Continuous Threat Exposure Management (CTEM)

Accelerate CTEM Adoption with Real-World Adversarial Exposure Validation

Build cybersecurity resilience by turning threat exposure insights into evidence-based action plans.

The Pentera Automated Security Validation platform challenges your defenses like an adversary and discovers exploitable security flaws. Emulate real-life attacks in your production IT environment to uncover true security gaps and ensure continuous security readiness.

Key Capabilities

Continuous Attack Surface Assessment
Find out where you are vulnerable by monitoring your internal, external, and cloud attack surfaces.

Risk-Based Prioritization
Prioritize proven exploitable security gaps based on their potential level of business impact.

Exposure Validation Testing
Reveal complete attack kill chains and know the true impact of vulnerabilities in your live environment.

Surgical Remediation Guidance
Eliminate critical attack paths with clear step-by-step guidance. Re-test to validate your security posture and confirm fixes.

Improve Your Cybersecurity Posture with CTEM

Continuous Threat Exposure Management (CTEM) is an emerging framework for ongoing proactive risk reduction. The goal of CTEM is to establish a systematic approach to identifying, prioritizing, and mitigating security gaps by continuously assessing and validating IT security posture. Organizations adopting CTEM can address potential risks early, adapt to evolving IT infrastructure and adversary techniques, comply with security policies and regulations, and enhance their resilience against cyber threats.

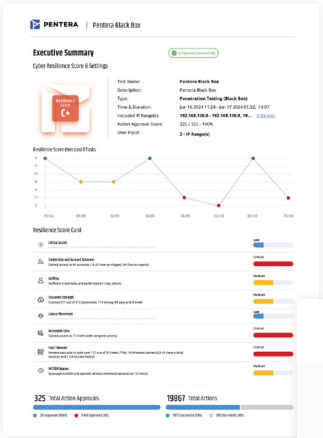
By 2026 organizations that prioritize their security investments based on a continuous exposure management program will be three times less likely to suffer a breach.

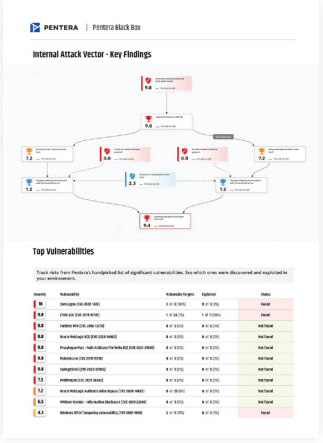
Gartner, "How to Manage Cybersecurity Threats, Not Episodes", August 21, 2023

At the Core of CTEM: Pentera's Adversarial Exposure Validation

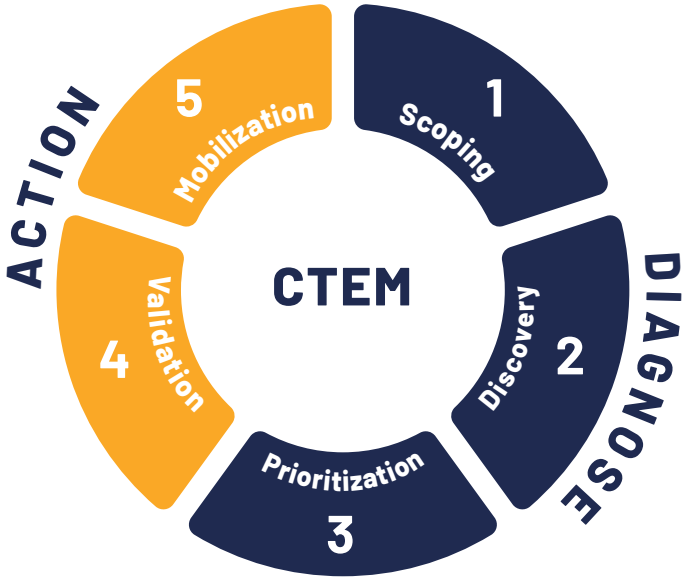
Adversarial exposure validation is a critical element within CTEM. It is essential for pinpointing true security gaps and ensuring defenses can withstand actual attacks, driving a resilient defense against cyber threats.

