PICUS

WHITEPAPER

BREACH AND ATTACK SIMULATION VS. TRADITIONAL ASSESSMENT METHODS

RED TEAMING, PENTESTING, AND VULNERABILITY ASSESSMENT

EXECUTIVE SUMMARY

Given the rapid advancements in adversarial techniques and the sheer number of breaches that occurred in 2023, sticking to outdated security assessment methods has proven insufficient. The benefits of traditional approaches have been surpassed by their limitations. Thus, we have arrived at a point where organizations continue to engage in traditional methods like red teaming, penetration testing, and vulnerability assessment merely to fulfill specific compliance requirements, not because they expect or intend to identify and address a security gap immediately.

Hence, many organizations have realized that traditional security control assessment methods, which focus on simply identifying system or network vulnerabilities or repeating typical attack scenarios across different engagements by the same professionals, are no longer sufficient. This realization has been supported in light of the increase in **hunter-killer** malware, as highlighted in the **Picus Red Report 2024**. Such malware is designed to systematically target and undermine existing security controls to maintain stealth over extended periods. So, traditional methods are insufficient are falling short to deliver attacker-like assessments practices.

Thus, forward-thinking organizations have started using Breach and Attack Simulation (BAS) technologies to address these limitations. Unlike traditional solutions, BAS **continuously and automatically** exposes implemented security measures to **a broad spectrum of cyber attack simulations** based on the up-to-date cyber threat intelligence to test how well their prevention and detection layer solutions are holding against a real-life-like **full kill-chain** of sophisticated adversaries.

By providing solid, **data-driven validation** of their security posture, BAS arms organizations with **actionable mitigation** suggestions. Unlike traditional methods, which often yield cryptic reporting and general remediation suggestions, BAS **eliminates the uncertainty of what to do after an assessment** when their security investments fail to perform as intended.

This whitepaper highlights these distinctions and offers a comprehensive comparative analysis of BAS versus traditional security assessment methods.

333%

increase in the use of hunter-killer malware that explicitly targets and disables security controls has been observed yearly.

The Red Report 2024
Picus Security

INTRODUCTION

The modern cyber threat landscape has dramatically changed, with adversaries deploying sophisticated and stealthy "**hunter-killer**" malware, so much so that this evolution has rendered traditional security validation techniques increasingly ill-sufficient as they struggle to provide an assessment that accurately reflects real-world security threats.

For instance, **penetration testing**, which identifies and exploits vulnerabilities, fails to mimic an attacker's entire strategy, potentially leaving the effectiveness of defense measures unvalidated for specific scenarios. Although **red teaming** offers a more attacker-centric evaluation of an organization's security posture, its resource intensity and infrequent execution—usually once or twice a year—risk leaving security controls misconfigured, non-optimized or even non-functional for extended periods against both known and emerging threats.

Similarly, despite their automated nature, **vulnerability assessments** are limited to pointing out potential vulnerabilities in networks, software, and systems without validating the exploitability in a possible scenario or assessing the business impact of potential breaches.

In response to these challenges, **Breach and Attack Simulation (BAS)** technologies have emerged as a superior solution for security validation. By leveraging continuous and automated attack simulations that mimic the entire kill chain of malware and threat actor behaviors, BAS addresses the limitations of traditional methods. These simulations identify gaps within the security posture and provide immediate, actionable, and vendor-based mitigation strategies for tailored needs. This approach enables BAS to offer a clear, data-backed evaluation of the effectiveness of current security measures across both prevention and detection layers. Crucially, the ability to effectively quantify and communicate actual risks to decision makers is key for securing the necessary support and investments to enhance an organization's security posture.

In this whitepaper, we will evaluate BAS against traditional security control assessment methods across five distinct categories, demonstrating why BAS represents the superior security validation practice.

26%

of the 600,000 malware sample analyzed were identified as hunter-killers that proactively seek and impair implemented security controls.

