SecureLayer7

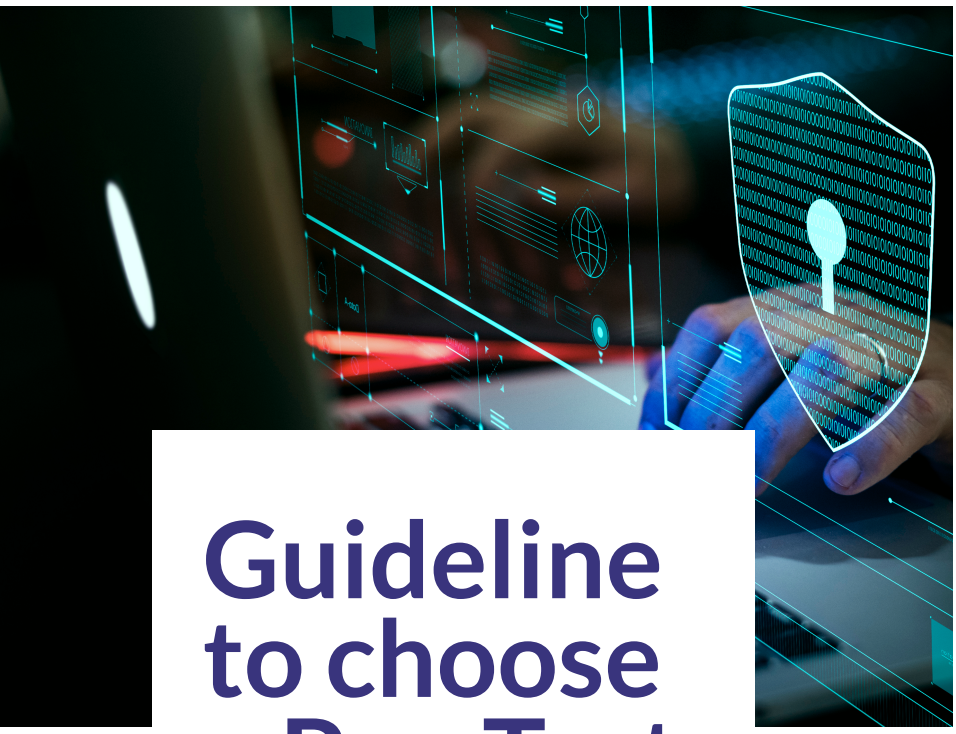
Time and Again, Securing you

Guideline to choose a Pen Test service partner

Published 11 September 2021 - 15 min read

Niranjana Dhumal

Security Research Analysts



Guideline to choose a Pen Test service partner

Digital transformation is driving enterprises to seize new emerging opportunities. According to Gartner, 91% of organizations are engaged in various digital transformation initiatives. However, this transformation brings to light one critical consideration for business leaders: Does the digital transformation strategy have a cybersecurity component?

Anecdotal experience tells us that digital transformation initiatives have led to an increase in the attack surfaces, and enterprises are being exposed to potential breaches. Add to this regulatory requirement that governs enterprises today.

Given the spate of attacks today, security leaders rely on penetration testing more than ever before to identify vulnerabilities so that the cyber control mechanisms are monitored. Pen testing, therefore, becomes a critical function, and choosing a competent partner is as important!

Digital transformation is driving enterprises to seize new emerging opportunities.

Does the digital transformation strategy have a cybersecurity component?

