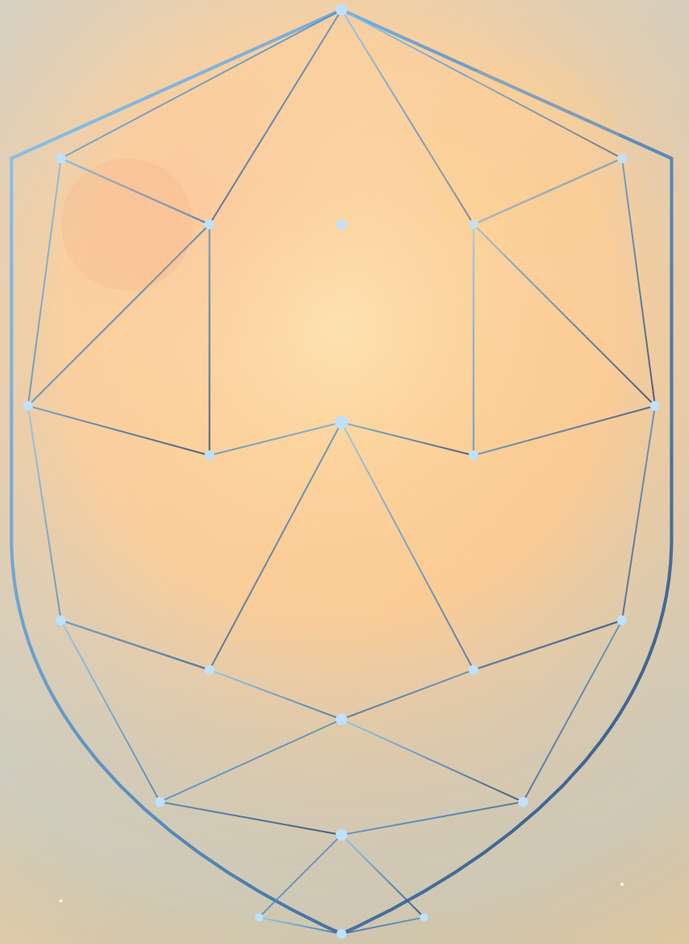
CYBERFERO

Vulnerability Assessment Penetration test



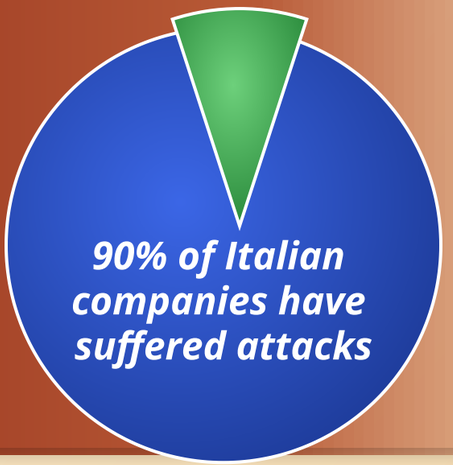
Check the **security** of your IT department

Spot threats before they become a problem

Implement solutions to strengthen your protection

*Your **data** is at risk.*
*Your **company's data** is at risk.*
*Your **clients' data** is at risk.*

Can you claim otherwise?



Source: Il Sole 24 Ore

Italian companies seem to have a problem: they don't take cybersecurity seriously enough — **90% of them have suffered a successful attack**.

The solution? **Design an effective prevention plan** that lets you intercept threats and mitigate attacks quickly.

Cyberfero offers a range of services for managing your company's security.

The core services every mid-sized company should adopt are:

