SOFTWARE SECURED

Pentest Buyers Guide

Everything you need to know to select the right penetration testing partner and maximize the value of your security investment.

17+ Questions
Answered

15min read
Comprehensive

Expert Vetted
Best practices

Table of Contents

1 Methodology & Quality

1 What testing methodology do you primarily follow?

Our pentesting aligns with industry-standard frameworks including:

- OWASP Top 10 - Critical web application security risks
- SANS Top 25 - Most dangerous software errors
- ASVS Level 1 - Application Security Verification
- Standard WSTG - Web Security Testing Guide
- NIST - National Institute of Standards and Technology

AI pentesting aligns with MITRE ATLAS, Google SAIF, and OWASP Top 10 for ML.
Mobile pentesting aligns with OWASP Mobile Top 10.
Backed by industry-specific test plans, informed by active attack patterns.
OWASPTop 10 SANS Top25 NIST

2 What is the typical split between manual and automated testing?

Our pentesting is ~90% manual effort. We leverage scanning tools and automation to speed our efforts and cast a wide net; however, the majority of the engagement is human-led hacking. On average, we find 26 vulnerabilities per web application pentest; 20% being critical or high.

We conduct product demos and light threat modelling during kick-off calls to build custom attacks tailored to your business logic and data flow - this yields more severe vulnerabilities that external threat actors would find.

3 Do you manually validate all findings to ensure zero false positives?

100% - we know our clients are busy and our reputation matters. All pentest reports go through QA with another pentester, and scoring is calibrated to 2 industry standards (CVSS 4.0 and DREAD) to remove any false positives and ensure quality.

4 What certifications do your testers typically hold?

All testers are FTE based in Canada and are required to possess at least one of: **OSCP, OSEP, GSSP, GWAPT, CEH, CREST, or CISSP.**

2 Scope & Approach

Testing Types Explained

Black Box Testing
Simulates an external attacker with no prior knowledge of your systems. Narrowest scope, budget-friendly. Meets standard compliance requirements (SOC 2) but provides less depth and coverage.

Gray Box Testing
Simulates an authenticated attacker with user-level access. Industry best practice for SaaS companies. Enterprise customers often require this level of security because it provides deeper coverage. Recommended for most SaaS companies.

White Box (Secure Code Review)
Simulates an attacker with full access to your source code. Highest level of depth and visibility into risk. Recommended for companies processing PHI or operating in regulated industries.

6 Which testing approach do you recommend?

For most SaaS companies, we recommend scoping both gray box and black box tests:

- Grey box is the industry's best practice for enterprise security requirements.
- A black box provides an external network assessment.
- We include an external black box network pentest with every authenticated gray box web app pentest.

7 How do you handle multi-site architectures?

For architectures with multiple client-facing websites sharing the same back-end, we recommend testing a staging environment of the shared back-end and a sample front-end site. Testing every site would become costly and likely produce redundant vulnerabilities.

8 Does testing include real-world attack chaining?

Yes! We include a Highest Threat Summary with gray-box pentests that outlines how multiple vulnerabilities could lead to a larger issue or highlight a theme in an area of improvement for your security posture.
We've found critical breaches by chaining together lower-severity vulnerabilities.

3 Reporting & Remediation

9 What deliverables are included?

- Executive summary - external facing for clients, partners and auditors
- Detailed technical report - internal facing for developers, IT and security teams Risk ratings with every vulnerability
- Remediation guidance
- Retesting (multiple rounds available based on scope)
- Readout report meetings
- Dedicated Slack channel for pentester communication
- Portal dashboard - custom SLAs, ticketing integration and compliance mapping

10 How do reports support SOC 2 Type II evidence requirements?

We offer one-way sync with Drata and Vanta GRC automation tools. Pentesting directly supports:

- CC7.1 - Monitoring
- CC7.2 - Vulnerability management
- CC4.1 - Ongoing and separate evaluations

We also map vulnerabilities to SOC 2 controls and are SOC 2 attested ourselves, in addition to mapping to ISO 27001, HIPAA and PCI-DSS.

4 Retesting Policy

Retesting Rounds

- Black Box: 1 round of retesting included
- Gray Box: 3 rounds of retesting included
- PTaaS: Unlimited retesting for biannual/quarterly/monthly clients

Retesting available for 6 months after report delivery. SLAs: 15 days critical, 1 month high, 3 months medium, 6 months low.