The Red Report 2024
Picus Security

SECURITY ASSESSMENT APPROACHES

Security assessment is a practice of evaluating the effectiveness of an organization's security measures in protecting against cyber threats. It involves comprehensively examining **preventative and detective security solutions** to ensure they are properly configured, optimized, and up and running as intended. This practice aims to proactively identify and address any gaps within the security posture before malicious actors can exploit them.

Here are the most commonly used security assessment methods.

Red Teaming

Red teaming is an advanced, adversarial approach utilized to evaluate the robustness of an organization's security measures. By adopting the perspective of real-world attackers, red team members use similar tactics, techniques, and procedures (TTPs) to orchestrate cyberattacks. These engagements target an organization's networks, systems, applications, and physical security defenses to uncover potential attack vectors and pathways leading to compromising critical assets, such as Domain Controllers (DC).

Penetration Testing

Penetration testing is a targeted security assessment method that identifies and exploits specific vulnerabilities in systems or applications, focusing on uncovering and mitigating security flaws through technical assessments. While it provides detailed insights into individual components' security, it differs from broader, more strategic security evaluations like red teaming by concentrating on immediate vulnerabilities rather than an organization's overall defensive capabilities.

Vulnerability Assessment

Vulnerability assessment is indeed a systematic process designed to identify, quantify, and prioritize vulnerabilities in a system. It typically includes scanning networks, systems, and applications to detect vulnerabilities such as software flaws, missing patches, misconfigurations, and web application vulnerabilities. The primary goal of vulnerability assessment is to determine the weaknesses present in information systems that could potentially be exploited by attackers to gain unauthorized access, disrupt services, etc.

Breach and Attack Simulation (BAS)

BAS is an advanced security assessment methodology that leverages automation to mimic diverse cyberattacks targeting an organization's security infrastructure. It systematically emulates attacker TTPs, enabling the identification of weaknesses in a non-destructive manner. Through continuous testing, BAS empowers organizations to gain real-time insights into their threat landscape, facilitating proactive defense enhancement and refinement of incident response strategies. Simulating various attack scenarios, such as network infiltration, email compromise, lateral movement, and data exfiltration, enables organizations to pinpoint vulnerabilities before malicious actors exploit them—also, detailed reports generated by BAS assessments aid in prioritizing remediation efforts based on risk severity.

COMPARATIVE ANALYSIS: TRADITIONAL SECURITY ASSESSMENT METHODS VS. BAS

This section introduces the seven key characteristics that our comparative analysis is based on.

1. Automation

Automation plays a vital role by reducing the need for human intervention, enabling organizations to focus their limited human resources on more critical issues that demand prioritization. This strategic reallocation enhances efficiency and ensures that key areas receive the necessary attention.

2. Continuous Assessment

Organizational security infrastructures are constantly evolving, with frequent updates to security controls, configuration changes, and introducing or eliminating security measures, a process known as "environmental drift." Simultaneously, the threat landscape is growing more complex. Therefore, adopting continuous security assessment practices is crucial to stay ahead of these changes effectively.

3. Assessing Security Controls

Organizations deploy numerous security controls as part of their defense-in-depth strategy, each with varying capabilities to defend against cyber attacks. These controls are often utilized across different networks and geographical locations. Since the strength of security posture is determined by their weakest element, security assessment methods should holistically test the entire security infrastructure to identify and address any gaps.

4. Actionable Mitigation

Security teams requires clear guidance after an assessment. Simply having visibility without the ability to quickly remediate risk gaps undermines the effort's objective. Therefore, security assessment methods should provide immediate, actionable mitigation suggestions that can be easily implemented into an organization's security infrastructure. This is particularly crucial when publicly available proof-of-concept exploits exist, and no patch is available.

93%

of security professionals believe that more automation would improve their work-life balance.

They expect automation to help their teams increase productivity, save time, and optimize performance and reliability.

2023 Voice of SOC Report
Eoin Hinchy
CEO and Co-Founder, Tines

5. Assessment Scope

Assessing the entire cyber kill chain is crucial because it allows organizations to identify and mitigate potential attack vectors within a possible kill chain. By examining threats from initial reconnaissance to data exfiltration, organizations gain a comprehensive understanding of their security gaps across different attack stages. This holistic approach to security assessment ensures robust protection, proactively preventing attackers from breaching systems and maintaining the integrity of organizational defenses.