Vulnerability Assessment &

Penetration Testing

CYBERFERO

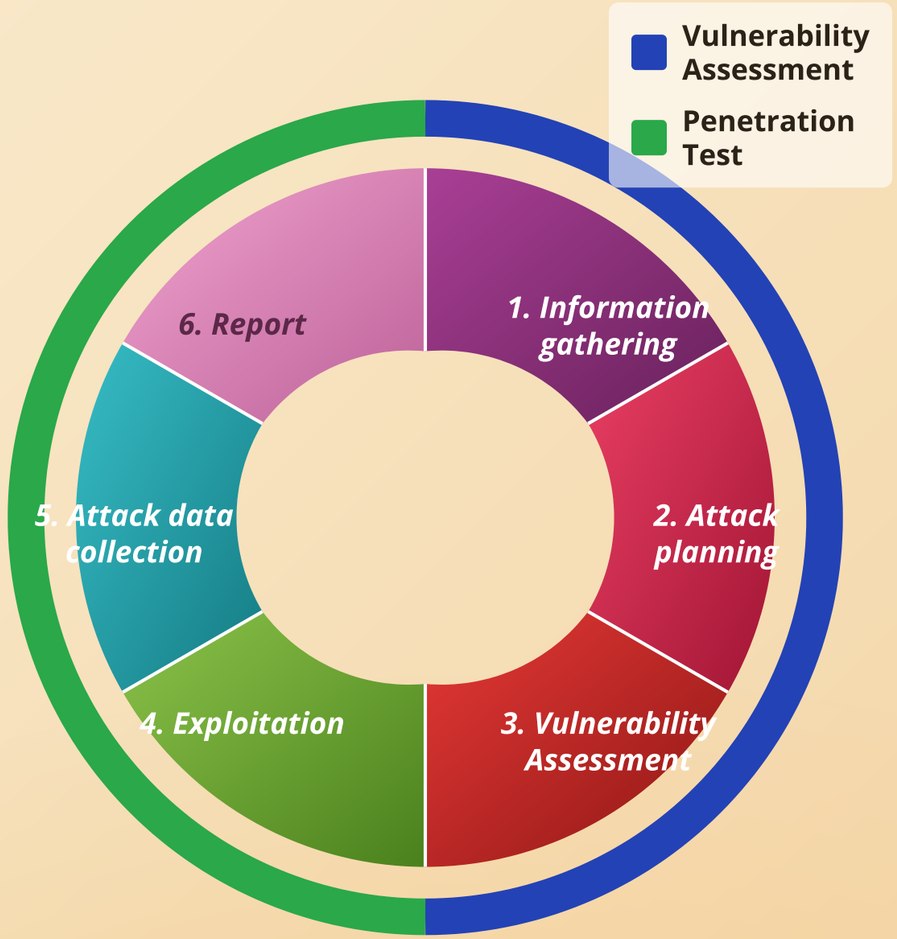
Our approach

As shown in the chart, the approach is divided into a first phase of **Vulnerability Assessment**, *during which the system is scanned and* **potential threats are identified**. *This phase covers steps 1 through 3 in the diagram.*

If the engagement doesn't include a Penetration Test, **a report is drafted summarizing the findings** *and solutions are recommended to address the issues — but their implementation is left to the client.*

When the engagement includes one, once potential threats are identified **they are tested and verified through a Penetration Test** *to validate the issues and pinpoint which techniques the system is most vulnerable to.*

The system is put to the test by a team of ethical hackers who verify whether it's possible to penetrate it by any means.



Some of the techniques used in our tests

- **Network Sniffing**: Capturing and analysing intercepted network packets
- **IP port scanning**: Scanning the network to identify access points
- **ARP spoofing**: Man-in-the-middle attacks against the network
- **Password deduction**: Attempts to capture and infer system passwords
- **System control**: Attempting remote control of the systems involved

CYBERFERO

How the Cyberfero engagement process works

The client requests support via our website

The request is reviewed and a service proposal is drafted

The proposal is submitted to the client and accepted

Vulnerability Assessment and Penetration Test begin

Threats are mitigated and breaches repaired (optional)

We remain available for further work and verifications

On completion, reports are drafted and delivered to the client

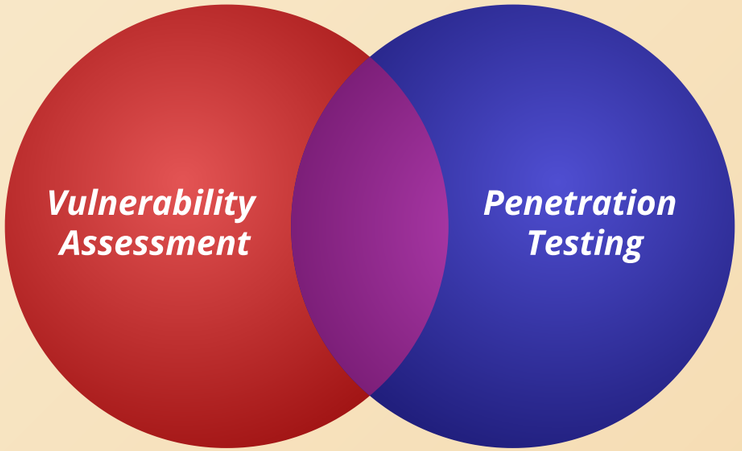
Threats and system flaws are identified and tested

CYBERFERO

Vulnerability Assessment vs. Penetration Testing

How to choose

When deciding whether to run just one or both, **you have to evaluate based on the results you need**. If you only want a general overview, a VA may be enough. If your goal is to **raise the overall security level of your system**, our advice is to run VAs regularly over time and PTs occasionally as verification — especially after major updates.



