HOLISTICYBER
DEFEND WHAT MATTERS | SOLUTION BRIEF

Penetration Testing & Vulnerability Scanning

Proactively revealing security vulnerabilities and protecting your organization.

What are penetration testing and vulnerability scanning?

HolistiCyber's Penetration Testing & Vulnerability Scanning form a unique program that pinpoints where cyber security vulnerabilities exist in an organization, and how a cyber offender would exploit them. The program is unique as it combines the use of sophisticated technologies, White Hat security experts and nation-state grade level defense expertise. First, vulnerabilities are proactively exposed, followed by recommendations how to close security gaps along with a clear priority list.
The goal is to mature the organization's pentesting program and elevate its overall security posture.

How does this work for me?

1. An organization can't protect against what it is not aware of. The program starts by scanning for vulnerabilities, and gaining the list of critical cyber risks and attack paths.
2. The team simulates attacks on the organization's IT systems, in different areas, including data, infrastructure, applications, endpoints and user IDs. All testing versions are included: Black, Grey and White Box.
3. Following testing, and in consideration with the company's business needs, top priorities are provided along with precise remediation workflows, to turn recommendations into actionable tactics.

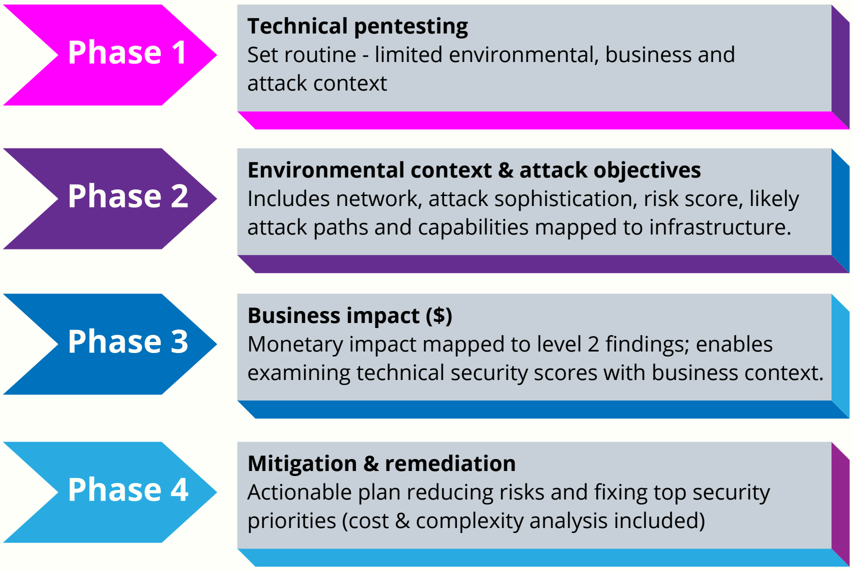
WHAT SHOULD YOU EXPECT?

- **Visibility to all key attack vectors including most sophisticated cyber-attacks.**
- **Planning and reconnaissance, threat identification and real-life testing.**
- **Clear and simple presentation of results.**
- **All compliance regulation versions fully supported.**
- **Tests include all key domains; IT systems, applications, endpoints, user IDs, etc.**
- **All testing versions included: Black/ Grey/ White box.**
- **Maturing organizational pentesting program to include business requirements and analysis.**
- **Clear prioritization of security threats that need to be handled immediately vs. items that do not pose an immediate risk.**
- **Streight-forward remediation and mitigation tactics and workflows.**
- **Elevating security posture.**

How can enterprises keep up with today's cyber threats? By getting ahead of them.

For many companies, pentesting has become a compliance requirement, a tick-box exercise demanded by regulators and customers, rather than a crucial tool to assuring business continuity and productivity and bolstering an organization's cyber security state. Additionally, once a pentest is concluded, it is not clear which findings should be prioritized in terms of focus and action. Enterprises wind up wasting time and budgets in fixing noncritical issues, while leaving significant risks unattended.

To address these issues, HolistiCyber employs a holistic approach to each test, which includes technical findings together with a deep analysis of business needs, the threats and the attackers' motivations. We advocate using the following phased approach to improve testing maturity:

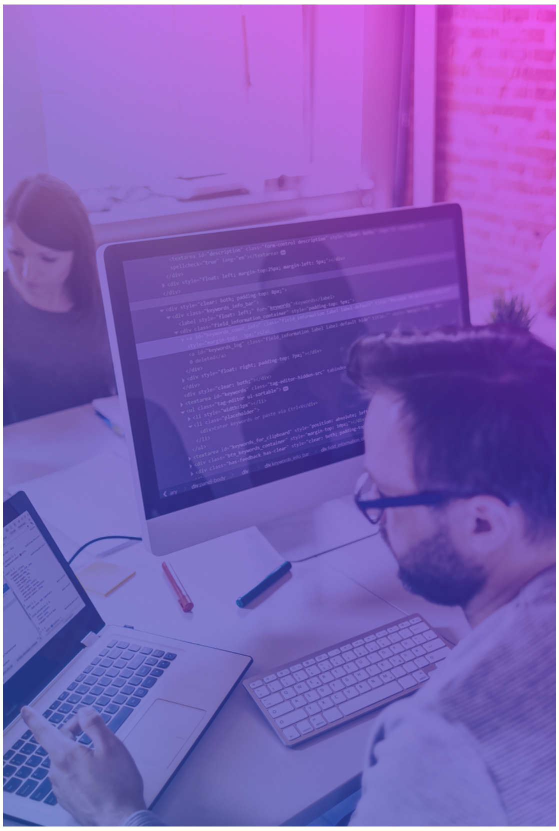


Phase 1 – **Technical pentesting**
Set routine - limited environmental, business and attack context

Phase 2 – **Environmental context & attack objectives**
Includes network, attack sophistication, risk score, likely attack paths and capabilities mapped to infrastructure.

Phase 3 – **Business impact ($)**
Monetary impact mapped to level 2 findings; enables examining technical security scores with business context.

Phase 4 – **Mitigation & remediation**
Actionable plan reducing risks and fixing top security priorities (cost & complexity analysis included)



Oftentimes, security teams limit pentesting to what we call phase one, the technical-led pentesting category, which will suffice for compliance purposes. However, using a minimized scope of work in a penetration scenario, typically leaves glaring security gaps unnoticed and unattended.
As more phases are applied, more business and security related priorities become clear and visible, along with actionable and pragmatic remediation tactics.

Why HolistiCyber?

We see things differently compared to other companies. Here's why.

1. **Nation-state grade expertise** - our staff of white-hat testers, former military and government offensive experts examine the attack surface from the **vantage point of the attacker** and not from the vantage point of the company. This includes a solid grasp of the **sophisticated tooling** available to today's attackers along with access to those attack tools.
2. **Holistic approach** - remediation and mitigation solutions are tied to each company's unique business objectives and workflows. Security should compliment productivity and growth and avoid hindering it.

"These guys really know what they are doing, and they provide customer service with each pentest that they do, above and beyond what we had received from other companies. They helped us to take control and drive results."
CISO, large utilities corporation, USA