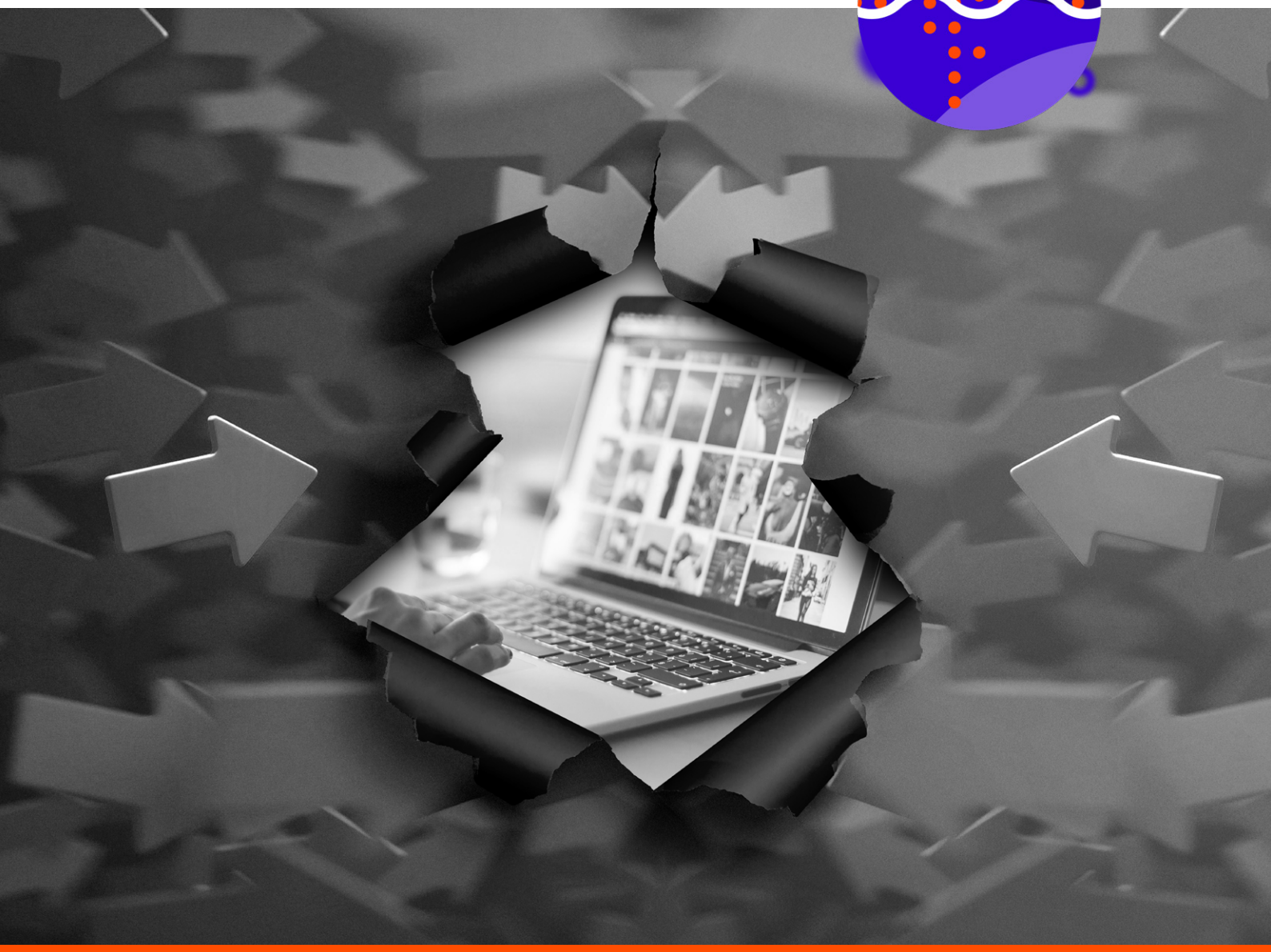
PEN TESTING

IDENTIFY WEAK LINKS IN YOUR SECURITY IT SYSTEMS.



