HADRIAN

A Modern Guide to Pentesting

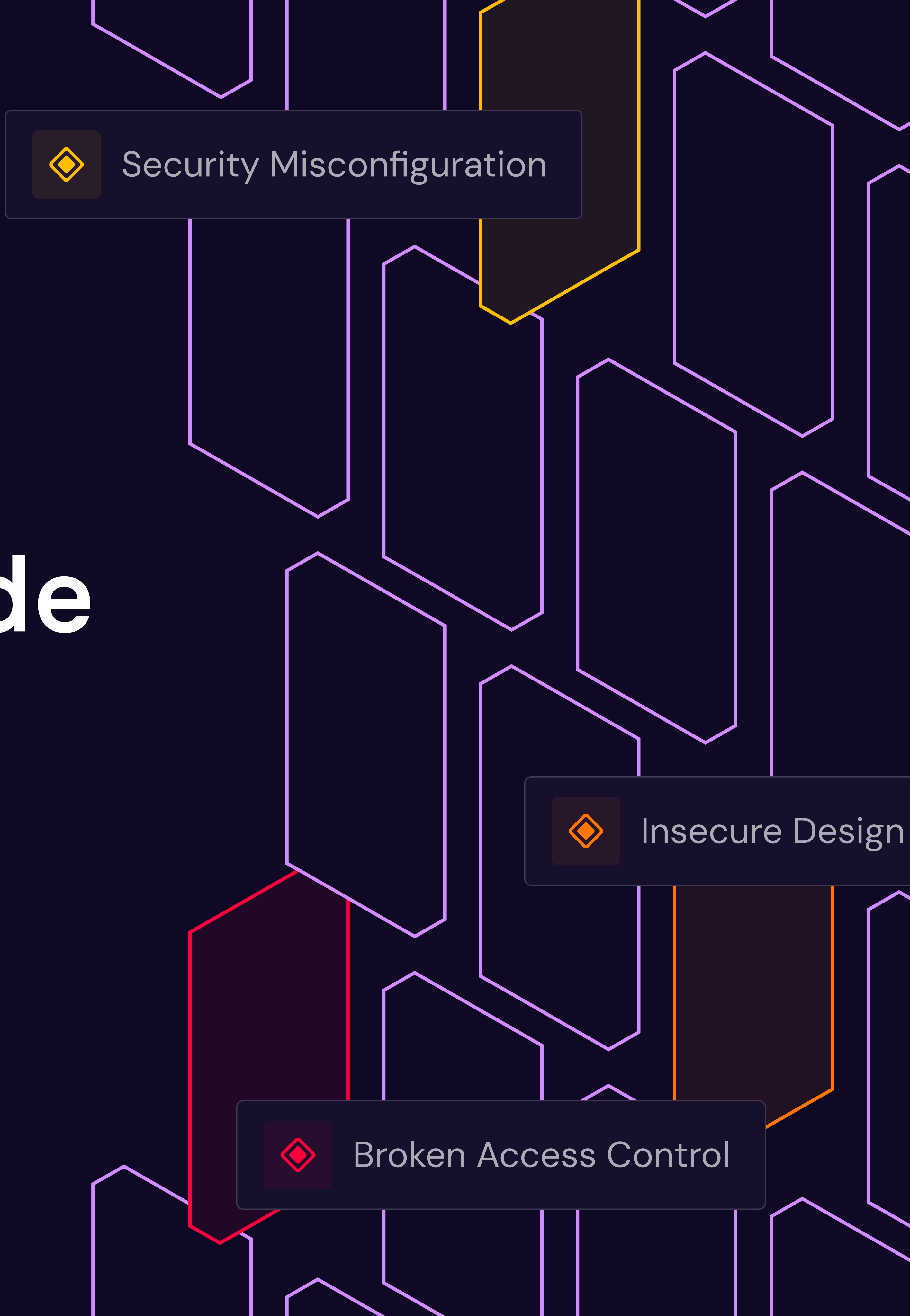


Table of contents

Strategic questions

Penetration testing is a common practice across many organizations. There is a vast array of use cases for testing and all share the common goal of minimizing exposure to threats. Over time these use cases have matured, necessitating the need for modernized approach to penetration testing.

