

UEMP PTaaS

Structured penetration-testing workflow from engagement to retest.

OPERATIONALIZE PENETRATION
TESTING FROM SCOPE TO VALIDATED
CLOSURE.

Product Overview

InVinsense UEMP Penetration Testing as a Service (PTaaS) manages manual penetration-testing engagements as a structured workflow with defined roles, controlled status transitions and asset-linked scope. It carries findings through remediation, retesting, reopening or formal risk acceptance and produces consistent branded reports. It replaces isolated, point-in-time pentest engagements with a governed, always-available testing model that closes findings faster and proves remediation with evidence.

Key Capabilities

Capability	What It Delivers
Engagement lifecycle	Manage request, approval, scheduling, testing, review and completion.
Scope synchronization	Add in-scope targets to the central asset inventory.
Structured finding workflow	Support developer fixes, pentester retesting, reopening and risk acceptance.
AI-assisted finding drafting	Assist descriptions, reproduction steps, impact and remediation.
Vulnerability library	Reuse finding templates through import and export.
Tool import	Import results from Burp Suite Pro, OWASP ZAP, Nessus and Acunetix.
Branded reporting	Reuse PwnDoc-style templates and generate branded reports.
Pentester workspace	Provide focused queues for assigned engagements and findings.

Business Outcomes



Govern penetration-testing engagements from request to completion.



Synchronize scope with the central asset inventory.



Track finding closure through fix, retest, reopen or accept-risk decisions.



Accelerate reporting with reusable templates and AI-assisted drafting.



Provide a focused workspace for pentesters and reviewers.



Use Cases



Engagement governance

Keep roles, approvals and status transitions controlled.



Reusable delivery

Standardize common findings and report templates.



Validated closure

Track remediation and confirm fixes through retesting.



Evidence and reporting

Produce structured outputs for technical and executive audiences.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation.

Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.

Gartner®

Infopercept is recognized as a representative vendor in multiple Gartner® reports

- UEMP (Exposure Management)
- AMTD (Preemptive Security)
- AEV (Security Validation)

[Learn More](#) →



Ready to try it out?

Sign up for a demo. Visit infopercept.com/book-a-meeting

Infopercept



Attacker's Mind. Defender's Brain.®

© Infopercept 2026

Contact us at
sos@infopercept.com

For more details visit
[Infopercept.com](https://infopercept.com)

Engage With Us  