6. Testing Emerging Threats in 24 Hours

Security assessment methods should allow organizations to test against emerging threats within 24 hours to effectively counteract the pace at which cyber threats evolve. This capability ensures security controls are robust and responsive, swiftly identifying gaps and weaknesses before attackers can exploit them. Quick adaptation to new threats helps maintain the integrity of security defenses, protecting organizational assets and preserving trust in a constantly shifting cybersecurity environment.

7. Risk-free Assessment

Security assessments must be risk-free and non-disruptive to avoid operational downtime and financial setbacks. Interruptions can erode customer confidence, hinder productivity, and lead to revenue loss. Ensuring these evaluations are seamless and without impact allows businesses to identify and mitigate security vulnerabilities effectively, preserving continuity, and safeguarding against potential threats without compromising daily operations or exposing new weaknesses.

72%

of cybersecurity leaders agree the threat landscape is becoming more challenging.

The Forrester Wave: Cybersecurity Skills and Training Platforms, Q4 2023

1. Automation

Automation mitigates the challenge of limited human resources and lightens the load on security teams. It streamlines security assessments, optimizes resource use, and focuses efforts on critical tasks. This enhances security posture without adding to the workload.

BAS

BAS is a technology that automates security assessments, allowing organizations to simulate cyber attacks against their defenses without human intervention. When configured correctly, it can automatically simulate the latest threats from its updated threat library, providing an easy-to-use and scheduled approach to testing security measures.

Penetration Testing

The success of this non-automated approach largely depends on the tester's skills and expertise. However, testers may not be able to apply all previously learned attack methods. Furthermore, it fails to offer comprehensive insights because it cannot assess all system components, such as lines of code, decompiled assembly, and web services, in contrast to what automated tools can achieve.

Red Teaming

Red teaming is a hands-on approach that mimics real-world threats through in-house or external expertise. It demands significant resources, regardless of being outsourced or conducted in-house. The lack of end-to-end automation makes exercises challenging to repeat consistently, complicating the assessment of environmental changes on security posture and the tracking of security performance over time.

Vulnerability Assessment

This automated approach offers a straightforward and schedulable method for detecting known vulnerabilities. It is efficient, capable of delivering results within hours, and does not demand specialized expertise. It often presented a more cost-effective solution for organizations compared to penetration testing.

Breach and Attack Simulation technologies allow enterprises to gain better visibility on their security posture weak spots by automating the continuous testing of threat vectors such as lateral movement and data exfiltration.

Hype Cycle for Security Operations, 2023
Gartner

2. Continuous and Consistent Assessment

Security assessments must be a continuous practice to help organizations stay ahead of new threats, changes in security controls and their settings, and the addition or removal of security measures, often referred to as "environmental drift."

BAS

BAS provides a continuous, **24/7/365** approach to security assessment, enabling organizations to identify and address *non-functioning, underperforming, or misconfigured defensive measures*. By constantly guarding against the latest threats, it offers a significant cost-benefit advantage over non-continuous practices.

Red Teaming

Continuous red teaming isn't feasible by nature, as it requires a lot of resources and involves simulating real cyber attacks with careful planning and specialized knowledge. It demands human judgment and analysis, and making an ongoing practice is costly. Also, continuous operations could exhaust resources and potentially disrupt the systems they're meant to safeguard.

Penetration Testing

Penetration testing cannot be a continuous practice due to its scope-based nature and the extensive preparation work needed. It requires deep understanding of the target system to find and exploit weaknesses, using methods that closely mimics an attacker's approach. This expertise-reliant process is customized for each environment, which is not appropriate for automation.

