Automated Security Validation Platform

PICUS Breach and Attack Simulation

1. Breach and Attack Simulation for Cyber Resilience

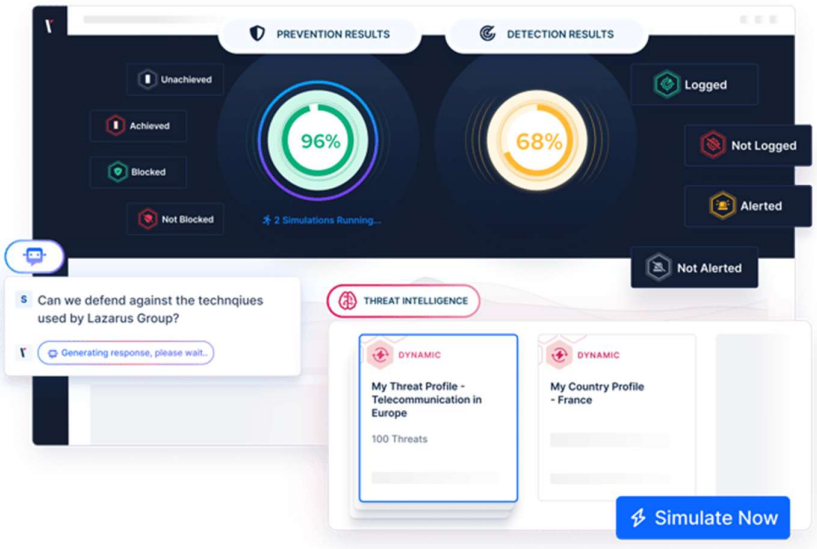
Breach and Attack Simulation (BAS) is a continuous and automated method for testing your defences by safely simulating and emulating real cyberattacks in a controlled environment. It uncovers blind spots, misconfigurations, policy gaps, and silent failures that traditional tools often miss.

Reasons to Validate Your Controls:

- **Configure settings to your environment**
- **Improve efficacy over time**
- **Reduce the risk of IT drift**

BAS helps verify whether your security technologies are doing what they're supposed to do. It shows if firewalls block malicious traffic, if EDRs detect threats, and if SIEMs generate timely alerts. It doesn't guess, it measures.

One of the most practical uses of BAS is validating security controls. This process, called Security Control Validation (SCV), focuses on confirming that your prevention and detection layers are working as intended. BAS powers SCV by running real attack scenarios and collecting measurable evidence of control effectiveness. That's why the next section focuses exclusively on this critical use case.



Security Control Validation

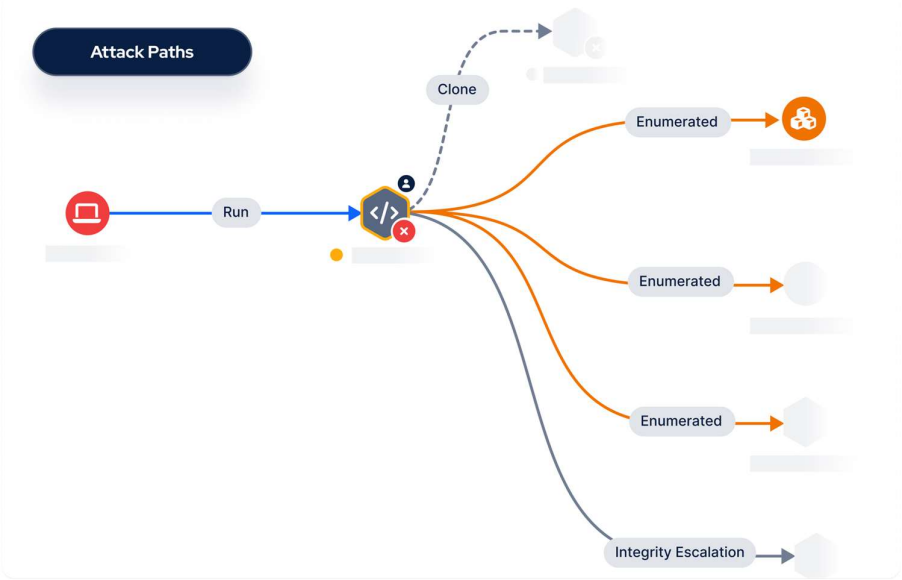
Picus Breach and Attack Simulation validates security controls and strengthens defenses by stress-testing your implemented solutions to identify gaps that adversaries could exploit. The platform not only uncovers vulnerabilities across a variety of security measures but also provides both vendor-specific and neutral mitigation suggestions that are ready to implement. This eliminates the need for manual research and rule validation, saving time and effort.

