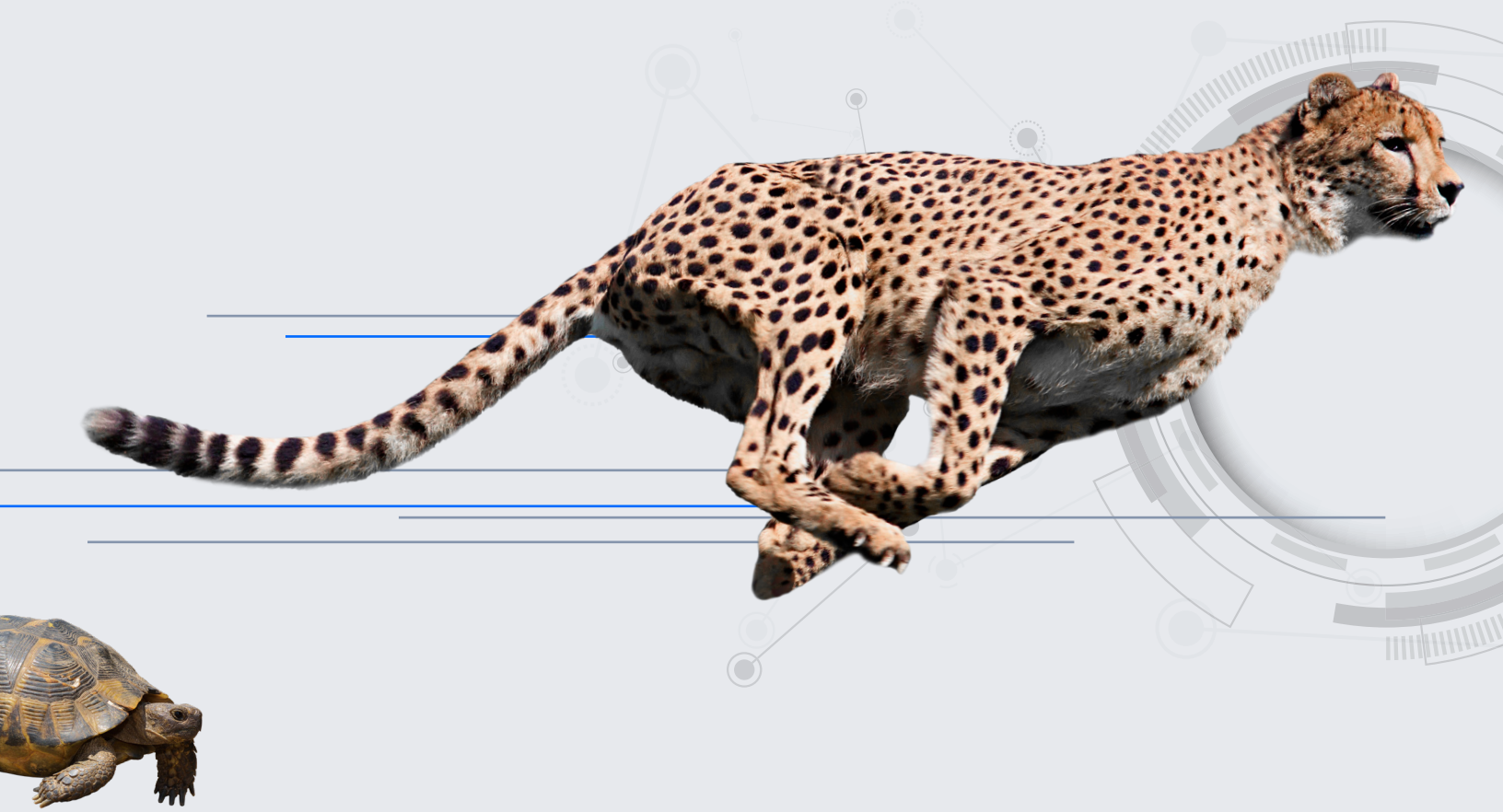
Synack

WHITE PAPER

TRADITIONAL PENTESTING:

A TURTLE CHASING A CHEETAH

By Kim Crawley



Pentesting Needs to Evolve

Simply doing more pentests in the traditional manner is not viable. While missing all kinds of critical vulnerabilities, traditional pentests can even make the ones that are found and reported difficult to keep up with. It's frustrating to think of all the money, labor and resources that are being spent by security teams and their contractors only for those efforts to fall short in response to today's and tomorrow's cyber threats.

In the words of Roman Medina, CISO at Jefferson Bank in Texas, "I do think we may miss critical issues or vulnerabilities if we stick to the same annual pentest year after year. The way we pentest has to evolve. I am looking at starting a continuous pentest service next year."