Vulnerability Assessment

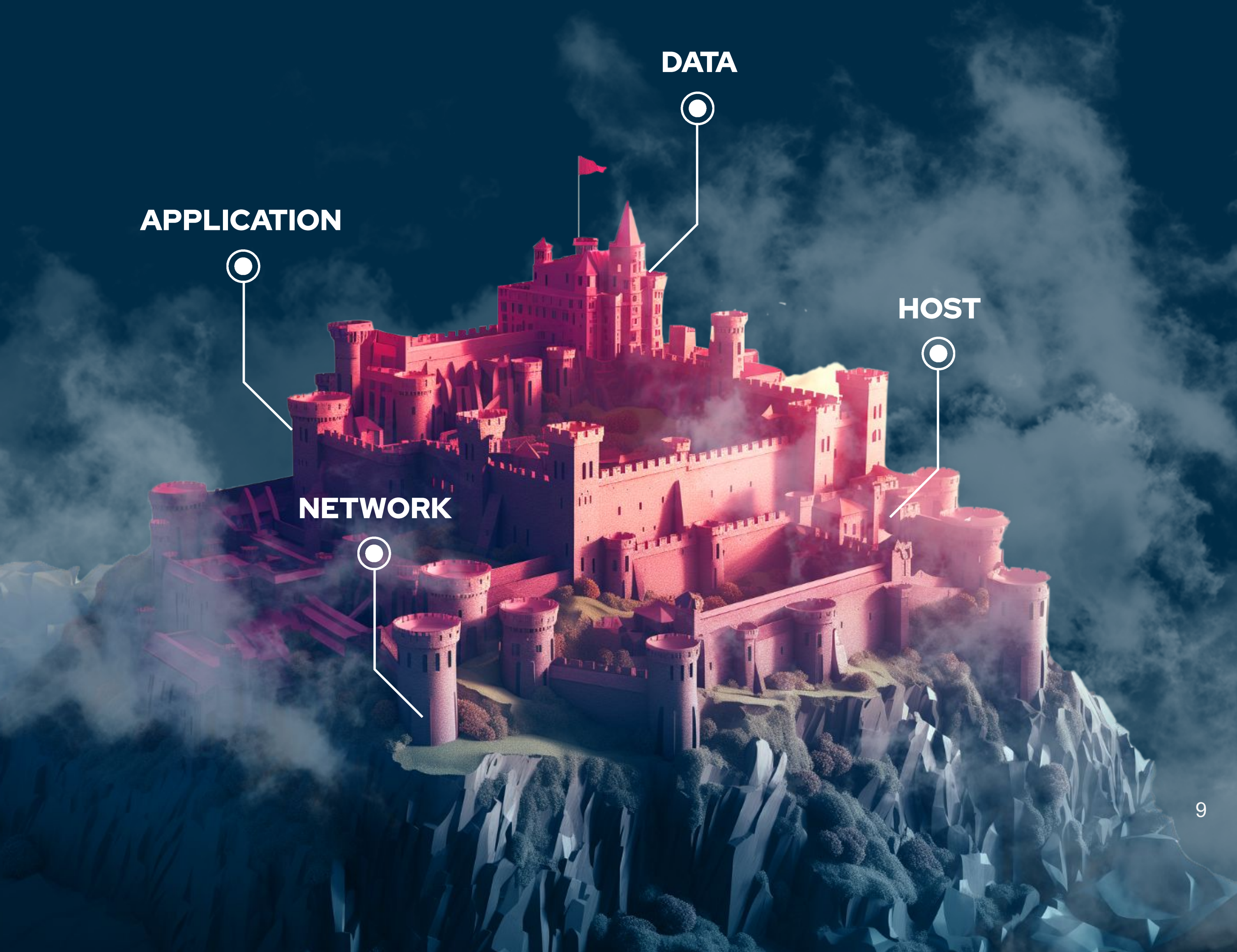
Vulnerability assessments are ideally designed for continuous execution, utilizing automated tools to consistently scan and assess systems for security vulnerabilities. This approach enables organizations to quickly identify and remediate new or previously unnoticed security flaws in their networks, systems, or software applications.

84%

Percentage of critical infrastructure incidents where initial access vector could have been mitigated.

X-Force Threat Intelligence Index 2024
IBM

An organization's **defense-in-depth** strategy is only as robust as the thorough **validation of its security controls**, ensuring each layer functions in perfect harmony.