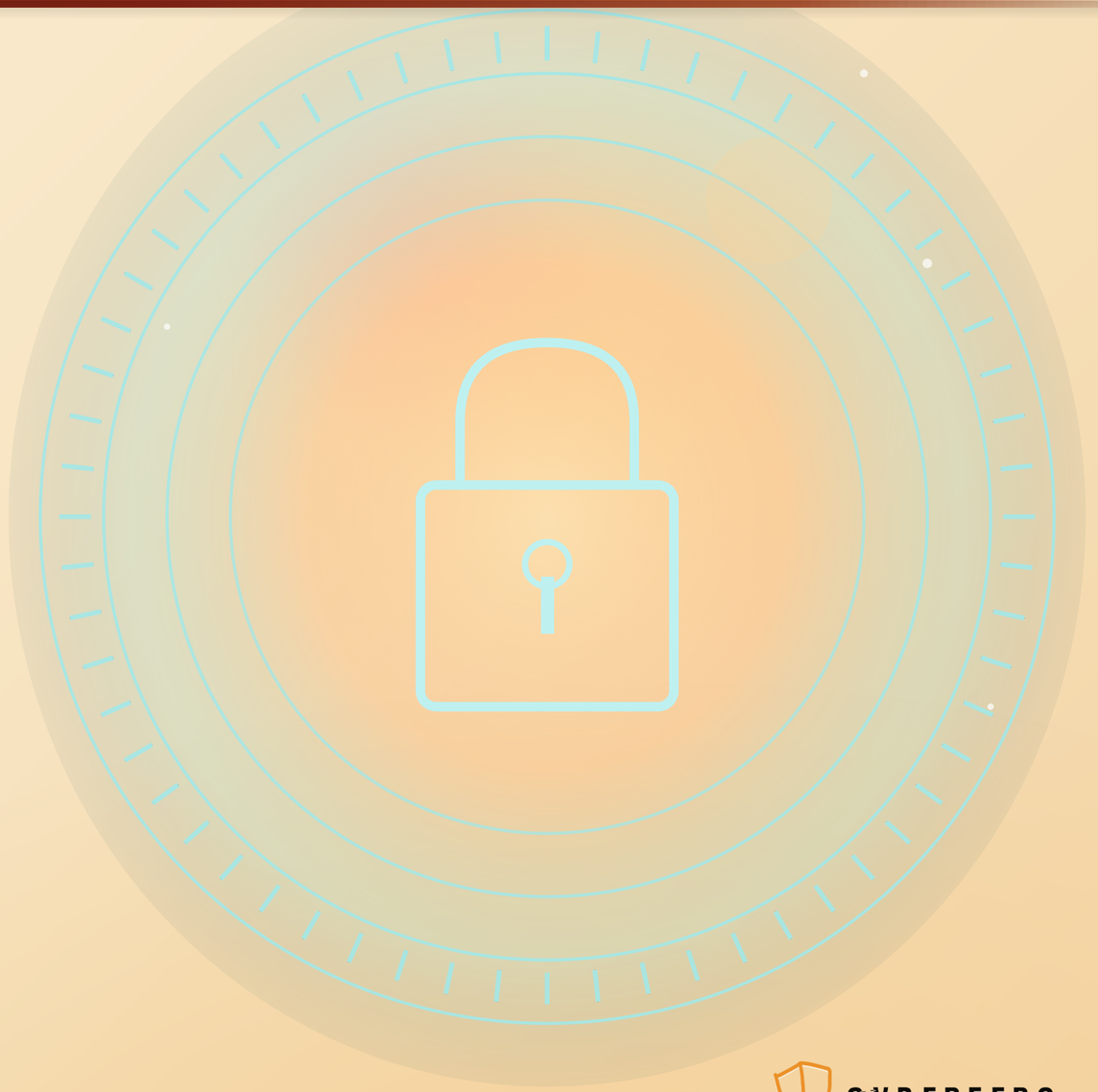
	Vulnerability Assessment	Penetration Testing
Purpose	Identify the system's weak points	Discover and exploit weak points
Deliverables	List of possible breaches and weaknesses	List of vulnerabilities, how to exploit them and recommendations
Next steps	Prioritise actions to contain the flaws	Contain the flaws and remediate the system

CYBERFERO

Choose security for your business

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

Discover the service on our website



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

CYBERFERO