It's not possible to staff a large enough team to perform traditional pentests in a more continuous manner. It's time to reimagine how pentests are staffed and performed. Organizations need scalable third-party solutions that harness technology combined with manual, human testing in order to provide more flexibility, continuity and intelligence than a traditional pentest.

> *I do think we may miss critical issues or vulnerabilities if we stick to the same annual pentest year after year. The way we pentest has to evolve. I am looking at starting a continuous pentest service next year."*
>
> ROMAN MEDINA - CISO, JEFFERSON BANK

Pentesting Deficiencies Analysis

As a security leader, you know why legacy tech is insecure, impractical and insufficient. In that spirit, we must also reconsider legacy pentesting practices. Using antiquated pentesting methodology in today's cyber-threat landscape is like sending a tortoise to catch a cheetah. It's a big hurdle to overcome, but we must face these challenges with tenacity and ingenuity.

Security teams have an incredibly important role in protecting their organizations. We hope that this white paper provides an understanding of objections to traditional pentesting. You deserve to find vulnerabilities that matter — not create more work and risk for your security team.

Here's a point-by-point analysis of why and how old-school pentesting is no longer up to the challenges we face today:

- **Too slow and static for the cloud era.** A traditional, annual pentest misses critical cloud risks and assets. It's point-in-time, has a vast landscape to cover, and doesn't adequately convey the state of the environment. A zero day vulnerability or misconfiguration can occur at any time regardless of defenses in place (e.g., Apache Log4j). Adversaries can and will exploit ephemeral cloud assets exposed on the Internet (e.g., containers, storage buckets, etc.).

- **Deployment lacks flexibility and scalability.** Traditional pentesting cannot scale in organizations with tens of thousands of assets. Organizations are frustrated with extended wait times for testing, the lack of effective coverage, and the inability to have insight into what was actually tested. The cumulative outcome of these gaps is the inability to have assurance and trust in your own capabilities.

- **Mere compliance means security on paper, not in the wild.** Regulatory compliance is a vital baseline for any security program, but it's not sufficient in measuring performance overtime or in communicating environmental hardness. When exploitable vulnerabilities are disclosed, malicious hackers immediately begin their enumeration process to identify targets. Attackers don't care about rules of engagement, and they certainly won't wait for you to patch.

- **Disrupts security and development workflows.** A traditional pentest creates anxiety and unnecessary work for security teams. Results are not actionable. Most vendors won't re-test, measure security improvements, or provide real-time analytics. Poor pentesting skills can also lead to disruption through accidentally taking network segments offline — leading to expensive downtime.

- **Lacks the creativity and resources of adversaries.** Organizations are living in the ransomware-as-a-service (RaaS) era. Attackers have a wide range of tactics, techniques and procedures (TTPs) that pentests need to replicate. Two consultants armed with a checklist can't and won't prepare you for what's coming.

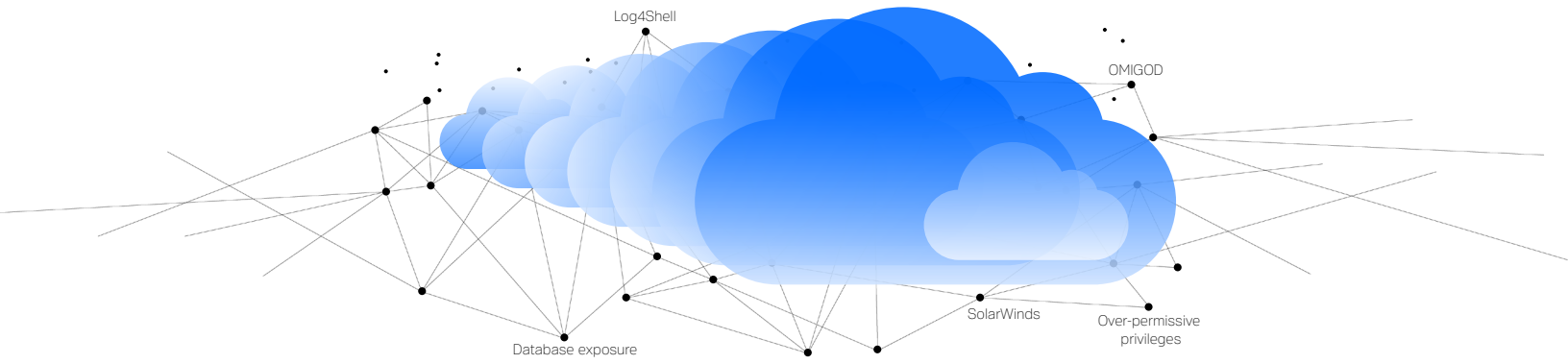
The Inconvenient Truth of Traditional Pentesting

Annual pentesting has been a compliance standard for a long time. Organizations frequently seek out pentesting as part of compliance with NIST, PCI-DSS, and GDPR. However, security teams need to rethink the way they pentest today to make sure they are not missing critical security vulnerabilities.