3. Assessing Security Controls

Validation processes must encompass existing controls and evaluate their readiness against threats, allowing for the prioritization and understanding of identified risks.

BAS

BAS solutions enable seamless integration across diverse prevention and detection technologies, enhancing organizations' defense-in-depth strategies. They cover the network layer (e.g., firewalls, IPS/IDS), host layer (e.g., EDR, HIPS/HIDS), application layer (e.g., WAF, ESG), and data layer (e.g., DLP) as well as cross layer solutions like SIEM. This integration provides data-driven insights into the effectiveness of security measures.

Red Teaming

Red teaming assesses the effectiveness of security controls through simulated attacks but cannot provide a comprehensive review of all security solutions, as exploring every potential attack path requires significant resources. This method focuses on identifying critical attack vectors and chaining them to uncover attack paths, rather than performing a detailed audit of every security measure.

Penetration Testing

Penetration testing evaluates the security of systems by actively exploiting vulnerabilities. However, it does not deliver an exhaustive analysis of all implemented security solutions. This approach is heavily targeted, aiming to breach specific components or systems within a limited scope and timeframe. Thus, it might not uncover every potential weakness across the entirety of an organization's security landscape.

Vulnerability Assessment

The vulnerability assessment spots weaknesses within system or network infrastructures but does not conduct evaluations of the effectiveness of existing security measures. Its primary goal is to identify potential attack vectors, prioritizing remediation efforts, rather than performing any kind of validation or security assessments.

41%

of cyberattacks bypass network security controls, such as IPS, NGFW, or WAF.

The Blue Report 2023
Picus Security

4. Actionable Mitigation

Security assessment methods should not only identify security vulnerabilities and gaps but also **offer actionable mitigation strategies** to enhance an organization's security posture.

BAS

BAS technologies provide easy-to-apply mitigation suggestions that are vendor-neutral and vendor-specific (from different vendors) for each simulated threat. This reduces the time spent on mitigation research conducted by defensive teams and offers quick and robust improvements in security posture, especially in the face of publicly available vulnerability exploit attack scenarios without a patch released.

Red Teaming

Red teaming exercises typically prompt mitigation efforts by an organization's security (or blue) teams based on their findings. However, these recommendations often lack depth and specificity, providing a general direction rather than detailed, actionable steps for addressing identified attack vectors or vulnerabilities.

Penetration Testing

Manual penetration tests often lack actionable insights. While a tester may identify a critical vulnerability, they may not provide guidance on mitigation. This leaves organizations aware of security gaps but without detailed assistance in addressing them, shifting the responsibility and operational burden of mitigation/remediation plans to internal teams.