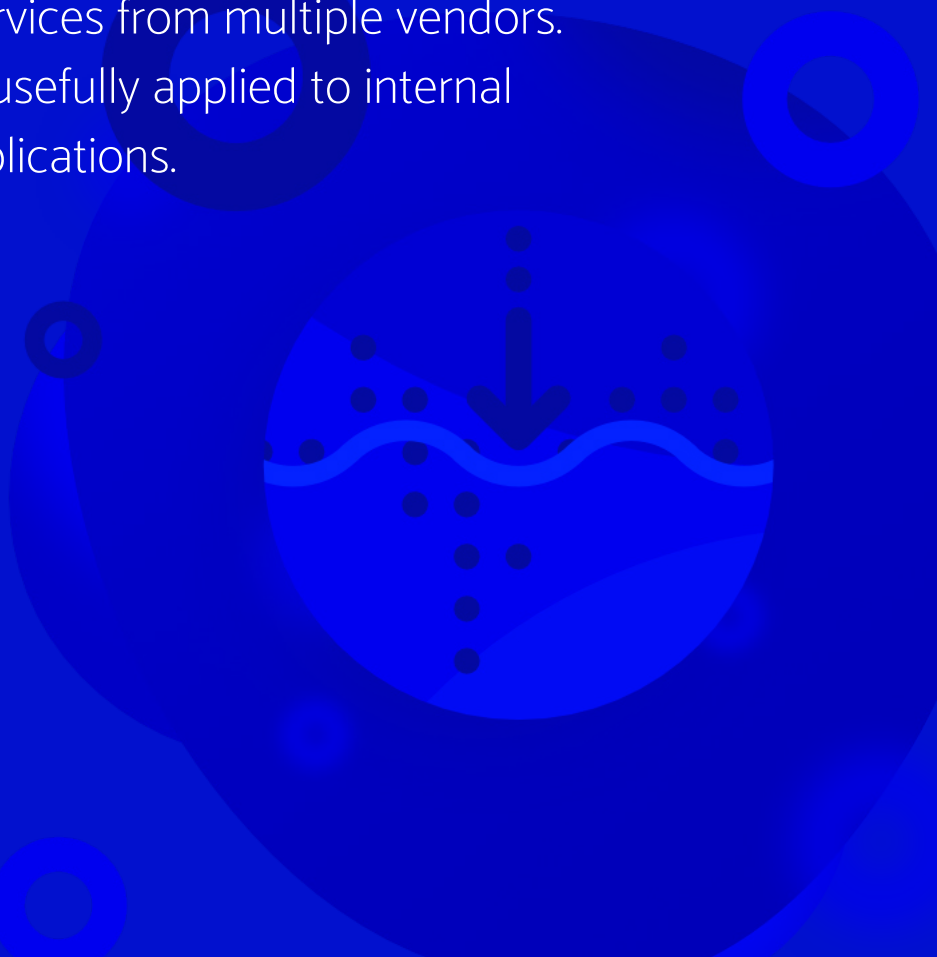
METCLOUD

GET CONNECTED • CYBER SAFE

What is PEN testing?

Penetration testing is a core tool for analyzing the security of IT systems. It is a method of gaining assurance in the security of an IT system by trying to breach its policies.

It should be considered a useful process but not the primary or the only method to detect vulnerabilities. PEN testing is an appropriate method for identifying the risks present on a specific, operational system consisting of products and services from multiple vendors. It could also be usefully applied to internal systems and applications.



Types of testing

VULNERABILITY IDENTIFICATION IN BESPOKE OR NICHE SOFTWARE

Most used in web applications. This type of testing must give feedback to developers on coding practices which avoid introducing the categories of vulnerability identified.

SCENARIO DRIVEN TESTING AIMED AT FINDING VULNERABILITIES

The penetration testers explore a specific scenario to discover whether it detects a vulnerability in your defenses. Our team is considering earlier incidents, which scenarios are most relevant to your organization.

SCENARIO DRIVEN TESTING OF DETECTION AND RESPONSE CAPABILITY

In this version of scenario driven testing, the aim is to also gauge the detection and response capabilities your organisation has in place. This will help you understand their efficacy and coverage in the scenario.

How does PEN testing work?

SCOPING

Scoping involves all relevant risk owners, informed technical staff about the targeted system and a representative of the penetration test team. This way any areas of special concern will be outlined, the technical team will profile the technical boundaries and the penetration team will suggest what testing will give a clear picture of the vulnerability status.

TESTING

During the testing phase, it is crucial to have a technical point of contact on call. This allows the test team to raise any critical issues found during the process and resolve them on time like network misconfiguration. It should be noted that it is possible to find more systems or components which lie outside the existing testing scope. In this case the testing team might change the testing scope and alter testing time frames or costs.

REPORTING

When the testing process is over, the generated report has detected any security issues and the risk levels that each vulnerability exposes the organisation to. Moreover, includes resolving methods per issue and improvements for the internal vulnerability assessment.

SEVERITY RATING

According to the Common Vulnerability Scoring System, severity rating tries to give a numerical score for any vulnerabilities found. Depending on the risk level of the vulnerabilities found the PEN team will decide if further mitigating controls need to be applied.

FOLLOW UP ON THE REPORT

The PEN report is assessed by the organisation's vulnerability team. Any new detected vulnerabilities will require special attention based on their severity and the PEN testers will suggest the best solutions for your needs.

PEN TESTING WITH METCLOUD

- Web Application Testing
- Network Services Testing
- Physical Testing
- Social Engineering Testing
- Client-Side Testing
- Mobile Application Testing

ADD ON SERVICES

- Red, blue, or purple testing teams
- IT Security Architecture Review (when the blue or purple team used)
- IT Security consultation services

Using PEN testing effectively

It is suggested to run PEN testing once every year, so you will not miss any vulnerability issues during this time. Third party PEN tests should be performed by qualified and experienced teams only, for the safety of your business. The National Cyber Security Centre recommends always using testers and companies which are under the CHECK scheme.

The NCSC recommends organisations to use testers and companies which are accredited at least with one of the following accreditations: **CREST, Tiger Scheme, CBEST, STAR, SCIR, CHECK, STARFS, ASSURE**

Why METCLOUD?

Award winning company for cybersecurity, innovation, and excellence. Our vision is to be the global brand of choice for next generation cybersecure cloud services. Our services have been architected with security by design. Ransomware, Cloud vulnerabilities, Phishing attacks Social engineering and vulnerability management are the five top global security threats. METCLOUD's portfolio of cyber security and cloud services will ensure that you protect, defend, and mitigate any potential cyber attack irrespective of how it was carried out.

Let’s get connected.

Speak to us and learn more about penetration testing.

Call 0121 227 0730
and speak to one
of our experts.

Email the team.
hello@metcloud.com

Visit our website for
more information.
metcloud.com

METCLOUD

GET CONNECTED • CYBER SAFE