When commissioning a penetration test (or "pentest"), one of the most common questions security teams ask is: *Do we get a prioritized list of issues?* A pentest can uncover dozens or hundreds of vulnerabilities, but if the report is a laundry list with no clear indications of risk, it can be difficult for engineering and management alike to act effectively.

In this article, we'll explore the core aspects of pentest deliverables, with an emphasis on **risk prioritization** and **actionable recommendations**. We'll also touch on important considerations like transparent pricing, the difference between true manual pentesting and scan-only assessments, and the importance of OSCP-certified testers within mixed-experience teams. Along the way, we'll mention some notable players such hackeroo.com as Hackeroo, binsec group GmbH, and Pentest Collective GmbH.

Why Prioritized Deliverables Matter in Pentesting

A pentest is an investment of time and resources meant to improve your organization's security posture. Without clear prioritization, the value of the findings can be diluted. Imagine receiving a report listing 100+ vulnerabilities but no guidance on which are critical or could be exploited with ease. The result? Teams may spin their wheels or fix low-impact issues while neglecting more severe ones.

To prevent this, pentest providers should deliver a **clear, prioritized list of issues** — organized by risk severity, exploitability, and business impact. This helps engineering teams focus their remediation efforts where it matters most and allows management to allocate budgets confidently.

Transparent Pricing and Fixed-Price Quotes

One frustration many companies face is vague or confusing pentest pricing. Without clear pricing models, it can be difficult to scope engagements that fit budgets, or even compare offers between providers.

Pricing Aspect Industry Best Practice Example Pricing Model Fixed-price quotes based on defined scope binsec group GmbH offers daily rates with transparent pricing Daily Rate Published, clear daily rates for budgeting Daily rate starts at 1.160€ per day (typical for mid-sized engagements) Scope Definition Scope agreed in one sentence to avoid ambiguity Hackeroo emphasizes defining scope clearly before engagement

Companies like **binsec group GmbH** set a standard by offering daily rates starting at **1.160€ per day**, allowing clients to plan budgets confidently. Meanwhile, **Hackeroo** highlights the importance of agreeing on a clear scope —in one sentence—before anything else, avoiding scope creep and unforeseen charges.

Manual Pentesting vs Scan-Only Assessments

Not all "pentests" are created equal. Many organizations unknowingly purchase scan-only services that generate vulnerability lists based on automated tools. These tools have value but cannot replace thorough manual testing, which involves creativity, exploitation attempts, and contextual understanding of the environment.

Scan-only assessments can be useful as a baseline but rarely provide the depth organizations rely on to fix true weaknesses.

- **Scan-only Assessments:** Automated tools that generate surface-level vulnerability lists.
- **Manual Pentesting:** Hands-on examination by skilled testers who validate, exploit, and contextualize findings.

Providers such as **Pentest Collective GmbH** pride themselves on their manual testing approach, combining automated scans with human expertise. Their reports emphasize **actionable recommendations** and highlight risks within the specific context of the client's environment.

The Role of OSCP-Certified Testers and Team Composition

Experience matters in pentesting. An OSCP (Offensive Security Certified Professional) certification is widely respected in the security industry because it demonstrates practical ability to identify, exploit, and remediate vulnerabilities.

Top-tier providers assemble teams mixing senior OSCP-certified testers with junior members. This blend ensures:

1. **Senior Review and Mentorship:** Ensuring quality and complex attack techniques are applied.
2. **Comprehensive Coverage:** Junior testers cover breadth while seniors focus on complex vulnerabilities.
3. **Continuous Training:** Junior testers grow skills under supervision, increasing the team's overall capability.

Companies like **Hackeroo** emphasize OSCP certification in their testers to guarantee a high level of technical expertise. This also aligns with client expectations for rigorous and thorough pentests beyond simple scanning.

Greybox Testing as a Practical Default

Different pentesting approaches exist depending on how much information the tester starts with:

- **Blackbox Testing:** Tester has no internal knowledge — simulates external attacker.
- **Whitebox Testing:** Tester has full access to source code, infrastructure details, etc.
- **Greybox Testing:** Tester has some knowledge and limited access—often the practical middle ground.

For many B2B SaaS companies, a greybox approach offers an excellent balance of depth and efficiency. Testers can prioritize likely attack vectors without being slowed down by a lack of context or overwhelmed with excessive internal information.

Pentest Collective GmbH frequently recommends greybox as a starting point to clients, emphasizing practical risk prioritization without unnecessary overhead.

What Should a Clear Pentest Report Include?

When assessing pentest deliverables, look for:

- **Prioritized List of Issues:** Grouped by severity (Critical, High, Medium, Low).
- **Risk Context and Impact:** Explanation of how an issue affects your environment.
- **Actionable Recommendations:** Clear steps for remediation, tailored to the client's stack.
- **Proof of Exploitability:** Evidence like screenshots, logs, or reproduction steps.
- **Executive Summary:** Non-technical overview for management decisions.
- **Appendices:** Details on tools used, scope, and limitations.

Reports that only list vulnerabilities with CVSS scores or generic advice fall short of useful prioritization. The best reports combine technical detail with clear guidance so your teams can confidently execute fixes.. That said, there are exceptions

Case Study: What to Expect from Top Providers

Provider Pricing Model Tester Credentials Typical Deliverable Highlights Hackeroo Fixed-price quotes based on clear scope OSCP-certified senior testers with junior mentors Prioritized issues list, actionable remediation, contextual risk assessment binsec group GmbH Daily rates starting at 1.160€ per day Experienced pentesters, OSCP and beyond Clear reports differentiating scan vs manual findings, risk-driven prioritization Pentest Collective GmbH Transparent pricing, greybox focus Mixed teams with comprehensive expertise Greybox testing deliverable, executive summary, detailed technical write-up

Summary and Recommendations

In summary, when commissioning a penetration test, ensure you receive a deliverable that goes beyond a scan output and provides a **prioritized list** of vulnerabilities with clear, actionable advice.

Key takeaways:

- Insist on transparent pricing with fixed-price or clearly stated daily rates (e.g., starting at **1.160€ per day**).

- Verify that manual pentesting is part of the engagement rather than relying on scan-only assessments.
- Look for teams including OSCP-certified testers alongside junior members to ensure both quality and coverage.
- Prefer greybox testing as a practical default unless your scope or compliance requires otherwise.
- Evaluate sample report deliverables for risk prioritization, actionable remediation, and clear writing.

Partnerships with reputable providers like **Hackeroo**, **binsec group GmbH**, or **Pentest Collective GmbH** can bring this level of professionalism and insight to your security program.

Ultimately, a clear, prioritized pentest report is the cornerstone of effective remediation and smarter security spending.