Vulnerability Assessment

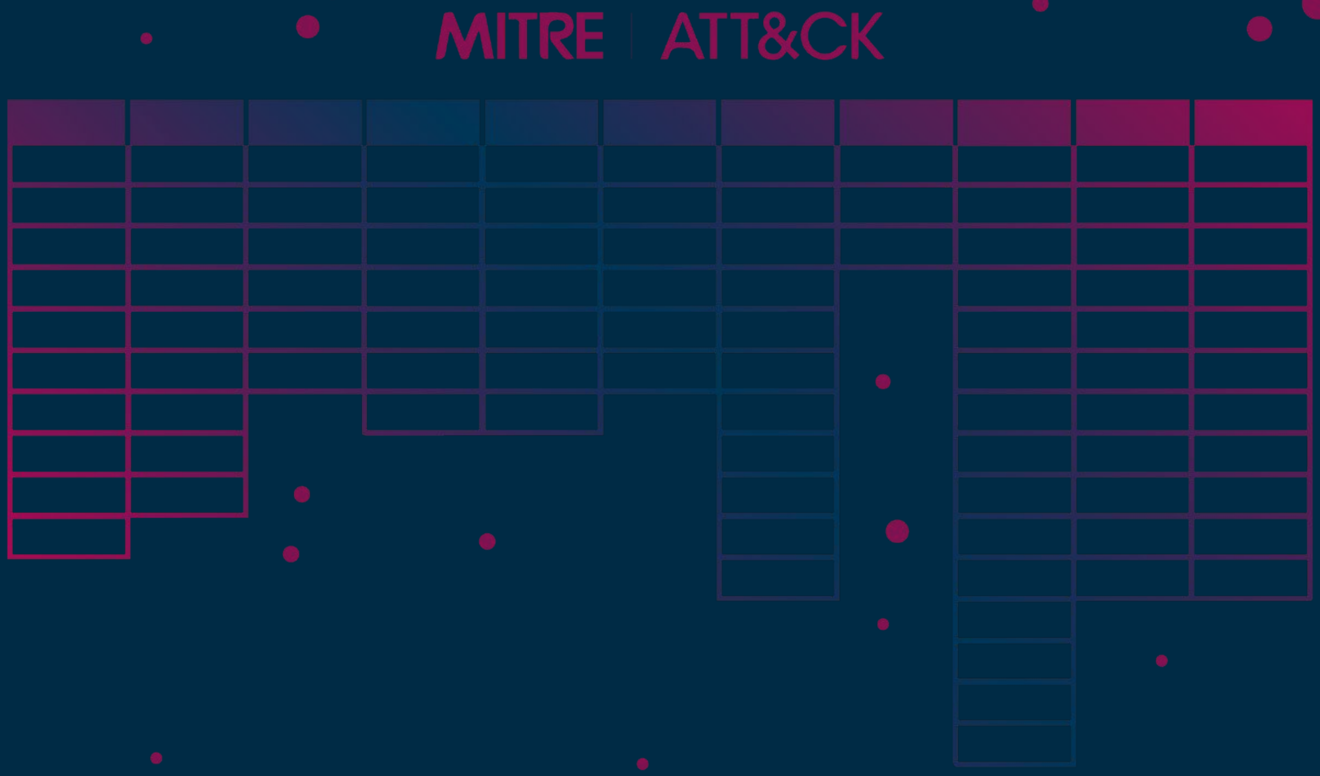
Vulnerability assessments do not typically provide specific mitigation strategies. This approach prioritizes the discovery of security weaknesses over offering direct solutions, leaving organizations to determine the appropriate remediation steps independently. Without guidance on mitigation, security teams may face challenges in prioritizing and addressing vulnerabilities effectively, potentially delaying the strengthening of their security posture.

65 days

is mean time to remediation (MTTR) for critical severity vulnerabilities.

The 2023 Vulnerability Statistics Report Edgescan

BAS simulates the **full cyber kill chain** of emerging threats, pinpointing critical **attack vectors** where security measures fall short and empowering security professionals **neutralizing attack paths** before an exploitation occurs.



5. Assessment Scope

The scope of an assessment determines the depth of the evaluation of security controls. A broad assessment scope ensures that organizations can effectively identify security gaps in their security posture in a contextualized manner, and take immediate remediation actions.

BAS

BAS can simulate attacks mirroring adversaries' **full cyber kill-chain**. From initial access, it executes techniques like privilege escalation, credential dumping, lateral movement, and data encryption safely. With threats mapped to frameworks like MITRE ATT&CK, BAS enables organizations to assess defensive capabilities across each attack step, identifying and eliminating potential chokepoints.

Red Teaming

Red teamers, tasked with objectives such as accessing the Domain Control (DC), devise a chain of attack vectors to achieve this specific goal. This practice focuses on critical attack paths toward the objective. It does not involve a comprehensive security assessment and may not reveal all attack paths to the DC; often, only one path is demonstrated to fulfill the objective, leaving many others undetected.

Penetration Testing

Penetration testing can't uncover all vulnerabilities threat actors could exploit as it works within a predefined scope. For example, if a test solely targets the IT infrastructure managing card payments, it provides limited insight into the organization's overall security control capabilities, potentially resulting in a low-quality assessment of their security posture.

Vulnerability Assessment

The scope of vulnerability assessments is broader than penetration testing but is focused on identifying known security weaknesses rather than exploiting them. This approach enables organizations to understand their exposure to potential threats by identifying and quantifying vulnerabilities.