Pentera offers unparalleled depth and breadth in automated, algorithm-based attacks. Pentera's platform conducts real attack techniques in live IT environments, ensuring safety by design. IT security, blue / red / purple teams, and SOC teams leverage Pentera to validate their cyber readiness anytime—daily, weekly, or monthly. Pentera provides detailed reports with actionable insights and step-by-step remediation guidance, enabling the effective identification and resolution of critical gaps.





Pentera Supports All Stages of CTEM



1. Scoping:

Define the attack surfaces of focus for threat exposure management to support business objectives.

Pentera maps your IT assets and associated attack surfaces. See your internal, external-facing, and cloud infrastructure through the lens of an adversary to identify the areas with the highest risk exposure.

2. Discovery:

Identify assets, vulnerabilities, and potential threats within the defined scope.

Pentera automates reconnaissance, enumeration, and vulnerability scanning on defined IT scopes. Uncover software vulnerabilities, misconfigurations, exposed credentials, and other security gaps.

3. Prioritization

Rank exposures and threats based on risk to the organization.

Pentera finds exploitable vulnerabilities, misconfigurations, and other security gaps in your live environment that allow adversaries to compromise your critical assets. Prioritize the highest-risk gaps based on proof.

4. Validation:

Test the effectiveness of security measures and remediation efforts.

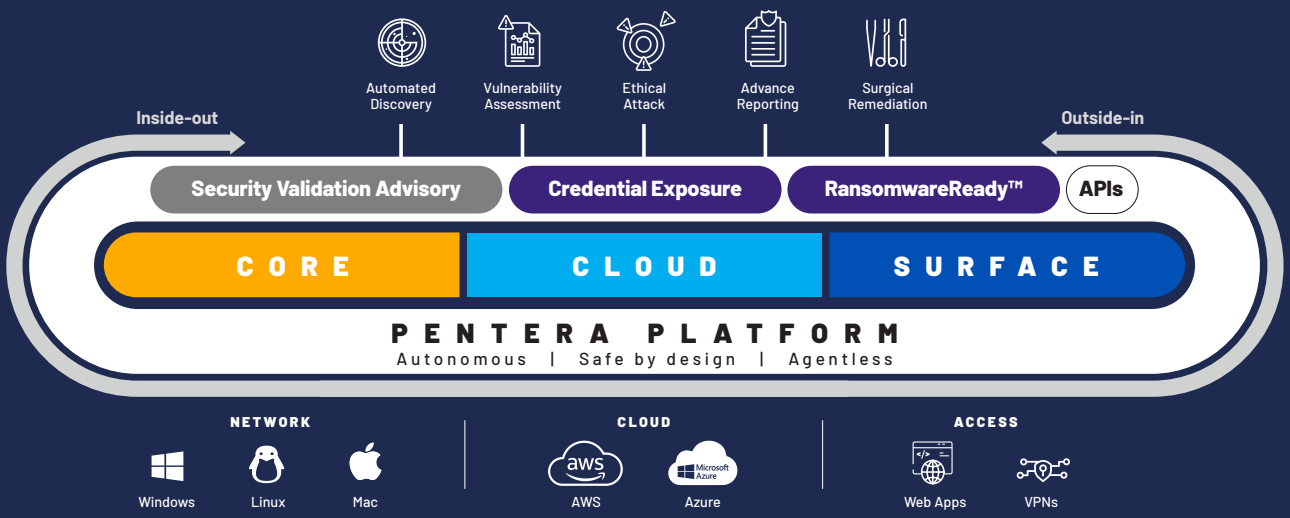
Pentera runs complete attack kill-chains, mimicking the behavior of an adversary. Assess vulnerabilities and security controls' effectiveness based on a true view of what attackers can achieve.

5. Mobilization

Implement improvements and adjust strategies based on findings and validations.

Pentera provides exposure insights and actionable remediation guidance on a continuous basis. Build collaboration and demonstrate continuous security posture improvement.

All your attack surfaces, tested continuously with the Pentera Platform



About Pentera

Pentera is the market leader in Automated Security Validation™, empowering companies to proactively test all their cybersecurity controls against the latest cyber attacks. Pentera identifies true risk across the entire attack surface, guiding remediation to effectively reduce exposure. The company's security validation capabilities are essential for Continuous Threat Exposure Management (CTEM) operations. Thousands of security professionals around the world trust Pentera to close security gaps before threat actors can exploit them.