Why is Pentest as a Service Better for Engineering Than Traditional Pentesting?

Traditional Pentesting

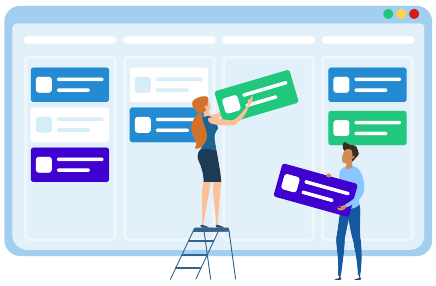
Pentest as a Service

Tools

Disconnected

Few to no shared digital tools, findings are lumped in a PDF report and sent over email

Integrated



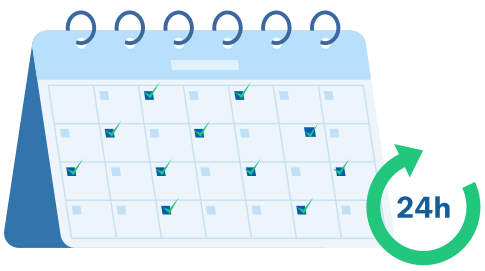
Cloud platform with bi-directional Jira and GitHub integrations and simple test reproductions

Alignment With Sprints

Restricted

Pentests have to be scheduled months in advance and happen once or twice a year despite frequent code deployments

Flexible



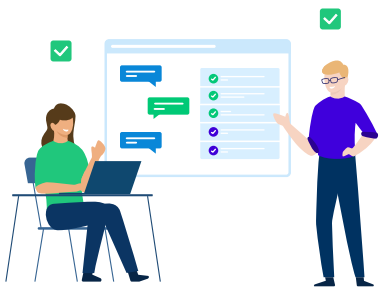
On-demand tests begin in 24 hours either ad-hoc or as part of a flexible pentest program in sync with the release tempo

Remediation

Siloed

Limited information on bug reproduction and communication overhead between engineers, pentesters and security

Collaborative



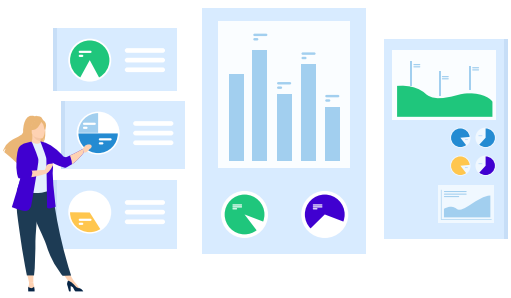
Descriptive findings delivered in dedicated communication channels where engineers and testers can collaborate in real time

Analytics

Vague

Limited exposure to data on vulnerabilities' criticality and distribution along the codebase, or engineering's impact on the company's security posture

Detailed



Dashboards display aggregated risk, vulnerability severity and distribution across assets for informed prioritisation and performance tracking

Learn more about how Pentest as a Service bridges the gap between DevOps and Security:
https://resource.cobalt.io/pentesting-in-devops-how-to-guide

Cobalt
Pentest as a Service