PENTERA

PENTERA AUTOMATED SECURITY VALIDATION™

Build your roadmap to exposure reduction

Security validation meets automation

An attack surface that has never been greater has made protection against sophisticated threat actors increasingly complex and time-consuming. As a result, security practitioners and regulators have never been more keenly aware of the need to integrate the adversary perspective into an organization's ongoing cyber defense strategy. However, siloed manual penetration testing and static vulnerability scanners fail to deliver on this need.

Pentera addresses this need with our Automated Security Validation™ platform that tests, assesses, and reduces corporate cybersecurity risk so you can know where you stand at any given moment. Running remotely on the cloud or on-prem, Pentera immediately puts to action a risk-based remediation roadmap by continuously emulating real-life attacks and validating the efficacy of your defensive controls.

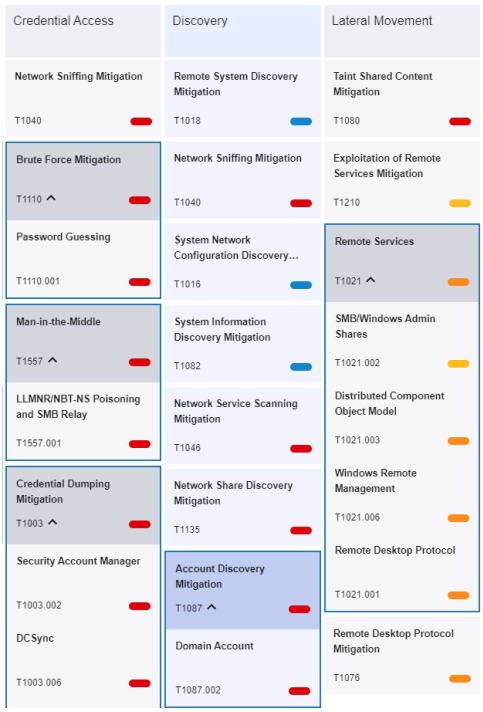
Use cases

- Security controls validation
- Automated Penetration Testing
- Risk-based vulnerability management
- Purple team practices
- MITRE ATT&CK alignment

Harden the enterprise

Security teams invest in preventative controls across the organization's perimeter with the goal of protecting the enterprise and reducing cyber risk. However, how confident can they really be that these defense controls are operating as designed? Shifting to automated validation of your security controls is required to manage the true exposure of critical assets. Pentera continuously improves cyber resiliency by optimizing the efficacy of defenses and reducing time-to-remediate. Validate without any agents. Legacy agent-based security attack simulation tools introduce overhead and coverage gaps that fall short of expectations. Pentera on the other hand validates without any prior installation or network configuration, providing security teams a complete view of their attack surface and security gaps. With Pentera's agentless approach you get immediate discovery and validation across a distributed and hybrid network infrastructure.

MITRE ATT&CK for enterprise



Achieve unprecedented speed and scale

When it comes to assuring cyber protection, speed and scale are top priority. However, these can be difficult to achieve with the limitations of incumbent solutions. The key to speed and scale is automation. The Pentera platform delivers on these needs by harnessing the built-in knowledge and ethical hacking experience of a thousand pentesters. Alongside Pentera's agentless architecture we help you discover, exploit, analyze, and create a complete red team operation automatically.

PENTERA

Prioritize and remediate with confidence

You have a long list of known static vulnerabilities sorted by CVSS ranking. Great. But - are each of these vulnerabilities real? and do you know which poses the highest risk? When lacking meaningful risk prioritization and actionable context, these questions remain unanswered, causing weaknesses to be piled on to an already long backlog. Pentera applies conclusive prioritization insight that speeds up surgical remediation steps against the vulnerabilities that pose the greatest risk to your organization.

Make false positives a thing of the past

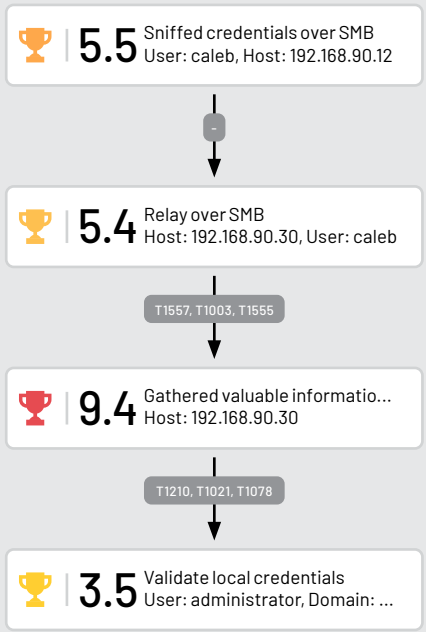
As your digital footprint grows, so do vulnerabilities and weaknesses. But not all vulnerabilities were created equal, and not all deserve your attention. So, how can you make sure your team is at top efficiency? Pentera offers a risk-weighted view that enables you to prioritize security gaps based on severity, exposure, exploitability, and business impact. This is how the Pentera platform enables your team to deal with increasing workloads and volumes of vulnerabilities driving unprecedented efficiency.

Key benefits

- Accelerated validation-remediation cycle
- Reduced third party testing reliance and expenses
- Increased cybersecurity team efficiency
- Seamless deployment and operation

Model attacker behavior

The effectiveness of your security program is directly related to your ability to think and act as your adversary would and do so before they attack. Knowing what the attacker's next move will be or where the next impactful breach may appear is an ambitious undertaking. Pentera helps you to achieve this goal by harnessing the capabilities of red-team frontline experience, a broad array of real-life hacking techniques, attack frameworks aligned to MITRE ATT&CK, and an ethical exploits arsenal. Armed with the attacker's perspective, you can now automatically expose security program gaps that would typically take a skilled pentester weeks to uncover, without prior knowledge of network topology.



Assure a program that is safe by design

Production-grade safety is a promise we live by, where multiple safeguards are easily configurable (range, scope, time, stealth) and rigorous, uncompromising tests are conducted for assurance. Hundreds of organizations trust Pentera and our do-no-harm policy, without ever locking out users, with no denial-of-service to the network, and with no out of scope testing criteria.

Learn more at www.Pentera.io

Put Pentera Platform To The Test