2. Automated Penetration Testing for Continuous Security

Traditional penetration testing is slow and resource-intensive. Picus Security's automated penetration testing continuously identifies vulnerabilities, validates security controls, and uncovers high-risk attack paths without requiring offensive security expertise. Get faster, scalable, and real-world attack simulations to stay ahead of threats.

Automate Penetration Testing to:

- **Uncover high-risk vulnerabilities**
- **Minimize manual efforts**
- **Achieve complete attack surface visibility**



Automated Penetration Testing Meets Precision

Picus Security combines automated penetration testing with attack path mapping to determine which vulnerabilities are exploitable and shortlist the attack paths.

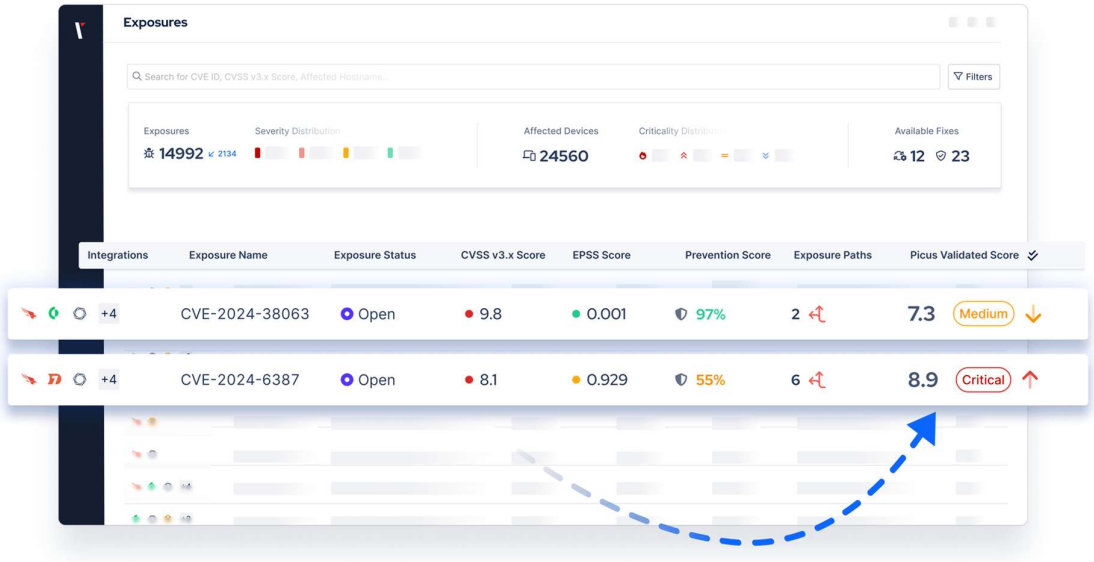
Automated Penetration Testing provides comprehensive coverage, uncovering a wide range of vulnerabilities and exposures across systems. Attack Path Mapping visualizes the most critical chokepoints that lead to domain admin compromise, disruptive ransomware attacks, and more.

With a unique combination of the two, security teams gain comprehensive visibility and targeted precision.

