Cobalt

Checklist for Evaluating PTaaS Vendors

Penetration Testing as a Service (PTaaS) transforms traditional pentesting into a strategic advantage by offering speed, scalability, and on-demand expertise. When evaluating PTaaS providers, security leaders should consider the following seven key factors to ensure the solution meets their organizational needs:

01 Speed and Agility

The ability to kick off pentests in 24 hours, receive reporting on vulnerabilities in real-time through a platform, and get rapid retesting are the hallmarks of top PTaaS platforms. This rapid turnaround allows organizations to test new products before launch without waiting for lengthy scheduling processes.

- ❐ How quickly can I start a pentest?
- ❐ How long does it take to get a report (on average)?
- ❐ Are findings delivered in real-time to enable faster prioritization and remediation? (As opposed to having to wait for the final report)

02 Expertise and Pentester Quality

People are the core of any offensive security engagement. The advantage of PTaaS is access to the experienced pentesters with a breadth of expertise such as support for niche technologies, without the overhead or risk of hiring and managing full time employees.

- ❐ How many pentesters (not bug bounty participants) are active in your community?
- ❐ How many years of experience do your pentesters have on average?
- ❐ What is the vetting process for pentesters? What certifications do they have e.g. CEH, CISSP, OSCP, or CREST?

03 Vendor Rotation

One of PTaaS's unique advantages is the ability to retain historical asset data within a consistent platform while rotating pentesting teams to get a fresh perspective. This fulfills the need for vendor rotation by leveraging the built-in diversity of a broad community of pentesters.

- ❐ Is the platform capable of rotating pentesters to ensure fresh perspectives while retaining historical asset knowledge?
- ❐ Does the platform support deep integrations into other systems to make actioning findings easy?

04 Collaboration and Transparency

PTaaS encourages direct collaboration between security teams and pentesters, ensuring that access issues are resolved quickly and findings are clarified in real time. This collaborative approach accelerates remediation and strengthens security knowledge.

- ❐ Do you enable direct collaboration between security teams and pentesters?
- ❐ Do you provide transparency through features like progress checklists and detailed methodologies?
- ❐ What happens if there is a critical finding; how is this communicated?
- ❐ What if my team has questions about the findings?
- ❐ How do findings get into my team's backlog? Are findings integrated into existing tools?

05 Retesting & Fix Validation

Instead of waiting to retest all vulnerabilities at once, PTaaS enables retesting on a per-finding basis. This ensures that critical vulnerabilities can be addressed as soon as they are fixed, rather than waiting for all findings to get addressed.

❐ Can retesting be done on a per-finding basis to ensure critical vulnerabilities are resolved quickly?

❐ What is the SLA or an average turnaround time for retesting to confirm fixes?

❐ Is retesting included at no cost?

❐ What is the retesting window?

06 Scalability & Flexibility

PTaaS can support a wide range of assets and a large number of concurrent tests to meet the demands of growing businesses. Leading PTaaS providers support complementary capabilities such as external attack surface monitoring and DAST to deliver a continuous view of organizational risk.

❐ Do you support specialized expertise for pentesting APIs, mobile apps, IoT, or LLM applications?

❐ Can you scale to meet the needs of growing organizations with multiple concurrent tests? How would you handle testing 50 applications at one time? How do you meet that need?

❐ What additional capabilities do you provide to complement pentesting efforts?

07 Customizable Reporting & Insights

PTaaS platforms offer customizable reporting to ensure stakeholders receive the information they need, in the format they require.

❐ Does the platform offer customizable, interactive reports tailored to compliance needs, board-level summaries, and customer attestations?

❐ Are reports designed to provide actionable insights to both technical and non-technical stakeholders?

A robust PTaaS solution provides the speed, expertise, scalability, and transparency necessary to transform penetration testing into a proactive security advantage.

**Ready to see how PTaaS can elevate your security program?
Get a demo of Cobalt today at www.cobalt.io/get-started**