Second Order Thinking: Construct a Decision Metric to drive partner selection

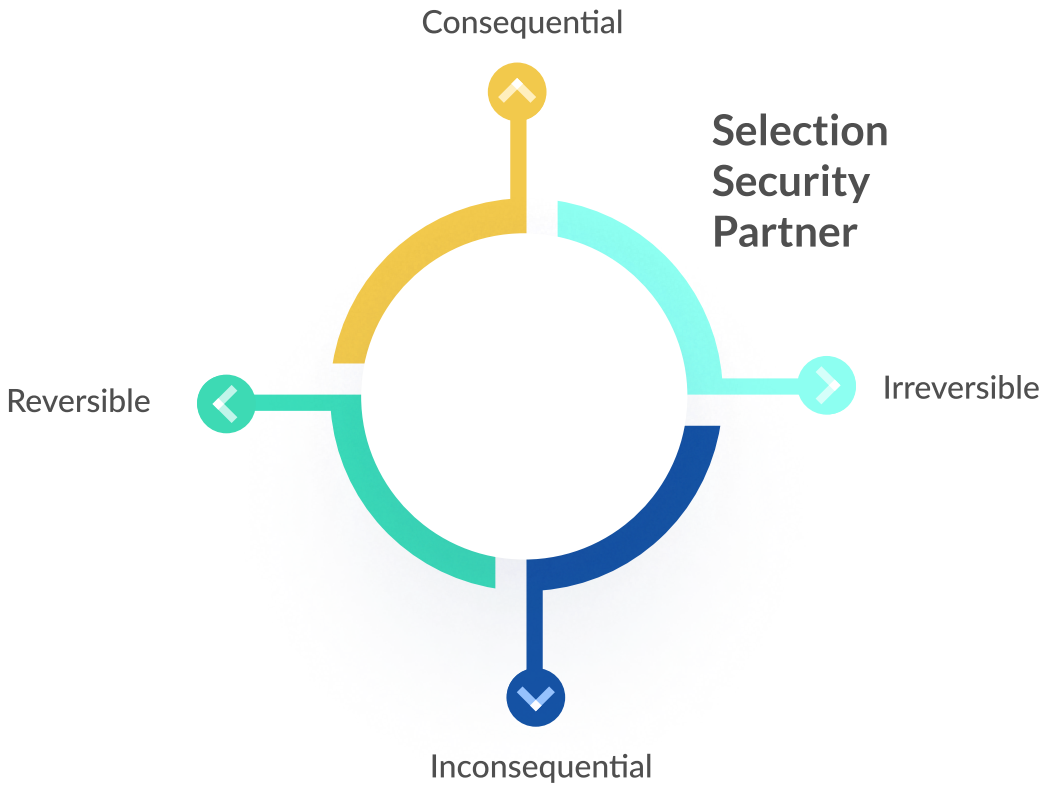


figure 1.0.

A security risk manager needs to obtain second-order thinking and use decision metrics to select Pen Test partners. The Pen Test partner selection process falls into the consequential and irreversible decision quadrant as shown in the below figure 1.0.

Consequential and irreversible decisions can often change the trajectory of your security goals and plan. Being able to identify them and break them down into smaller and more manageable decisions is the first step to select a Pen Test Partner.

Key traps to avoid

Tendency to outline the choices too narrowly in binary terms instead of thinking of the decision as a principle.

Avoid pretending we want the truth, however we are often looking for reassurance of our beliefs.

8 Critical factors to consider while selecting a Pen Test partner

1. How much budget is enough for a good pentest, how to balance cost and quality? Does money matter? Where to draw the line?
2. How about achieving various levels of compliance, such as SOC2 Type II, GDPR, or ISO? Does your pentest partner assist you on that journey?
3. How about your company's policies regarding fixes for vulnerabilities, can you handle the effort and have sufficient capacity? Does your pentest partner help with live-reporting and similar services?
4. Are you reaching out to your peer's suppliers for understanding who helped you to secure assets?
5. Do you know how Pen Test Partner is going to manage the entire Pen Test lifecycle?
6. Do you know how Pen Test Partner estimates the cost for one-time or yearly engagement?
7. Do you know how Partner vet Pentesters for allocating on the Pen Test activity
8. Do you know how much duration of Pen test activity data is stored and how secured it is?

Drive collaboration and co-opt stakeholders in the pen testpartner selection decision

To make a good decision for an organization, as a security risk manager you might need to involve the relevant stakeholders who should weigh in on this decision. You need to communicate differently with each type of stakeholder. Refer the 2x2 framework below to help you find the right set of stakeholders and ensure you have communicated the right decision as per their requirements.

