Using the Quantimatter for pentesting

The value of Quantimatter automated pentesting vs manual pentesting is reflected in the following features of our platform*:*

1. shortcuts/accelerates time from initiating an assessment to presenting insights/findings on level of exposure to cyber threats. The speed increase is 3-4 orders of magnitude faster than traditional (human expert-based) cybersecurity testing (from weeks to minutes).
2. access to expertise is simplified through a self-service platform that allows users to initiate a cybersecurity assessment at different levels of depth with minimal instructions or know-how.
3. affordability is increased and therefore ability to conduct repeat assessment periodically (weekly, monthly etc.) and ensure new threats are detected sooner and overall cybersecurity resilience is maintained consistently.

The table below provides a side-by-side comparison of scoping/exposed vulnerabilities.

Quantimatter platform	Manual pen testing
Main objective is to: Identify security vulnerabilities, prioritize remediation and reduce risk. Exploit security weaknesses in a non-intrusive way to flag the vulnerabilities before unauthorized users can exploit them.	Same as Quantimatter but could also include: ● Intrusive exploit of weaknesses ● Some level of white-box testing
Focused on assessing the overall security of the target systems and supporting architecture to determine if vulnerabilities are present and performing steps to exploit the vulnerabilities to correlate the overall exposure of the resources. The testing is performed using a static IP with no privilege to systems or networks.	Same as Quantimatter but if includes white-box testing will likely require privileged access to back-end architecture. Testing could also replicate more sophisticated scenarios like usage of dynamic IPs, simulation of DDoS attacks etc.
Standards followed or leveraged: ● Open Web Application Security Project (OWASP) Top 10 ● MITRE Common Vulnerabilities and Exploits (CVE)	Sames as Quantimatter but could also include: ● Certified Ethical Hacker (CEH) standards ● Payment Card Industry (PCI), ISO and other industry-specific standards
Steps in the assessment process: ● High-level web scan (known vulnerabilities, simple exploits, poor hygiene) using web scanning tools API's.	Most manual assessments follow a similar set of steps with scans, discovery and active exploits. Custom test and specialized engagements can also cover internal infrastructure exposures (provided

● Footprint Analysis and Information Gathering, Network Enumeration - Using proprietary and public tools the platform discovers the underlying infrastructure of the online targets and specific external-facing network components. Also by scanning open ports on each system connected to the network, the platform attempts to extract as much information as possible from the target system(s) ● Active pen tests and exploits: the platform uses the information from the previous step to attempt various exploits referenced in the CVE database as well as from the OWASP Top 10. ● Reporting – Once the test completes the online dashboards and charts are updated and a comprehensive report with deep analysis and recommendations on how to mitigate the discovered vulnerabilities is available immediately for download.	privileged access is obtained) and verifying that network and infrastructure meet baseline security standards defined by the industry.
Examples of exploits flagged and threats to online infrastructures that a customer needs to fix include: Data Leakage, Security Policy/Options, SQL Injection, click/formjacking, brute force credentials attacks, PII exposure, content policies exploits, path traversal, XSS, file inclusion, open ports, outdated libraries exploit, SSH exploits, Buffer Overflows, CGI attacks, PHP Attacks, HTTP Headers Server Side Code Injection, XXE exploits	Same as Quantimatter but if required can include custom/specialized testing for: DDoS attacks, malware/Trojans, Viruses, Phishing, misconfigured network devices etc.

Comparison of pricing

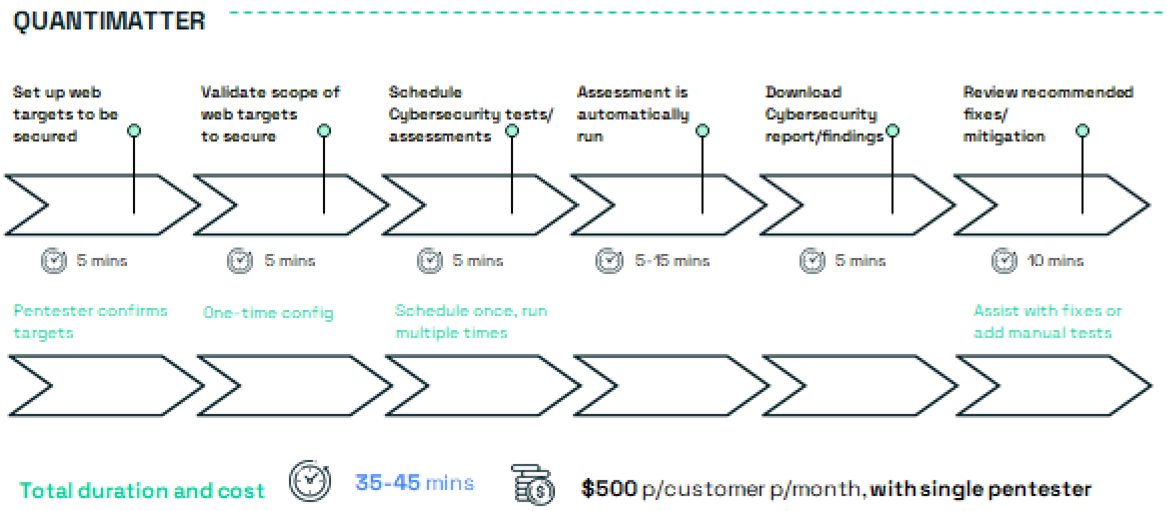
Quantimatter platform	Manual pen testing
$99 p/month per asset (unique IP, VPC, ULR). Assuming 3-4 assets per customer, unlimited assessments: **TOTAL 1 year spend: ~$4k-5k**	One-time manual assessment: $15k-30k[1] Web scans or one-off crowdsourced tests: $700-$1k[2] Assuming 6 assessments p/year (3 assets): **TOTAL 1 year spend : ~$18k-$180k**

[1] https://www.securitymetrics.com/blog/how-much-does-pentest-cost

[2] https://onlinehackscan.com/step1

If you or your business leverages human pentesters to help businesses secure their online infrastructure, then Quantimatter can help you compensate for the shortage of skilled experts by automating 80-90% of their work. Using the Quantimatter platform you could serve 10-20 customers simultaneously leveraging a single human expert, who could complement our pentesting platform for more in-depth assessments like white-box testing.

The summary below is an example of how pentesters could operate with the Quantimatter on-demand cybertesting platform:


QUANTIMATTER
Set up web targets to be secured
Validate scope of web targets to secure
Schedule Cybersecurity tests/ assessments
Assessment is automatically run
Download Cybersecurity report/findings
Review recommended fixes/ mitigation
5 mins
5 mins
5 mins
5-15 mins
5 mins
10 mins
Pentester confirms targets
One-time config
Schedule once, run multiple times
Assist with fixes or add manual tests
Total duration and cost
35-45 mins
$500 p/customer p/month, with single pentester

For a Cybersecurity business employing a handful of pentesters and serving dozens of customers each month, revenues from the Quantimatter platform could easily exceed $100k per month with 50% margins due to the extensive automation that can be leveraged.

If you are interested in finding out more about partnering with Quantimatter contact us on our website or email our partner desk at **partnership@quantimatter.com**.