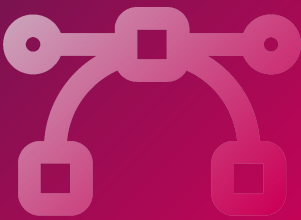


Picus Autonomous Penetration Testing

Defensible Decisions, Proven by Real Attack Chains



Picus Autonomous Penetration Testing runs AI agents that chain real-world attacks across your environment to reveal which exposures are genuinely exploitable and how to close them, all within the guardrails you define.

Problem:
Expanding Attack Surface & Unproven Risk

Metric	Pain Point
~135 new CVEs / day ¹ , and 0.5% ever patched ²	Backlog grows faster than any team can safely clear
Unproven exploitability	A flagged CVE may not actually be exploitable
Score-based triage	Every call rests on assumptions, not evidence

Solution:
Picus Autonomous Penetration Testing

AI agents chain real exploits across hosts, identities, and misconfigurations to reach your crown jewels, safely and continuously, in production.

- **Act on real risk:** exploitability and blast radius, not severity.
- **Cut wasted effort:** fix what matters, then re-validate it.
- **Decide on evidence:** a real exploit chain behind every call.

Built for AI-speed threats
Runs the loop, **24/7**

AI agents adapt and chain techniques as they go, so your validation keeps pace with threats that now move at AI speed.

Respond faster
89% Lower MTTR³

Evidence-backed response to the exposures that actually matter, not the ones that merely look urgent.

Stop firefighting
92% Fewer SLA breaches⁴

On high & critical vulnerabilities: fewer escalations, defensible exceptions, audit-ready records.

Core Capabilities

- ✓ **Attack surface mapping**
Enumerate external assets, internal networks, identities (AD / Entra), and misconfigurations across the environment.
- ✓ **Credential brute-forcing**
Test credential-based attack vectors to expose weak authentication in Active Directory and remote access services like SSH, FTP, Telnet, and VNC.
- ✓ **Real, safe exploit chains**
Launch and chain real-world exploitation across hosts autonomously, within the guardrails you set.

- ✓ **Proof of compromise, by blast radius**
Reach crown-jewel assets and capture concrete evidence of the choke point that breaks the chain: proof ordered by reachable impact, not CVE counts.
- ✓ **Staying current with full chain of custody**
Schedule runs, launch on demand, or let it validate itself on new CVEs, drift, and emerging TTPs. Tunable autonomy, fully supervised, or anywhere in between.
- ✓ **One-click re-validation**
Get fixes written for your exact stack, then re-run the exact path to confirm the gap is closed, in minutes, not weeks.

¹ 2025 Vulnerability Forecast: Year-End Review by FIRST, ² Project Glasswing: An initial update by Anthropic, ³ & ⁴ Picus Customer Results

Picus Autonomous Penetration Testing

One part of the Picus validation loop

Picus Autonomous Penetration Testing is the real-world exploitation engine of the Picus Platform. It works alongside two other validation components in a continuous loop, validate, decide, fix, re-validate, so you act on what attackers can truly exploit and back every decision with a real attack chain.

Security Control Validation
Breach and Attack Simulation
Picus Breach and Attack Simulation continuously tests the live stack to validate which prevention and detection controls actually work.

This Product
Autonomous Pentesting
Executes real exploit chains against reachable assets to show what an attacker can actually reach and do, safely, in production.

TTP-Chain Validation
Exposure Validation
Proves exploitability without firing an exploit, covering the restricted assets and CVEs no live test can safely touch.

Can you answer “is it exploitable here?” for...	AUTONOMOUS PENTEST ALONE	PICUS VALIDATION LOOP
Reachable assets with a known, safe exploit	● Yes	● Yes Picus Autonomous Pentesting
Business-critical, restricted, or air-gapped assets	No	● Yes Exposure Validation + BAS
CVEs with no available exploit	No	● Yes Exposure Validation + BAS
Brand-new CVEs, on the day of disclosure	Not until an exploit ships	● Yes, immediately
Whether the decision stays defensible over time	No	● Yes, continuously re-validated

AI Built for Security Teams

AI accelerates Breach and Attack Simulation across the Picus Platform, generating custom, ATT&CK-mapped threat scenarios from intelligence reports through AI Threat Builder, correlating attack data, and guiding remediation through Numi AI.

picussecurity.com

Experience Picus *in Action*

GET A DEMO



4.8/5.0
#1 Solution Provider*
Breach and Attack Simulation
*G2, Breach and Attack Simulation (BAS) Solutions, Fall Grid Report, 1 September 2026



4.8/5.0
Highest-rated vendor*
Adversarial Exposure Validation
*Gartner, Voice of the Customer for Adversarial Exposure Validation, Peer Contributors, 27 August 2026