In this guide we describe a penetration testing methodology that supports the business and technology needs of modern organizations.

Despite their advantages, pentesting comes with a number of questions:

How frequently testing should be conducted?

What assets should be included in the scope?

Are there methods to shorten testing timelines?

Can operational continuity be maintained?

Is there an ideal process for managing remediation?

Key use cases

Indepth

Covers exposures across all risk categories for a given asset. The assessment is often for specific purpose which requires a report as its final output. Common frameworks include SOC 2, ISO 27001, PCI-DSS, CREST, and HIPAA.

- Compliance
- M&A Due Diligence
- Incident response preparedness
- Customer Request

Agile

Targets specific exposures across a number of assets. The assessments typically lightweight and conducted frequently. The output of the assessment is usually automatically generated and for internal purposes.

- New release testing
- Regression testing
- Zero-day response
- OWASP assessment

Discovery

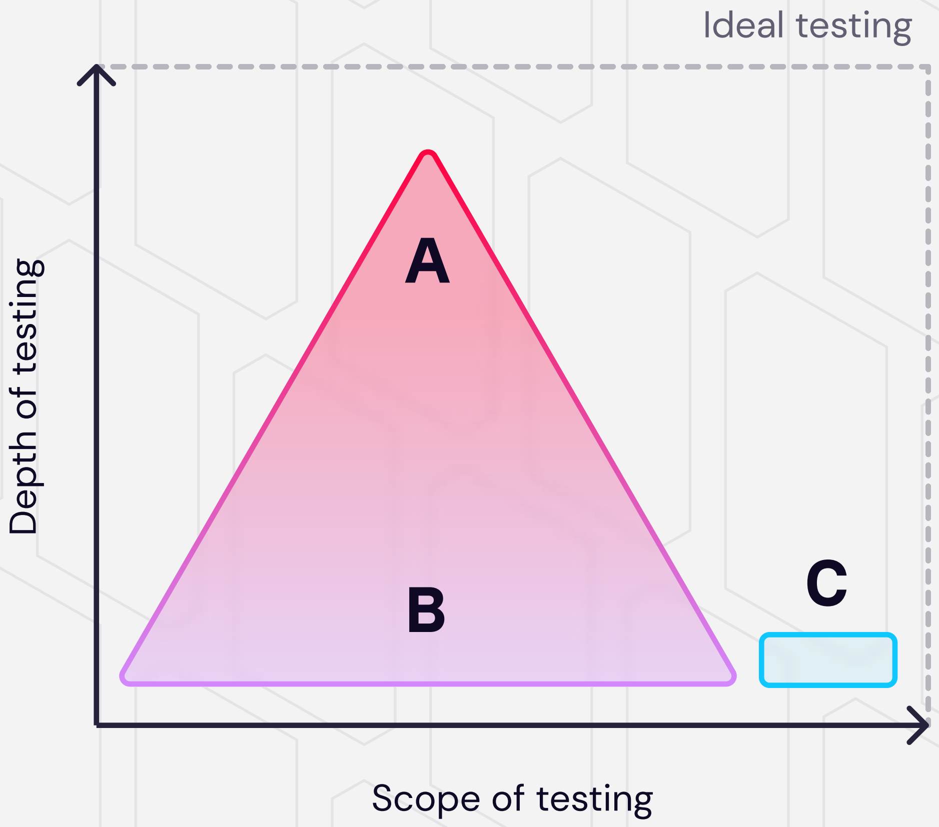
Seeks to identify and catelogue the assets that organizations have little or no visibility of. The assessments are conducted across the internet to identify the missing assets.