5 Timeline & Process

12 What is the typical timeline from kickoff to final report?

Generally, we book 3-6 weeks out as we are a manual shop. Once the pentest is completed, we take 2 days for QA before shipping the final report. Need this faster? Tell us your deadline - we'll do our best to prioritize and accelerate where possible.

If you need to change testing dates, we require at least 2 weeks' notice.

13 How collaborative is the process?

You will have:

- A dedicated pentester to work with
- A Pentest Manager (Senior Pentester) overseeing the kick-off and support Account Manager for ongoing support
- Portal for project management

We provide draft reports when we find critical vulnerabilities in production, allowing clients to remediate before test completion.

Average Preparation Time
On average, clients take 8 minutes to complete the preparation checklist in the Portal.

6 Pricing & Engagement

BLACK BOX PENTEST

$5,400 Starting price

- External networktesting
- 1 round of retesting included
- ~8 vulnerabilities found on avg
- Meets standard SOC 2 compliance

Learn more ->

GRAY BOX PENTEST

Recommended

$10,800 Starting price

- Authenticatedwebapp testing
- 3 rounds of retesting included
- ~26 vulnerabilities found on avg
- Includes black box network test

Learn more ->

15 For subsequent engagements, do you perform full re-tests or delta testing?

Annual pentests are full pentests on the entire app, as new CVEs are found every day and code changes over time. For PTaaS (more frequent than annual testing), subsequent tests focus on the delta and cost fewer days of testing once the baseline app has been pentested.

When to Consider PTaaS

Usual triggers to invest in more frequent pentesting:

- Pushing so much code each sprint that annual pentests create too much risk Contractual mandates from major clients
- Recently raised funding and growing dev team faster than security
- Want to reduce the bottleneck of annual remediation work

Learn more about PTaaS ->

7 Crowdsourced vs Full-Time Pentesters

When deciding between crowdsourced and full-time pentesters, it's essential to consider how each aligns with your organization's security needs, long-term goals, and budget.

Crowdsourced Pentesters

External cybersecurity professionals who participate in bug bounty programs or are contracted by pentesting firms. Platforms like Bugcrowd, HackerOne, and Synack connect organizations with a global pool of skilled testers.

Full-Time Pentesters

Cybersecurity experts employed directly or through dedicated firms. They have deeper understanding of your business logic, systems, applications, and security requirements.

8 External Pentest vs Vulnerability Scanning

Understanding the Difference

The difference between external network penetration testing and vulnerability scanning is significant. Each approach has its own advantages and disadvantages, and knowing when to use each one is crucial.

Feature	Vulnerability Scanning	Penetration Testing
Purpose	Identify weaknesses	Exploit & validate
Depth of Analysis	Surface-level	Deep analysis
Methodology	Automated scans	Manual + automated
Skill Level Required	Low to medium	High expertise
False Positive Rate	Higher	Zero (validated)
Business Logic Testing	No	Yes

9 Testing Tools & Resources

A selection of open source and commercial tools used in our pentesting engagements:

NETWORK / INFRASTRUCTURE LAYER

Nmap
Network discovery & port/service scanner for host enumeration and OS detection

Nessus
Commercial vulnerability scanner for network/host assessment and compliance checks

DNSRecon
DNS enumeration and zone/record discovery tool for domain reconnaissance

WEB APPLICATION LAYER

Burp Suite Full-featured web security testing proxy suite	**ffuf** Fast web fuzzer (directory/virtual-host/parameter fuzzing) written in Go
sqlmap Automated SQL injection detection & exploitation tool	**AppScan** Enterprise application security scanning suite

RECON / OSINT

subfinder Fast passive subdomain discovery using many passive sources and APIs	**reconFTW** Automated reconnaissance framework bundling subdomain enumeration, scans, OSINT and fuzzing
cloud_enum Multi-cloud OSINT enumerator for public cloud resources across AWS/Azure/GCP	**BBOT** Multipurpose OSINT/recon scanner for automated recon workflows

10 Preparation Checklist

Key Preparation Steps

- Prepare staging environment with production-equivalent configuration
- Gather IP addresses and URLs for external network testing
- Create test accounts with appropriate role levels
- Document any areas of concern for the security team
- Notify relevant stakeholders about testing windows