44%

of multi-stage attacks cannot be prevented by security controls.

This indicates a significant vulnerability in current defense strategies against sophisticated attack scenarios.

The Blue Report 2023
Picus Security

6. Testing Emerging Threats in 24 Hours

When an emerging threat aggressively targets an organization's region/sector in the wild, or when a new zero-day vulnerability in a product that a company is using is being exploited, it is crucial to test the effectiveness.

BAS

BAS technologies provide a continuously updated threat library that is fed by deep threat intelligence research conducted by red teaming professionals. Hence, even if there is a zero-day exploit with a proof of concept in the wild, BAS technologies can add the corresponding threat to the library within 24 hours, allowing organizations to swiftly simulate the threat and test their defenses against possible exploitation attacks.

Red Teaming

A red teamer can learn new attack techniques by conducting CTI research, exploring exploit databases, or delving into underground hacking forums. This approach ensures they stay abreast of the latest attack vectors being employed in the wild. However, to conduct an attack simulation within 24 hours, organizations must engage in continuous red teaming practices, which are both computationally and resource-wise infeasible.

Penetration Testing

Penetration testers can also swiftly learn about a new attack techniques/vectors. However, performing it within 24 hours is often infeasible, as the scope of the test as well as the engagement letter should be defined beforehand, which takes time and diminishes the benefit of immediate testing against a particular threat.

Vulnerability Assessment

The vulnerability assessment practice mainly relies on automated vulnerability scanners, whose databases are updated with newly discovered vulnerabilities. However, it is important to note that these updates are generally not implemented within the 24-hour time period after the discovery of the vulnerability, such as CVEs.

Only 29% of security professionals said they have high confidence that they have a robust mechanism to test their environments against the most current threat vectors.

Building a Case for a Virtuous Cycle in Cybersecurity
Darktrace

7. Risk-free Assessment

Security assessment methods should be risk-free to the operational environment to ensure they do not disrupt business processes or compromise system integrity.

BAS

BAS technologies conduct attack simulations safely and non-disruptively by simulating cyber threats within a controlled environment. Before a threat is added to its library, it undergoes security and performance testing to confirm proper simulation functionality without causing unintended system or network load. This ensures that operational workflows are not interrupted and system performance remains unaffected.

Red Teaming

Due to their attacker-centric approach, red teaming prioritize a stealthy, non-noisy presence. However, this similarity to actual adversaries means that the changes they introduce to the environment, such as the *creation of new services and users with high privileges*, can inadvertently introduce new attack vectors if not properly reversed or cleaned up. This oversight may leave systems more vulnerable than before the exercise.

Penetration Testing

Penetration testing can be inherently disruptive due to its aggressive approach to identifying and exploiting vulnerabilities, often without prioritizing the reduction of noise or network load it generates. This method does not shy away from employing techniques that can strain system resources, trigger implemented defensive measures, or disrupt operational workflows, solely aiming to identify and exploit critical vulnerabilities.

Vulnerability Assessment

Vulnerability assessment methods are designed to be safe and risk-free to ensure they do not jeopardize the operational integrity or security of the systems being tested. By employing non-invasive scanning techniques, these assessments identify weaknesses without disrupting normal operations or exposing systems to potential threats.

30%

of security breaches are caused by the abuse of valid account credentials, making this one of the most common entry points for cybercriminals.

X-Force Threat Intelligence Index 2024
IBM

CONCLUSION

In today's digital age, the necessity for robust security measures has never been more critical. The evolution of cyber threats, especially with the rise of sophisticated "hunter-killer" malware, demands a paradigm shift in how organizations assess their security postures. Hence, while valuable, traditional security assessment methods, such as red teaming, penetration testing, and vulnerability assessments, are increasingly proven inadequate in the face of sophisticated cyber threats.