- 3rd party risks
- Shadow IT
- Cloud infrastructure
- IoT and OT assets

Defining testing objectives

Security assessments can be categorized along two dimensions: depth and scope*. The approach taken is typically based on the organization's evaluation of its assets. In the ideal world, there would be complete coverage, and all assets would be tested in-depth, but this is not practical.

	Challenge	Statistics	Goal
A	Indepth	Critical	Identifying all of the exposures
B	Agile	Majority	Scanning for common issues
C	Discovery	Unknown	Expanding the attack surface



Practical Limitations

Intuitively, the strategy used by many organizations has been to align the toolkit available to them with their penetration testing needs. As a result, the effectiveness of the assessments is restricted by the toolkit utilized. To date, strategies have been manageable for many organizations today because they have historically had relatively small environments.

However, external and internal forces on security teams reveal the flaws in this strategy.

Indepth

Traditional penetration services that rely on human expertise

Challenges

- ✓ High cost per asset
- ✓ Limited asset scope
- ✓ Long gaps between assessments

Agile

Scanners that are run on known infrastructure or codebases

Challenges

- ✓ Large number of false positives
- ✓ Subset of exploits are tested
- ✓ Limited reporting capabilities

Discovery

Open-source or in-house developed scripts that are run by security teams

Challenges

- ✓ Asset context not understood
- ✓ Risk testing is not conducted
- ✓ Results are not actionable

Shifting Forces

Meeting compliance requirements is no longer enough to maintain a strong security posture. For many organizations, the attack surface, which can be targeted by threat actors, grows and changes on a daily basis. Moreover, the development of new techniques and the automation of exploits by threat actors is on the rise.

The result is that penetration testing strategies are unable to scale to meet modern security needs.

69%

of organizations have experienced an attack targeting poorly managed external-facing assets.1

69%

of all cyberattacks exploit vulnerabilities that have had a patch available for over a year. 2

86%

of codebases contain at least one vulnerability, with 48% containing a high-risk vulnerability.3

52%

of organizations are considering changing to new assessment solutions to reduce false positive alerts.4

66%

of security teams find it difficult to protect complex and dynamically changing attack surfaces.5

A Modern Strategy

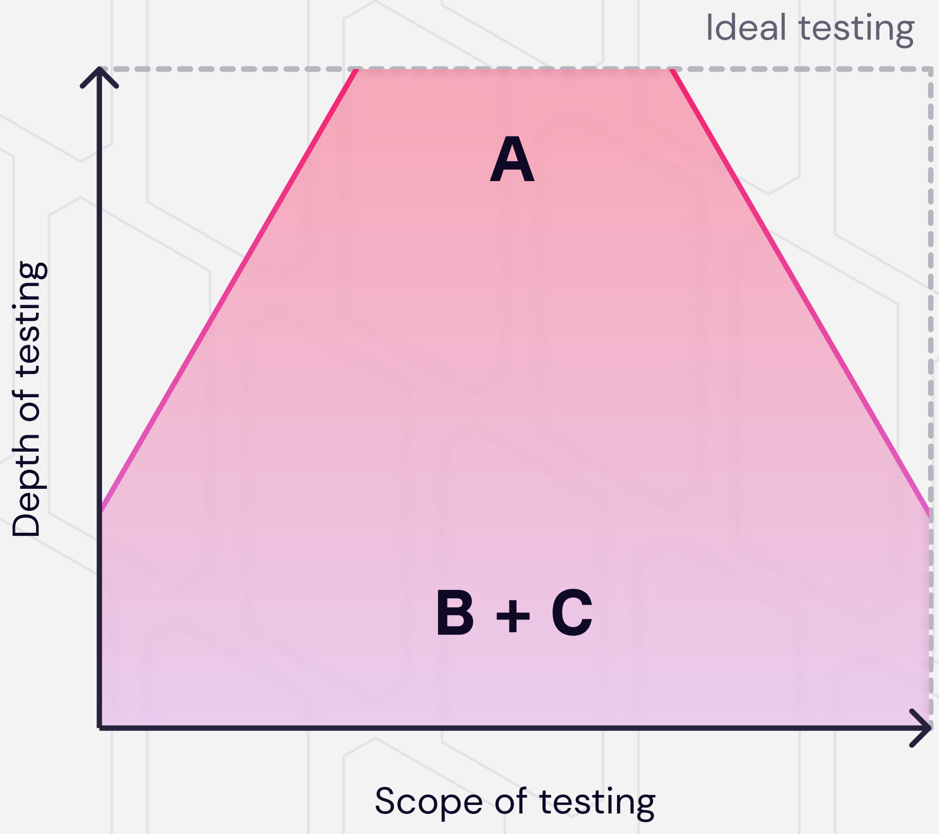
By adapting the methodology and tools used, greater coverage can be achieved and more complete visibility is made possible. In order to gain this, organizations should consider making changes to their security testing strategy:

