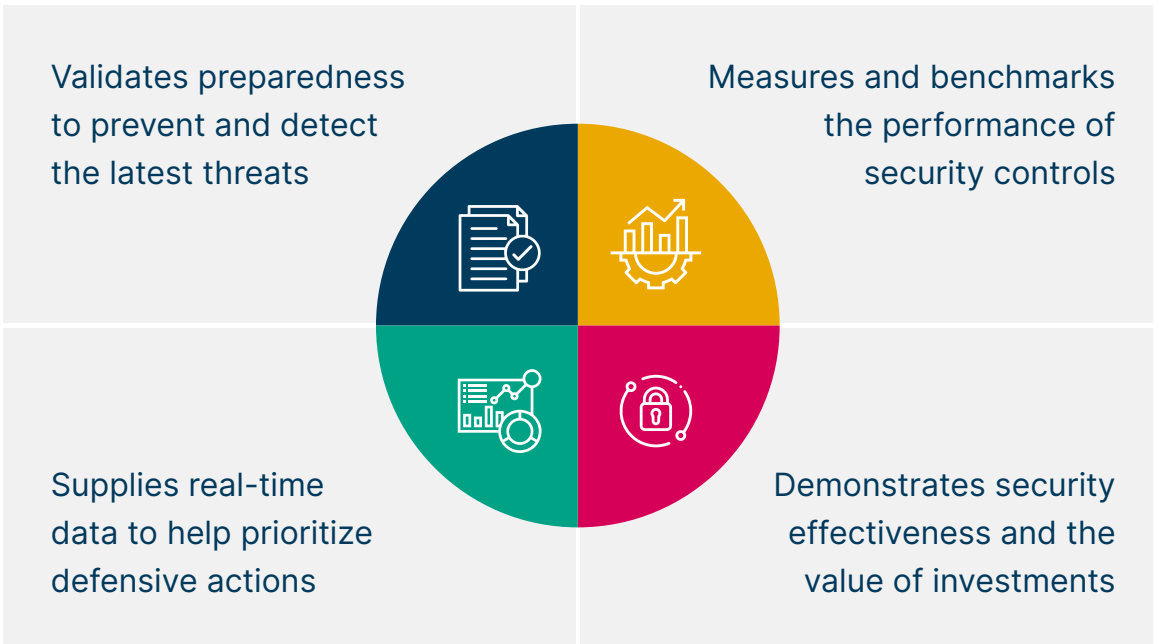
	BAS	Red Teaming	Pen Testing	Vulnerability Scanning
Fully automated	✓	✗	✗	✓
Consistent and continuous assessments	✓	✗	✗	✓
Validates security control effectiveness	✓	✓	✗	✗
Identifies vulnerabilities	✗	✗	✓	✓
Simulates attacks targeting specific CVEs	✓	✗	✗	✗
Performs testing across the cyber kill chain	✓	✓	✓	✗
Supplies mitigation insights for security controls	✓	Limited	Limited	✗
Accelerates adoption of security frameworks	✓	✗	✗	✗
Generates quantifiable metrics	✓	✗	✗	✗
Safely assesses production environments	✓	✗ (some risk)	✗ (some risk)	✗ (some risk)

Security Control Validation with BAS

Security control validation (SCV) is the foremost use case of Breach and Attack Simulation and is key to helping organizations answer the essential security questions needed to become threat-centric. With a BAS solution that offers a complete approach to SCV:

- Test and measure the performance of security controls, both individually and collectively, across prevention and detection layers.
- Obtain actionable insights and recommendations to maximize utilization of tools.
- Simulate a wide range of threats, such as malware and ransomware, as well as techniques used by Advanced Persistent Threats Groups (APTs).
- Perform continuous or on-demand simulations and generate security scores that can be used to measure readiness to defend against attacks.

Why Security Control Validation Is an Essential BAS Capability



Quantitative Insights a SCV Platform Can Provide

Prevention Insights

Controls supported:
Firewalls, Next-Gen Firewalls (NGFW), Web Application firewalls (WAF), Intrusion Prevention Systems (IPS), Endpoint Protection Platforms (EPP), Secure Email and Web Gateways (SEG)

Validates:

- Prevention of vulnerability exploitation attacks
- Prevention of web application attacks
- Blocking of malicious incoming and outgoing traffic, e.g.
  - Command and control activity (C2)
  - Malicious file downloads
  - Exfiltration of data

Detection Insights

Controls supported:
Security Incident and Event Management (SIEM), Endpoint Detection and Response (EDR)

Validates:

- Logs and telemetry are being captured and parsed
- Security events are accurately timestamped
- Correlation rules are in place and generate alerts
- Alerts are generated promptly following detection of malicious behavior

How SCV Compares to Other Types of BAS

Rather than specializing in Security Control Validation, some BAS tools are focused on Attack Path Management and Attack Surface Management. While these solutions are effective at satisfying a particular set of use cases, such as helping to identify how assets could be compromised, they often fail to answer some of the most fundamental questions about an organization's security posture.

The same limitations are also true of automated penetration testing tools. While automated pen test tools can be used to better understand how specific vulnerabilities could be exploited, the findings they generate can lack context.

Control failures was the #1 concern of cybersecurity executives in 2021

Source: Gartner

An SCV solution provides richer threat-centric insights by:

Assessing Readiness Against Specific Threats

SCV platforms can simulate specific threats—such as ransomware strains and APT groups—and quickly determine if an organization's security controls are effective against them. This is unlike attack path management solutions which identify the routes attackers take but provide limited insights to evaluate prevention and detection capabilities.

