Cybersecurity Services FAQ: Penetration Testing, Compliance and Incident Response

Author: Kamakshaiah Musunuru | **Published:** 11 September 2026 | **Category:** FAQ | **Read time:** 2 min read

Tags: cyber fraud, incident response, penetration testing, security audit, data privacy, FAQ

Q1: What exactly is a penetration test?

A penetration test is an authorised, simulated attack on your application, infrastructure or APIs to find exploitable weaknesses before real attackers do. It typically covers web and mobile applications, cloud configuration, networks and social-engineering gaps, and it ends with a prioritised remediation roadmap.

Q2: How often should we get tested?

At minimum annually, and whenever you release significant new features or change infrastructure. For high-risk platforms, continuous or quarterly testing is advised, paired with automated scan tools in CI.

Q3: We think we have been a victim of cyber fraud — what do we do first?

Three things happen in parallel: contain (isolate affected systems and preserve evidence), investigate (identify how access was gained, with digital forensics if needed) and notify (your legal team, insurers and, where required, CERT-In or the regulator). Speed matters — data deleted by investigation is evidence lost.

Q4: What does a data-privacy compliance audit involve (DPDP/GDPR/ISO 27001)?

We map your data flows, review how consent and privacy policies work, check technical controls (encryption, access, logging) and identify gaps against the relevant regime. You receive a written gap analysis and a prioritised remediation plan — not a box-ticking exercise.

Q5: How is AI used in cybersecurity?

AI powers the defensive side too. In our security operations, AI helps correlate alerts, detect anomalies that look different from normal behaviour, prioritise incidents and triage findings from scans. No AI replaces a human security analyst — it removes noise and makes them faster.

Q6: How long does an engagement take?

A focused web application test typically runs 1-2 weeks including reporting. Compliance audits depend on scope, and incident response is measured in hours with a dedicated team. We match the engagement to your risk, not to a fixed menu.

Q7: Our team wants to build security in-house — can you help?

Yes. We offer secure architecture review, DevSecOps pipeline integration, code review (SAST/DAST), threat-modelling workshops and developer security training, so your team ships fewer vulnerabilities in the first place.