Traditional pentesting is too slow and static for the cloud era

The cloud has revolutionized how business is done these days. Cloud assets are elastic, dynamic and growing faster than ever:

- Containers and virtual machines can have life spans of mere days. Cloud resources can double and halve in size in the blink of an eye.
- Traditional pentesting is designed for a pre-cloud world where networks are entirely on premises and change much more gradually.
- Case in point: According to research from Palo Alto Networks, large organizations add 1,300 new publicly accessible cloud services per a year on average.[1]



1. Cortex Xpanse Research

Old fashioned pentesting deployments fail at flexibility and scalability

Deployments may take weeks or months to schedule, which significantly delays the testing process:

- When a new exploitable vulnerability appears on Twitter or Reddit, organizations often don't have the flexibility to check for that specific CVE on demand.
- A recent research report examining software vulnerabilities on social media found that on average they are discussed on Twitter, Github, and Reddit for 87 days before being added to the National Vulnerability Database (NVD).[1]
- It's impossible to scale manual testing deployments from one to tens of thousands of assets.
- A related problem is that pentests require the work of specialists with different skill sets, and it's difficult to schedule them if you plan engagements the traditional way.

Mere compliance should not be a security baseline

Regulatory compliance is an important component of a security program, but **compliance checklists fall short:**

- If you're pentesting periodically according to compliance rather than pentesting continuously, it's difficult to measure security hardening and security maturity over time.
- Finding and addressing exploitable vulnerabilities months after they emerge is fine for compliance because audits don't happen every month.
- The inconvenient truth is that cyber threat actors are testing you every day, much faster than the bureaucratic pace of HIPAA, Sarbanes-Oxley or the GDPR.
- When zero day vulnerabilities are released, malicious hackers can immediately begin their enumeration process to identify targets (e.g., Microsoft Exchange).
- If your organization's sensitive data is breached in the months it took to find a vulnerability, it may still lead to unwanted headlines, compliance violations or damage to the brand.
- Point-in-time reporting fails to provide timely assessments of new and exploitable vulnerabilities.

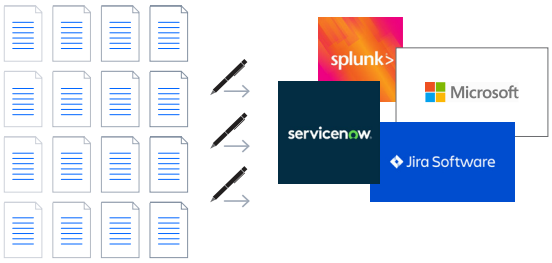
The inconvenient truth is that cyber threat actors are testing you every day, much faster than the bureaucratic pace of HIPAA, Sarbanes-Oxley or the GDPR.

1. Shresthra et al. "Multiple social platforms reveal actionable signals for software vulnerability awareness: A study of GitHub, Twitter and Reddit." March 24, 2022.

Traditional pentesting disrupts security and development workflows

One reason why organizations don't pentest anywhere near as frequently as they should is that traditional pentesting is disruptive:

- Many scanners used in pentests surface noisy results, distracting from critical vulnerabilities which should be addressed first.
- Vendors send pentest reports in formats that are not actionable (e.g., PDFs and Excel sheets).
- Assuming reports are not lost, a security team member needs to copy and paste information into ticketing tools like Jira or ServiceNow.
- A pentest can cause an entire network segment or company department to go offline.
- Sometimes pentests need to be repeated to gather more information. But when pentesting is disruptive, repeating an exploit can be messy and aggravating.
- Faster remediation is more important than ever as hackers will prioritize externally facing vulnerabilities like misconfigured S3 buckets or supply chain vulnerabilities.



Traditional pentesting fails to match the creativity and resources of adversaries

Simply put, traditional pentesting is ineffective in every applicable way:

- It can be difficult to find top pentesting talent, especially those with specific specializations.
- Inevitably, the knowledge and skills of a few pentesters are limited compared to that of a couple hundred or even a thousand pentesters.
- Collective intelligence is a measurable phenomenon, one that can be more inventive and effective in discovering vulnerabilities and exploits.
- Traditional pentesting engagements are limited in scope by design, partly to avoid disruption and partly due to limited time and resources. Significant areas of your network will be missed.
- The reality is that networks are getting "pentested" frequently every day by threat actors, but your organization doesn't benefit from seeing the results.
- Today's cloud and hybrid networks are elastic and dynamic, as are the cyber threats organizations of all kinds now face. You can't counter a dynamic threat with a static tool like traditional pentesting.