Discovery and Agile testing should be conducted in parallel. When new assets are discovered automated testing should be triggered. This will reduce the risk that unknown unknowns pose to the security posture.

Agile assessments should incorporate Active Testing. By testing for a greater range of exposures more in-depth assessments can be conducted autonomously. Active Testing can also validate that risks are exploitable, eliminating false positives

In-depth penetration testing should build on Agile. Using Agile testing as a force multiplier, human-powered penetration testing can focus on testing exploits that can't be automated. In-depth testing can then be conducted on a greater number of assets or kept as cost savings.

	Challenge	Statistics	Goal
A	Indepth	Critical	Identifying all of the exposures
B	Agile	Majority	Scanning for common issues
C	Discovery	Unknown	Expanding the attack surface



HADRIAN

Capabilities to Consider

To execute a modern penetration testing strategy the following capabilities could be considered:

□ **Automatable testing**
AI-driven Active Testing allows for a greater range of exploits to be automated.

□ **Continuous discovery**
To find new assets (or changing ones) continuous passive scanning should be performed.

□ **Event-based architecture**
An event-based architecture can be used to trigger security testing when needed.

□ **Result validation**
False positives can be removed from penetration test results by requiring verification of exploitation.

□ **Risk-based prioritization**
In-depth testing can be focused on the most important risks by prioritizing the results of Agile testing with threat intelligence.

□ **Zero-day exploit detection**
The latest exploits can be detected by selecting Agile testing partners with platform update SLAs.

□ **Context awareness**
To prevent unnecessary automated scans, context-aware testing platforms will only test for relevant exploits.