Simulating TTPs Across the Kill Chain

SCV platforms help security teams to understand the bigger picture by simulating threats across the cyber kill chain, pre- and post-exploitation. Other BAS solutions operate based on an assumed breach so don't provide insights to improve awareness of how attackers could infiltrate an organization.

Supplying Continuous Insights

Unlike automated pen testing, which has to be planned in advance to minimize any possible disruption to operations, security control validation can be performed on an ongoing basis. This makes it possible to identify and respond to risks sooner.

Providing Deeper Context

By analyzing the event logs generated by security controls, security control validation solutions provide the extra level of detail that security teams need to better understand weaknesses and take swifter, more effective actions.

Helping to Mitigate Weaknesses

Security control validation solutions don't just identify security gaps. They also provide actionable insights and recommendations, including prevention signatures and detection rules, to help address them.

By enabling organizations to understand the readiness of current controls to defend against specific threats, a security control validation platform answers fundamental questions other BAS solutions cannot

Considerations When Selecting A BAS Tool

When evaluating a BAS solution, there are several important factors that must also be factored in beyond its core competency. To ensure that it delivers the best security outcomes, assess its suitability in the following areas:

Simulation Capability

The diverse range of entry points and methods attackers use means it is vital to obtain a holistic view. To better understand how threat actors could gain initial access to an environment and move laterally, prioritize a solution capable of simulating attacks across the cyber kill chain and via network, endpoint, email and cloud vectors.

Threat Coverage

The ability to simulate the latest attacks is an essential capability of all BAS solutions. Evaluate platforms both on the strength of the number of real-world threats they offer as well as how quickly they are updated to incorporate emerging threats. Be aware that some vendors may charge a premium for early access to new simulation content.

Ease of Use

A BAS solution shouldn't add to the challenges of security operations by being difficult to deploy, use and manage. To avoid adding to the workload, prioritize a solution that makes simulating threats simple and hassle-free, and can empower red and blue teams to achieve a much greater impact with less effort.

Real-Time Reporting

To take swift and effective security actions, having easy access to the data required to make informed decisions is vital. Ascertain whether a BAS solution supplies data in real-time and overcomes the need for manual reporting by automatically generating reports suitable for security and business leaders.

Technology Integrations

A BAS solution's ability to integrate seamlessly with a wide range of security controls is another important factor to consider. For platforms that specialize in security control validation, out-of-the-box support for network and endpoint security tools will likely mean a deeper level of validation and the ability to automate mitigation actions.

Support for ATT&CK

By documenting threat behaviors, MITRE ATT&CK has become an important resource for security teams. Consequently, a BAS tools' ability to map the results of simulations to ATT&CK is a highly desirable feature, helping to visualize threat coverage and improve decision-making.

Cloud and On-Premises Deployment Options

Flexibility in terms of how a BAS solution can be deployed is another important factor. Requirements vary and change over time so choose a solution that is easily scalable and can adapt to support evolving business and security needs.

When evaluating BAS tools, security teams should prioritize a solution that only raises awareness of the threats organizations face but also provides actionable insights to mitigate the risks they pose

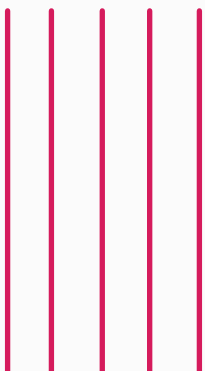
Become Threat-Centric and Level-Up Cyber Resilience with Picus

To enhance cyber resilience in a rapidly evolving threat landscape, the need to be threat-centric is more important than ever. Only by improving awareness of the specific risks they face can organizations make better security and investment decisions, be more proactive and minimize burnout. However, the limitations of traditional security assessments and difficulties of operationalizing threat intelligence mean that even enterprises with the deepest pockets can struggle to obtain the insights they need.

Breach and Attack Simulation enables organizations to obtain answers to questions about risks that have long proved elusive. With the ability to simulate real-world threats automatically and continuously, organizations can achieve an up-to-date and holistic view of their security posture as well as make prioritized decisions based on quantifiable evidence rather than assumptions. Bearing in mind key considerations like ease of use, frequent threat library updates, and the quality of mitigation insights provided, security leaders and teams can also leverage market-tested BAS solutions to alleviate resource challenges, empower organizational buy-in and improve remediation efforts.

As the pioneer of BAS, Picus Security is dedicated to making it easier for organizations of all sizes to become threat-centric. The Picus Complete Security Control Validation Platform empowers security teams by identifying threat coverage and visibility gaps and helps to address them swiftly and effectively.

With The Picus Platform, simulate the very latest cyber threats as soon as they emerge, continuously validate the effectiveness of prevention and detection controls, and obtain actionable mitigation insights to maximize security outcomes and demonstrate assurance.



About PICUS

At Picus Security, we help organizations to continuously validate, measure and enhance the effectiveness of their security controls so that they can more accurately assess risks and strengthen cyber resilience.

As the pioneer of Breach and Attack Simulation (BAS), our Complete Security Control Validation Platform is used by security teams worldwide to proactively identify security gaps and obtain actionable insights to address them.

FROST & SULLIVAN
LEADING VENDOR IN BAS MARKET 2020

2021 Cyber Security Awards WINNER BEST SECURITY PRODUCT OF THE YEAR PICUS COMPLETE SECURITY CONTROL VALIDATION PLATFORM PICUS SECURITY

CYBERTECH100 2021
The World's Most Innovative CyberTech Companies for Financial Services

2021 Computing Security Awards WINNER
Breach and Attack Simulation Solution of the Year

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2022

Interested to Learn More About BAS and Security Control Validation?

REQUEST MORE INFO

picussecurity