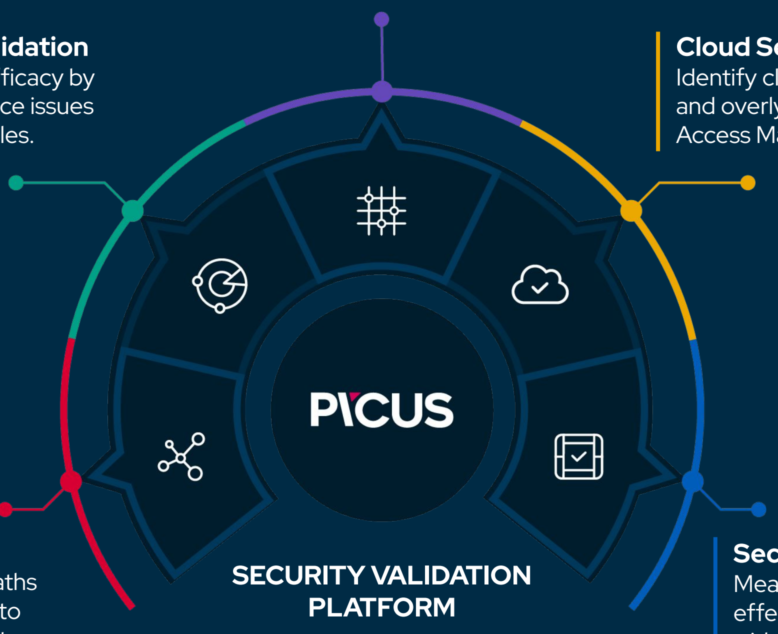
	Breach and Attack Simulation (BAS)	Red Teaming	Penetration Testing	Vulnerability Assessment
Automation	✔	✘	✘	✔
Continuous Assessment	✔	✘	✘	✔
Assessing Security Controls	✔	Limited	✘	✘
Actionable Mitigation	Ready-to-Use Mitigation Content	Limited with Generic Suggestions	Limited with Generic Suggestions	Limited with Software Patches
Assessment Scope	Entire Kill Chain	Limited by Predefined Objective	Limited by Predefined Scope	Limited by Predefined Scope
Quick Response to New Threats	Testing New Threats in 24 Hours	No Response Until New Engagement	No Response Until New Pentest	Plugin Updates Happen Within 3-5 Days
Risk-free Assessment	✔	✘	✘	✔

BAS technologies have emerged as a critical solution to these challenges. Unlike traditional methods, BAS offers continuous, automated testing of security defenses against a wide array of cyber threats. This approach not only identifies vulnerable points in both prevention and detection layers across the entire cyber kill chain but also provides specific, actionable mitigation suggestions to address these weak points. BAS's ability to simulate real-world attacks continuously and non-disruptively ensures that security measures are tested against known and emerging threats. Furthermore, BAS's automation significantly reduces the burden on security teams, allowing them to focus on prioritized mitigations rather than constantly reacting to new threats.

The comparative analysis demonstrates that BAS stands out as the superior method for security validation in today's threat landscape. By offering continuous, automated, and comprehensive assessments across all security layers, BAS ensures that organizations can swiftly identify and mitigate security weaknesses before attackers can exploit them. This proactive and holistic approach to security validation is not just about keeping pace with cyber threats but also staying ahead, ensuring that security defenses are continuously optimized and ready to defend against new challenges.

ABOUT PICUS

As the pioneer of Breach and Attack Simulation, Picus Security helps security teams consistently and accurately validate their security posture. Our **Security Validation Platform** simulates real-world threats to evaluate the effectiveness of security controls, identify high-risk attack paths to critical assets, and optimize threat prevention and detection capabilities by including:



Attack Surface Validation
Enhance visibility of internal and external cyber assets and the security risks they pose.

Detection Rule Validation
Optimize detection efficacy by identifying performance issues affecting detection rules.

Cloud Security Validation
Identify cloud misconfigurations and overly permissive Identity and Access Management (IAM) policies.

Attack Path Validation
Eliminate high-risk attack paths that attackers could exploit to compromise users and assets.

Security Control Validation
Measure and optimize the effectiveness of security controls with Breach and Attack Simulation.

Elevate your security capabilities with the Picus Security Validation Platform

REQUEST A DEMO

picussecurity.com