

Pentest preparation checklist

Save this list and go through it before the kickoff meeting:

- ☐ Formulate the business question: which data, money or operations must be protected above all?
- ☐ Collect an exact list of domains, IPs, web applications, APIs, mobile components and cloud environments.
- ☐ Mark what you own and what is run by a hosting provider, a payment service or another vendor. Obtain the necessary permissions.
- ☐ Decide whether to test production or a separate environment. Define work windows and times when risky checks are prohibited.
- ☐ Prepare test accounts for different roles and safe test data. Do not hand over employees' regular passwords.
- ☐ Agree in writing the prohibited actions, load limits, stop procedure, escalation contacts and backup recovery.
- ☐ Inform the on-call engineers and the response team, but not necessarily every employee, if the scenario does not require it.
- ☐ Define the report format, a secure delivery channel, the retention period for materials and the terms for deleting them.
- ☐ Establish what "retest completed" means and when it ends.

Want to go through this checklist together? Write to us and we will review your scope.
veiltrack.io/en/contact