ASSESS YOUR OVERALL SECURITY BEFORE ATTACKERS DO

Advise Tech

VONAHI SECURITY

WE NOW LIVE IN A DIGITAL ECONOMY

56% OF ALL INTERNET TRAFFIC IS CRIMINAL IN NATURE.

AN ERA WITH DATA BREACHES ON THE RISE

2005

157
data breaches

66.9 million
records exposed

2022

11,476
data breaches

1.66 billion
records exposed

Source: https://www.idtheftcenter.org/data-breaches/

61% of small and medium businesses are now being hit by cyber attacks every year, and the average cost of a cyberattack has ***increased to $4.5 million***, making it extremely difficult for businesses to recover.

SMBs with fewer than 100 staff members account for **98%** of all U.S. companies — that's ***5.7 million businesses*** according to the U.S. Small Business Association.

90% of those businesses have fewer than 20 employees and simply can't afford to spend $2-5k for an annual penetration test. **That's where we come in!**

How Do *Data Breaches* Occur?

A *data breach* occurs when a cybercriminal infiltrates a data source and extracts confidential information. This can be done by accessing a computer or network to steal local files or by bypassing network security remotely. The most common cyber attacks used in data breaches are outlined below.

RANSOMWARE

MALWARE

PHISHING

DENIAL OF SERVICE (DOS)

The *best defense* is a good offense.

OFFENSIVE SECURITY

- Vulnerability Assessments
- ***Penetration Testing***
- Social Engineering

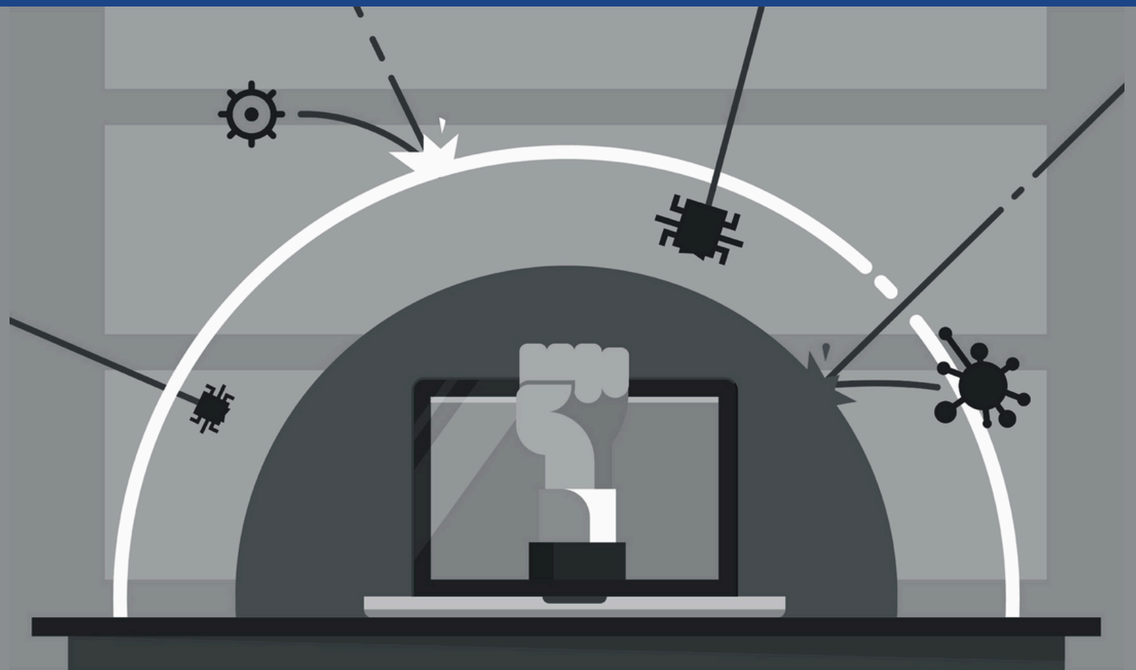
DEFENSIVE SECURITY

- Implementing Controls
- Security Monitoring
- Incident Response

Why Does Your Organization Need a *Penetration Test*?

Penetration tests allow organizations to *assess their cyber security posture based on* ***realistic attack scenarios***, which enables them to address issues that would be overlooked if they followed a solely defensive approach.

Penetration tests reveal crucial security flaws.

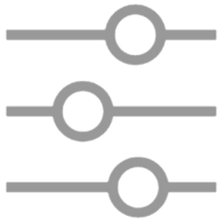


They expose issues beyond the scope of vulnerability assessments.

Penetration Testing Works

Penetration testing is clearly *effective in exposing ways* in which threat actors could break into and move across your network in order to:

ACCESS



MANIPULATE

DAMAGE

SELL

valuable data and systems within your organization. Focusing on defensive security alone, like many companies do, is a fundamentally flawed strategy.

