Pentesting Use Cases

OVERVIEW

Pentesting can do more for your security program than just fulfill compliance obligations. If your team is launching a new feature, making code changes to an existing feature, or preparing for an M&A, pentests can help maintain critical security standards. The best part? With Cobalt, you can pentest for a wide range of scenarios without sacrificing your agility and speed.

USE CASES

Compliance Testing

Pentest to meet or maintain compliance.

Examples: SOC 2, PCI-DSS, ISO 27001

Comprehensive

M&A Due Diligence

Pentest to identify and eliminate any risks for all sides involved in an M&A transaction.

Comprehensive

Delta Testing

Pentest for incremental improvements based on code differences since date or version.

Example: Changes to an existing asset

Agile

Exploitable Vulnerability Testing

Pentest a single vuln or small subset of vulns across an asset to validate fixes.

Example: Log4j

Agile

Customer Requests

Pentest to adhere to a customer or third party attestation request.

Comprehensive

New Release Testing

Pentest a new release before or shortly after it reaches production.

Example: New feature

Agile

Single OWASP Category Testing

Pentest a single OWASP category for a web/mobile/API asset.

Example: Access control

Agile

Microservice Testing

Pentest kubernetes within AWS, Azure, or GCP, as well as hosted network services.

Example: Serverless application testing

Agile

PARTNER WITH COBALT FOR YOUR PENTESTING NEEDS

Cobalt's Pentest as a Service (PtaaS) platform is paired with an exclusive community of testers to deliver the real-time insights you need to remediate risk quickly and innovate securely. The flexible, on-demand consumption model enables security and development teams to proactively meet modern pentesting needs.

Cobalt buckets pentests into two offerings: Comprehensive Pentesting and Agile Pentesting.

A **Comprehensive Pentest** encompasses all vulnerability categories across an asset. It is broad in scope, and requires a report as a final deliverable. Examples of Comprehensive Pentesting include compliance testing, testing for customer requests, and M&A due diligence.

- Meet or maintain compliance frameworks, such as SOC 2, ISO 27001, PCI-DSS, CREST, and HIPAA
- Adhere to a customer or third party attestation request
- Identify and eliminate any risks in an M&A transaction

An **Agile Pentest** focuses on a specific area of an asset, or a specific vulnerability across an asset, is flexible in nature, and usually has a smaller scope. The final artifact for an Agile Pentest is an automated report, intended for internal use. The most common use cases include new release testing, delta testing, exploitable vulnerability testing, single OWASP category testing, and microservice testing.

- Test a new release or code change before it reaches production
- Validate fixes on a single vuln or small subset of vulns across an asset
- Target a single OWASP category for a web/mobile/API asset

"Datto's pentesting program is evolving by using Agile Pentesting, as we're able to schedule more pentests and allow ourselves to only look at the delta between the last pentest that was run and the newer pentest that would then occur. This gives us a better idea of what has already been tested and only focuses on the newer portions instead of always going to the same parts of the product that may not have changed over the course of a year, six months, or three months."

Jeremy Galindo
Offensive Security Manager | Datto

Interested in learning more?

Visit us today at www.cobalt.io