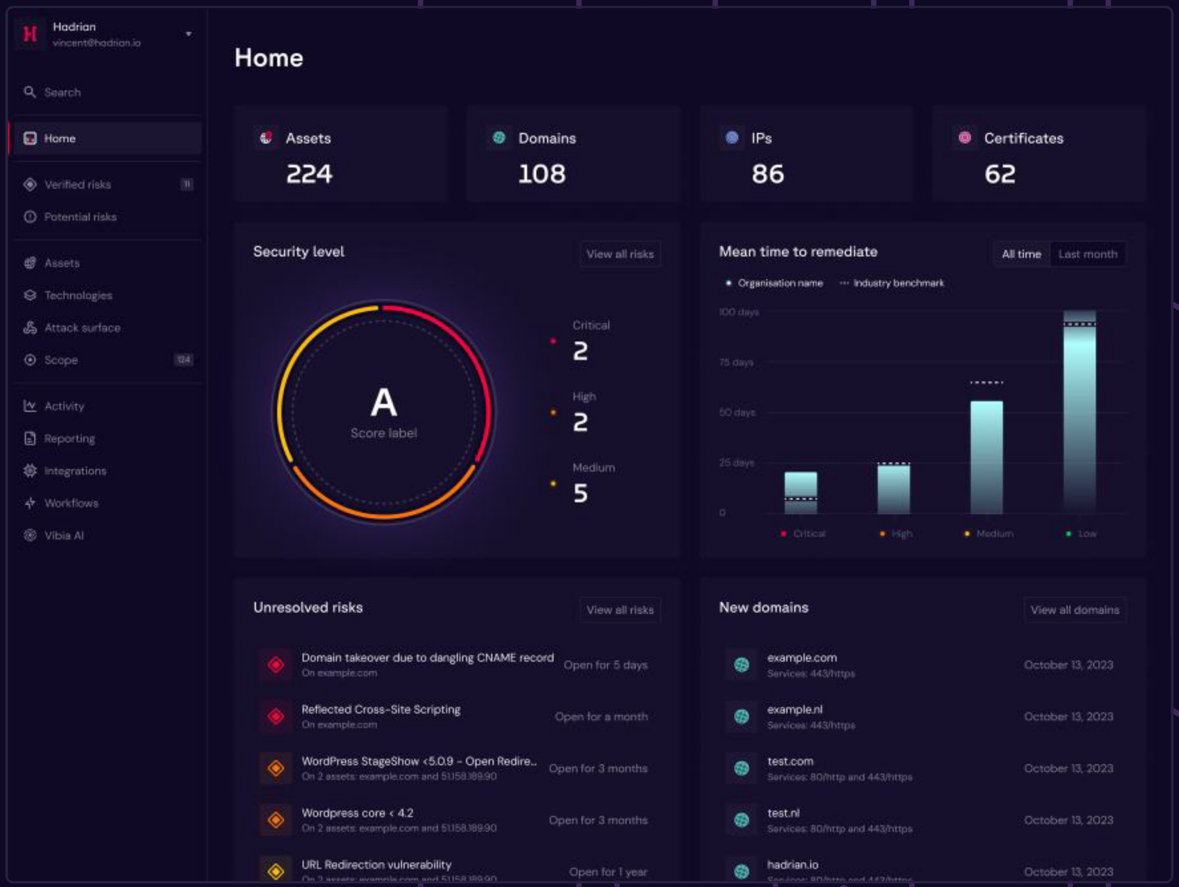
□ **Step-by-step remediation**
Researching how to resolve a risk can take precious time, detailed instructions help teams take action quickly.

About Hadrian

Hadrian provides the hacker perspective, revealing the targets and methods that could be used in a real-world data breach. Hadrian's continuous and comprehensive testing discovers and validates risks completely autonomously.

Hadrian's platform combines attack surface discovery, automated penetration testing, and threat exposure management technologies in a cloud-based and agentless platform. The cutting-edge technology is constantly updated and improved by Hadrian's in-house hacker team.

Book a demo



Domain takeover due to dangling CNAME record
On example.com
Open for 5 days

Reflected Cross-Site Scripting
On example.com
Open for a month

WordPress StageShow <5.0.9 - Open Redire...
On 2 assets: example.com and 51.158.189.90
Open for 3 months

Wordpress core < 4.2
On 2 assets: example.com and 51.158.189.90
Open for 3 months

URL Redirection vulnerability
On 2 assets: example.com and 51.158.189.90
Open for 1 year

example.com
Services: 443/https
October 13, 2023

example.nl
Services: 443/https
October 13, 2023

test.com
Services: 80/http and 443/https
October 13, 2023

test.nl
Services: 80/http and 443/https
October 13, 2023

hadrian.io
Services: 80/http and 443/https
October 13, 2023

Trusted by market leaders

ABN·AMRO

SHV ENERGY

macmillan education

CTC GLOBAL

WeatherTech

LEROY MERLIN

LOTTOMatica

RITUALS...

BIOLANDES

nedap

Van Oord

Sources

1 – ESG, Security Hygiene and Posture Management (2022)

2 – Abdalslam, Patch Management Statistics, Trends And Facts (2023)

3 – Synopsys, Open Source Security and Risk Analysis Report (2023)

4 – Netwrix, Vulnerability Assessment Analytical Note (2022)

5 – Ponemon, The Cybersecurity Illusion: The Emperor Has No Clothes (2019)