Full-Spectrum Validation

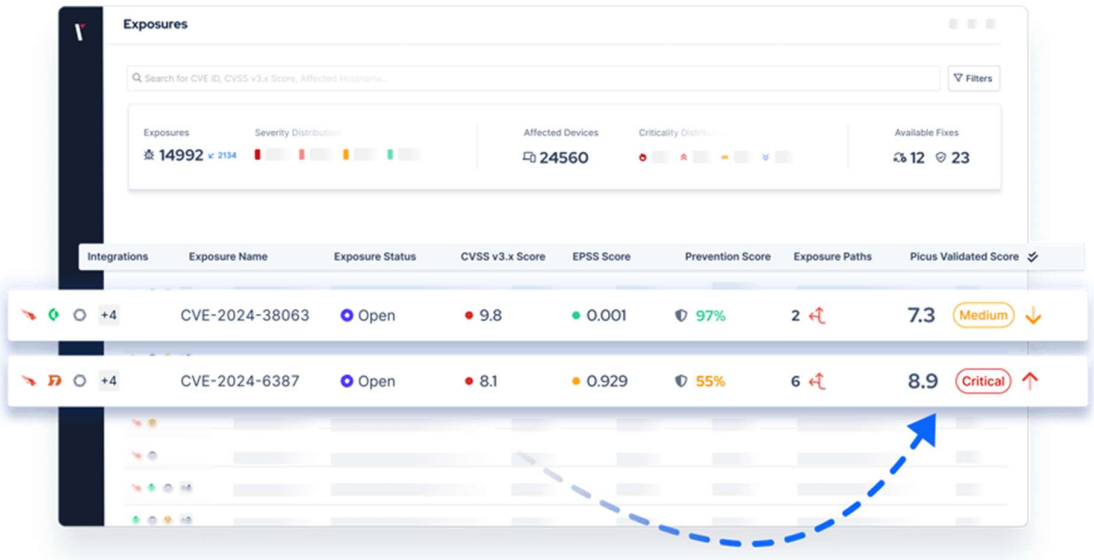
By combining Automated Penetration Testing and BAS, organizations don't just detect vulnerabilities; they validate which security gaps can be chained from the start to full domain compromise. This integrated approach uncovers whether an attacker can bypass firewalls, exploit misconfigurations, escalate privileges, and execute ransomware, while also testing if security controls can detect and stop these actions.

This unique combination drives Exposure Validation, enabling security teams to have end-to-end visibility, prioritize and remediate the exposures posing the greatest risk.



3. Adversarial Exposure Validation

Simulate adversarial attacks to identify exploitable vulnerabilities and prioritize the most critical threats for remediation.



What is Adversarial Exposure Validation?

Adversarial Exposure Validation is a proactive approach to measuring and improving an organization's security posture. By continuously verifying various threats, such as security vulnerabilities, misconfigurations, and control gaps, AEV identifies exposures that attackers can realistically exploit.

Thus, it helps teams filter out exposures with no business-critical impact and focus on the issues that most significantly reduce overall risk.

Reasons to Validate Your Exposures:

- **Separate theoretical risks from actionable ones**
- **Ensure your security controls are prepared for real world attacks**
- **Streamline targeted, non-disruptive remediation**

VAPT & SOC Solutions Strengthening Cyber Defences

1.Build skills through cyber warfare training

A hyper-realistic simulation platform that composes of a cyber range orchestrator, important third party tools, and necessary hardware - designed for modern teams to learn the best Infosec skills by fighting real-world cybersecurity attacks.

2.Accomplish machine- speed incident response & resolution

A unified platform for enhancing security operations with threat intelligence integration, security orchestration, automated response and threat hunting

3.Purple Teaming and Vulnerability Assessment

Our specialized services include vulnerability assessments, penetration testing, and collaborative exercises with Blue Teams, enabling organizations to simulate and defend against cyber threats in real time.

4.SOC Services, NOC Services, Incident Response and Threat Management

We offer 24x7 SOC services in collaboration with our partners. Purplesynapz Managed Incident Response Platform provides real-time threat intelligence aggregation and automated response capabilities, allowing clients to maintain a proactive security posture.

5.Splunk Development and Customization

Expertise in Splunk integration and custom app development tailored for MSPs, providing clients with advanced SIEM and identity management capabilities.

6.Knowledge Base (Purplebox)

Unleash Your Inner Hacker with our PurpleBox & Master Cybersecurity Attack and Defence

Virtual Academy

Learn top cybersecurity courses online

7.Cybersecurity Training Programs

From foundational programs for freshers to advanced corporate training, we offer various options:

Cyber Ramp Up: Tailored training for entry-level professionals.

Corporate and Long-Term Skill Development: Programs that transition L1-levelstaff to L2 proficiency, enhancing operational efficiency and expertise.

Cyber Academia Collaborations: Degree and vocational courses in partnership with educational institutions.