High

Interest

Low

Involve

Inform Regularly

- Security Analyst
- Internal Security Team
- External Peers
- External Research Experts e.g. Gartner Forrester, and mckinsey

Collaborate

Involve in Decision Making

- Chief Technology officer
- Chief Information Security officer
- Sr. Security Infrastructure
- Application Architect
- Sr. Principal Security Architect
- Product Manager
- Manager - IT Security

Inform

Inform Periodically

- Developer Team
- Product Owners
- Program Manager
- IT/Infrastructure Staff

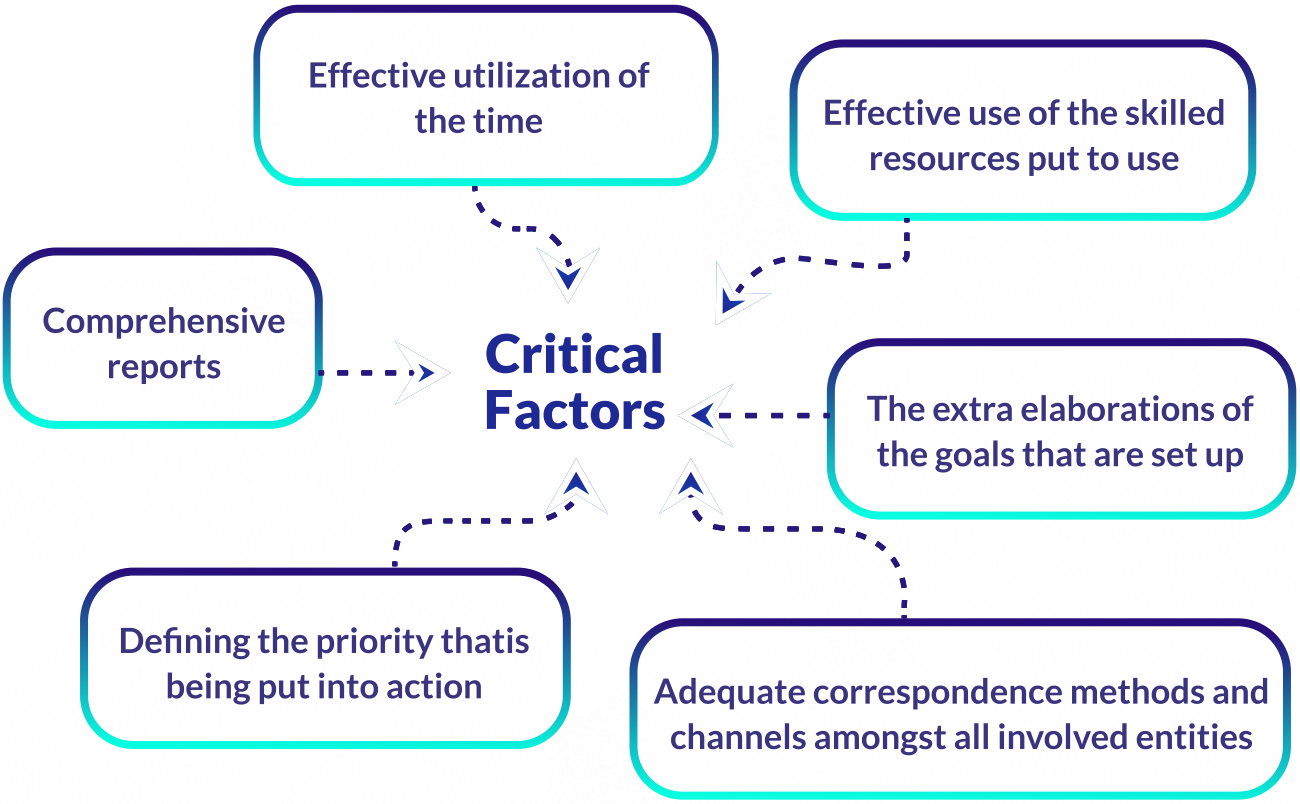
Consult

Inform Regularly

- Procurement Manager
- Chief Finance Officer
- Legal Team
- Chief Executive Officer
- Governance and Risk Managers

Low ---------- Power/Influence ----------→ High

Critical Factors for a successful Pentest



Conclusion

The information and framework presented above will help you decide on a pen test partner. The next time you are about to make a key decision, take a moment to think about the following:

- Does my decision frame have a Yes/No (binary) option?
- Have I lived with the decision for some time?
- Am I jumping on to the first information that has come my way?
- Am I deciding based on just what I believe in or have I validated it with evidence that supports the belief?

SecureLayer7

Time and Again, Securing you

Thank you for reading the research report

If you have any questions, feedback or comments please get in touch via the website.

Contact us

www.securelayer7.net

info@securelayer7.net