Continuous Automated Penetration Testing

Testing your system's weaknesses and making sure there are no possible breaches in the perimeter should be a recurring practice.

Continuous automated penetration tests ensure these checks across the entire perimeter.

CYBERFERO

Clus**t**
Associazione Italiana per la Sicurezza Informatica

Realistic simulation

The test attack, run in a controlled and therefore zero-risk environment, is executed exactly as it would happen in the real world: **directly from the network, with no known credentials — just as a hacker would.**

No service interruption

The goal is to stay unnoticed; that's why we make sure the process won't disrupt the service, simulating the techniques a real attacker would use. **An attacker would try to stay undetected, and so will we.**

Reporting and remediation

The service delivers a detailed report of every step of the attack vector. From it, **we compile a list of vulnerabilities with the corresponding mitigations to apply by order of risk priority.**

What a Penetration Test is for

A *Penetration Test*, or *Pentest*, is a security tool designed to test the strength and security of a network. The idea is to simulate the behaviour of malicious actors and try to breach the system in various ways.

We recommend running a *Pentest* regularly, especially after significant infrastructure changes. However, a classic *Penetration Test* isn't enough to make sure that day-to-day operations don't put the entire infrastructure at risk.

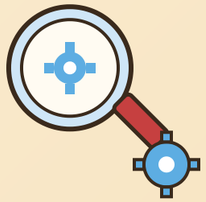
That's why continuous automated Pentesting was created. By running automated exploits directed at the network, it becomes possible to constantly verify that the infrastructure is safe and not exposed to risk.

CYBERFERO

Our Penetration Tests

Up-to-date techniques

The system will always use the most up-to-date penetration techniques, for the best possible check.



Variable test frequency

The frequency of continuous testing can reach a daily cadence, so you can continuously verify the state of your infrastructure.

No interference with other services

Continuous automated *pentesting* does not affect any other services **Cyberfero** offers for your business's security.

Manual vs. continuous Pentest comparison

Pentest	Manual	Automated
Duration	A few days	Continuous over time
Techniques used	Limited to the tester's knowledge	Always up-to-date. No far-fetched scenarios are implemented
Coverage	Partial, circumstantial	Complete
Execution skill	Fluctuating	Consistent
Risks	Could cause downtime	No risk

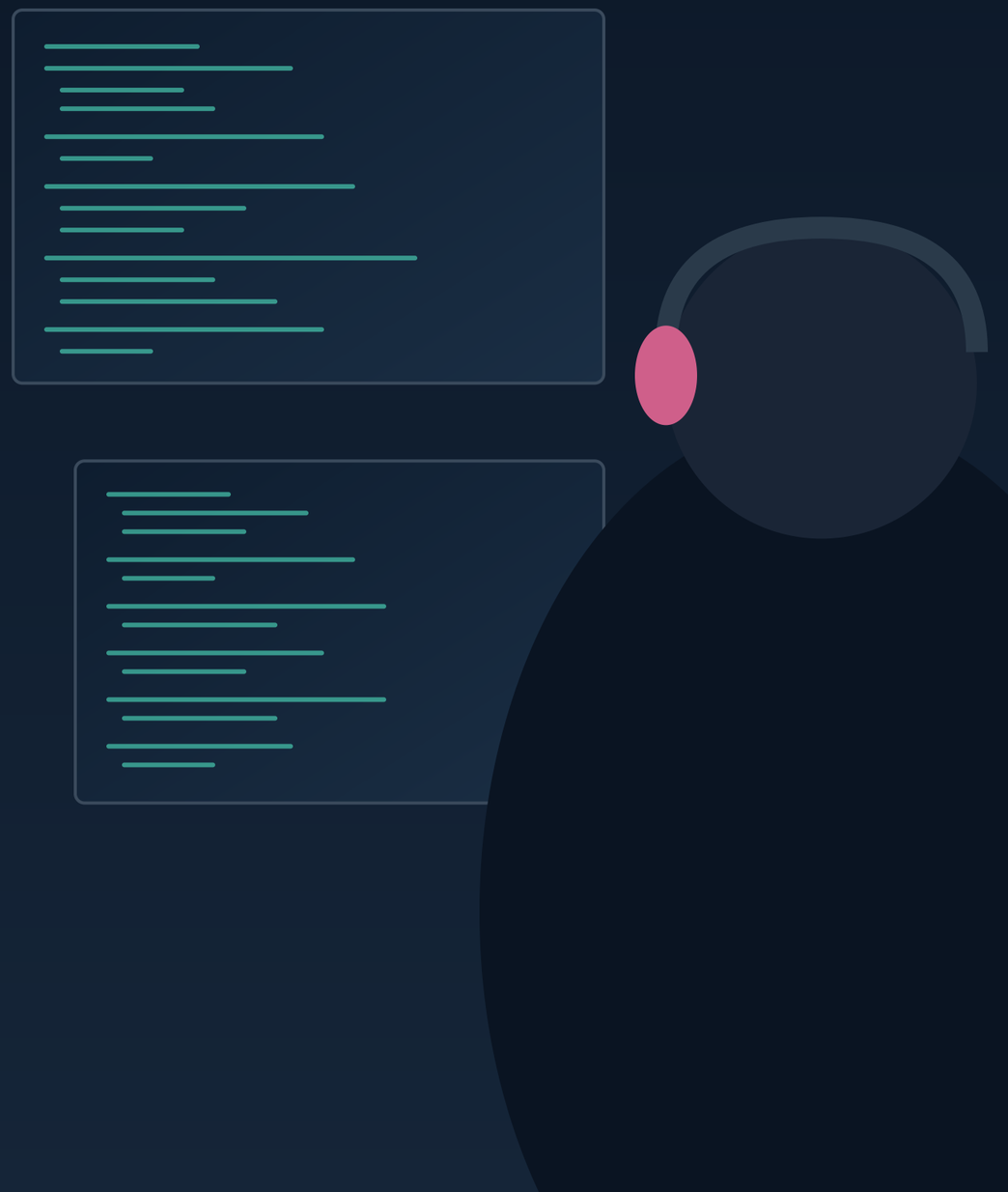
Note: *Continuous pentesting doesn't replace manual pentesting, which it's still good practice to schedule regularly.* ***The two services don't exclude each other — they complement one another.***

CYBERFERO

Our approach

Our advice is to run a thorough manual *Penetration Test* once a year (or after significant infrastructure changes) and to run automated *pentests* continuously.

Other services that can be paired with continuous pentesting: **Web Application Test**, **Cyber Threat Intelligence**, **SOCaaS**.



CYBERFERO

Since 2011 we've been working in Cloud technology and cybersecurity — rely on experienced professionals.

Choose security for your business

Discover the service on our website

CYBERFERO

For more information, our contact details are:

Via Statuto 3,
42121 Reggio Emilia (RE), Italy
www.cyberfero.com

Phone: +39 0522 1685330
E-mail: info@cyberfero.com
PEC: cyberfero@pec.it
VAT ID: 03058120357

Clust
Associazione Italiana per la Sicurezza Informatica