Penetration Testing and its Purpose

01 **Demonstrate real-world risk** by simulating a malicious threat actor

02 **Evaluate current** security detection and monitoring controls

03 **Provide businesses** with remediation strategies to mitigate risk

04 **Understand how attackers target** their most confidential/sensitive data

We make Penetration Testing **More Affordable**

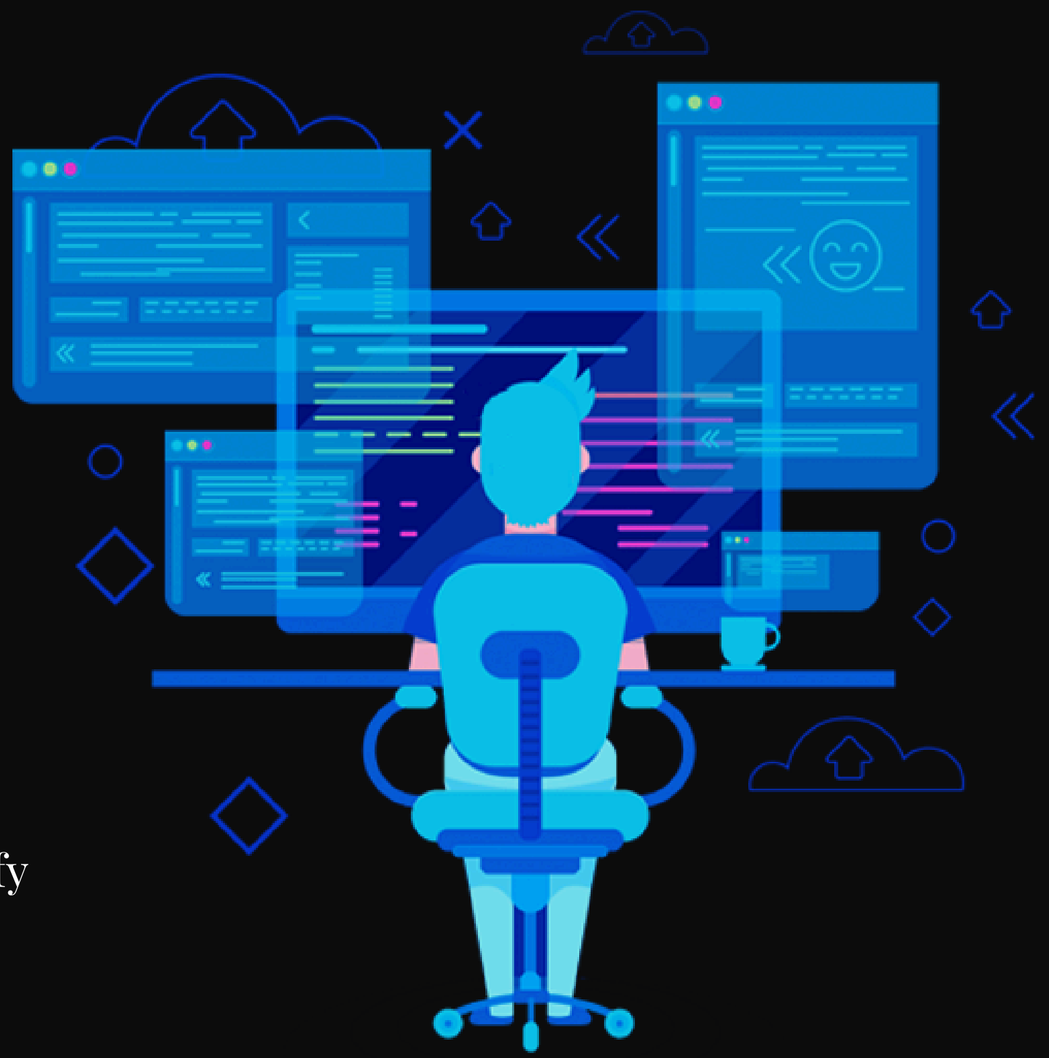
- We deploy the **latest technology** that helps our team perform penetration testing more efficiently and we pass those savings to bring you pen-testing at an affordable cost.
- More penetration tests **without breaking the bank**

We make Penetration Testing **More Valuable**

- Email and SMS **notifications** to stay in the loop during the penetration test
- **Real-time** tracking of attacks and findings
- **Reports** are available within 24 hours after a penetration test is complete.

We make Penetration Testing **More Continuous**

- **Move beyond compliance** and meet industry best practices
- Perform a penetration test **whenever and however often** you want.
- **Stay in the know** rather than hope for the best



Penetration Testing is Worth Every Penny

Using the results of a penetration test, your organization can identify ways to ***protect its most valuable data*** by reducing the number of attack vectors and accessible paths to sensitive resources and systems.