DECISION TREE

Choose a pentest that matches your business risks

Without the right access, a pentester may miss problems behind the login page.

WHAT IS INSIDE

- [ ] Choose one of three testing approaches
- [ ] Prepare accounts and required materials
- [ ] Send a ready-to-use request to the provider

For: Business owners, CTOs and technical leaders

🖨️ **The last page is for printing**

Veiltrack

Independent security testing

DECISION TREE

The situation

A company orders a pentest of its customer portal. The pentester receives only the website address, so they may miss whether customers can access each other's invoices.

A pentest checks for security vulnerabilities. The approach determines what access and information the pentester receives.

For most business applications, start with grey box: provide separate test accounts to check features after login.

DECISION TREE

01 / 05

Identify the risk you want to test

Read the brief. Is it clear what needs testing: external access, other users' data, user permissions or code flaws?

> The brief only says 'check the website for vulnerabilities'.

→ **Name the specific risk and use the decision guide to choose an approach.**

02 / 05

List the systems and features to test

Compare the brief with the application. Does it cover the customer portal, payments, admin pages and data exchange between systems?

> The brief only includes the homepage address.

→ **Add the required addresses and features. Agree on the list with the provider.**

03 / 05

Create separate test accounts

Log in to each account. Check that the two customers have different test data and all required roles are available.

> There is only one customer account. Access between customers cannot be compared.

→ **Create the missing accounts. Check logins and test data.**

04 / 05

Document who can do what

Read the permissions guide. Is it clear who can view invoices, change payments and manage other users?

> Nobody knows who is allowed to see other customers' invoices.

→ **List the permitted actions for each role. Share this with the provider.**

DECISION TREE

05 / 05

Share materials and agree on the rules

WHAT GOOD LOOKS LIKE

The provider received required materials. Both sides agreed on boundaries, restrictions, contacts and secure access sharing.

HOW TO CHECK

Compare the materials with the brief. Are prohibited actions, the main contact and a secure way to share access defined?

SIGN OF A PROBLEM

The provider does not know the restrictions or has no contact person.

WHAT TO DO

Agree on restrictions and a contact person. Share access securely.

DECISION TREE

DECISION

What exactly do you need to test?

What an outsider can see without logging in
Choose black box. The pentester will test the agreed external addresses without provided accounts.

Whether users can see others' data or bypass permissions
Choose grey box. Provide two independent customer accounts and accounts for other required roles.

Whether payment, login or permission code has flaws
Choose white box. Provide the source code and system architecture overview. Test the running application too.

DECISION TREE

READY-TO-USE SCRIPT

Ready-to-send request to a provider

«Please test [application] for [risk] using [approach]. Scope: [features]. We can provide [test accounts, permissions guide or source code]. Please confirm missing materials and required testing rules.»

DO NOT

Do not send live passwords or customer data by regular email.

VEILTRACK

Independent security testing

PRINT · TEAM HANDOUT

Which Pentest to Choose and How to Prepare

Print it and hand it to the team. Keep it in sight for 30 days and tick each day you followed it. Once it is a habit, the sheet can come down.

Before ordering a pentest or changing its scope:

- [ ] Identify the risk and choose an approach.
- [ ] List the addresses and features to test.
- [ ] Prepare two customer accounts and other roles.
- [ ] Document who can view and change what.
- [ ] Agree on rules and share required materials.

30 DAYS TO A HABIT: TICK THE DAY

	Mon	Tue	Wed	Thu	Fri
WEEK 1	☐	☐	☐	☐	☐
WEEK 2	☐	☐	☐	☐	☐
WEEK 3	☐	☐	☐	☐	☐
WEEK 4	☐	☐	☐	☐	☐

Name, team: _____ Start: _____

Security questions? Write to us



Vlad Kraevsky

founder of Veiltrack

WEB

veiltrack.io

EMAIL

vlad@veiltrack.io

LINKEDIN

linkedin.com/company/veiltrack