PICUS THE COMPLETE SECURITY VALIDATION PLATFORM

A BUYER'S GUIDE

# BREACH AND ATTACK SIMULATION

How BAS compares to Pen Testing & Red Teaming

Worldwide, more and more security teams are leveraging Breach and Attack Simulation (BAS) to enhance organizations' threat readiness and manage risks more effectively. The aim of this guide is to help you understand the value of BAS and how it compares to manual security assessments such as Pen Testing and Red Teaming.

## WHAT IS BAS?

Breach and Attack Simulation describes security technologies that simulate real-world cyber threats. The most common use cases of BAS are Security Posture Management, Security Control Validation, Attack Path Management and Security Operations Center Optimization.

## How does BAS compare to manual assessments?

As an automated solution, a BAS tool enables security teams without offensive security expertise to simulate threats consistently and continuously. In contrast, manual Pen Testing and Red Teaming are human-led, required skilled testers and usually conducted periodically.

The fact that Pen Testing and Red Teaming are performed by human testers means that they are slow to deliver results, have a narrow scope and only provide results at a single point in time. It's why agencies such as CISA and the NCSC now recommend organizations also embrace automation to achieve a holistic view and be proactive.

**Companies should embrace automated continuous testing to protect against longstanding online threats.**

Cybersecurity and Infrastructure Security Agency (CISA)

## Does BAS replace other approaches?

BAS does not negate the need for Pen testing and Red Teaming. Indeed, these exercises remain an important part of a comprehensive approach to risk management, such as Gartner's CTEM program.

Instead, BAS augments manual assessments by supplying real-time insights that enable security teams to measure day-to-day changes to organizations' threat readiness, and respond to known risks more swiftly.

With BAS, organizations can achieve greater and more actionable outcomes from security testing budgets. They can also ensure that manual assessments are focused in the right areas and on identifying exposures which require human ingenuity to discover.

**"By leveraging BAS, security teams can maximize outcomes from testing budgets and ensure that manual assessments are focused in the right areas."**

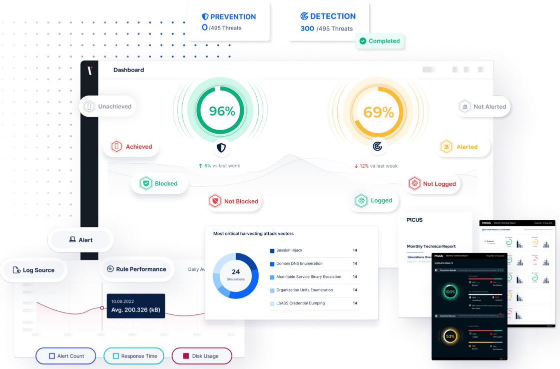
## HOW THE PICUS PLATFORM COMPARES

**The Picus Complete Security Validation Platform** is an easy to use BAS solution that simulates thousands of real-world cyber threats and attack techniques. Here's how the platform compares:

| | The Picus Platform (BAS) | Red Teaming | Pen Testing | Vulnerability Scanning |
|---|---|---|---|---|
| Fully automated | ✓ | ✗ | ✗ | ✓ |
| Consistent and continuous assessments | ✓ | ✗ | ✗ | ✓ |
| Simulates the latest cyber threats | ✓ | ✗<br>Determined by skill of tester | ✗ | ✗ |
| Validates security control effectiveness | ✓ | ✓ | ✗ | ✗ |
| Focused on identifying vulnerabilities | ✗ | ✗ | ✓ | ✓ |
| Simulates attacks targeting specific CVEs | ✓ | ✗ | ✗ | ✗ |
| Performs testing across the cyber kill chain | ✓ | ✓ | ✓ | ✗ |
| Generates metrics to measure effectiveness | ✓ | ✗ | ✗ | ✓ |
| Supplies actionable mitigation insights | ✓ | Limited | Limited | ✗ |
| Accelerates adoption of MITRE ATT&CK | ✓ | ✗ | ✗ | ✗ |
| Safely assess production environments | ✓ | ✗<br>Scoping minimizes risks | ✗ | ✗ |

## ACTIONABLE INSIGHTS NOT GENERIC GUIDANCE

To enable security teams to measure and respond to risks more effectively, The Picus Platform supplies real-time metrics and actionable mitigation suggestions.



### Benefit from real-time metrics to measure your security posture

Unlike Pen Testing and Red Teaming, the platform provides performance scores that enable cyber resilience to be measured and tracked over time.

To help address policy gaps and misconfigurations, the platform also offers actionable insights and vendor-specific mitigation content for the latest prevention and detection controls.

## ONE FLEXIBLE SOLUTION FOR ALL YOUR BAS NEEDS

The three products that comprise our complete platform:

### Security Control Validation

Validates and enhances the effectiveness of security controls to prevent and detect cyber threats.

### Attack Path Validation

Discovers high-risk attack paths that could enable attackers to compromise systems and users.

### Detection Rule Validation

Optimizes threat detection and response by identifying issues that affect the performance and hygiene of SIEM detection rules.

## Interested to Learn More About BAS?

REQUEST MORE INFO

### It's a game changer!

"Although we always used pen test and other assessment practices, none of them gave us the depth and width we need to understand our security posture against the possible attack scenarios extensively."

IT Platform Security Expert Lead, ING Bank

**www.picussecurity.com**

picussecurity