Continuous Assurance Program

Cut down security gaps with continuous validation of your security program.

What is Continuous Assurance Program?

CAP is a managed cyber security service that includes year-round penetration tests, holistic risk assessments, and domain expert strategies to close security gaps in the enterprise and avoid vulnerability exploitation.
Security vulnerabilities are proactively exposed while security experts apply nation-state-grade expertise and strategies to close the gaps along with a concise priority list to handle risks.

How does this service work for me?

The program is provided as a single subscription and incorporates people, processes, and technology in one package.
A dedicated team of experts is assigned to the customer company to map out the organization and its threat landscape, along with hands-on tests and assessments throughout the year.
When additional expertise is required, such as for a newly acquired technology, a significant acquisition, or a period of change, HolistiCyber delivers surge capacity as part of the engagement. As such, the service helps organizations to quickly fill the growing cyber security skills gap in a lean and efficient way while delivering year-round assurance.
Onboarding processes are tailored to scale with the organization for a seamless transition between HolistiCyber and in-house security teams. The handoff often follows the 'assess' phase, allowing security teams to focus on prioritized remediation.

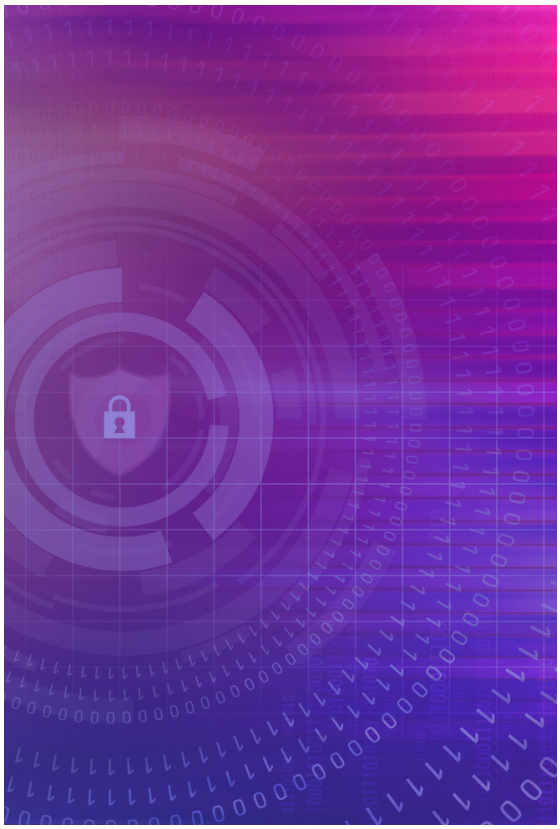
How can enterprises keep up with today's cyber threats? By continuously getting ahead of them.

For many companies, pentesting and risk assessments have 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.
At the same time, organizations are being breached every day because of the complexities in managing wide-ranging, variable, and unknown attack surfaces. Cyber risk exposure is rapidly evolving, often due to business factors that are outside the influence of security teams:

WHAT SHOULD YOU EXPECT?

- **Tailored and scalable security assurance program.**
- **Zero overhead, fully managed service.**
- **A single subscription service incorporates people, processes & technologies in one package.**
- **Visibility to all key attack vectors, including most sophisticated cyber-attacks.**
- **Planning and reconnaissance, threat identification, and real-life testing.**
- **Assessing all key domains; IT systems, applications, endpoints, user IDs, etc.**
- **Policy outline adapted to unique company business needs, priorities, and risk tolerance.**
- **Maturing organizational security program to include business impact analysis.**
- **Additional assessments and testing as needed.**
- **Continuous prioritization of security threats that need to be handled immediately vs. items that do not pose an immediate risk.**
- **Straight-forward remediation and mitigation tactics and workflows.**

- Mergers and acquisitions bring new attack surfaces into the organization
- IT testing and shadow IT may not follow security procedures, creating rogue assets
- Changes in personnel or a lack of documentation lead to knowledge expiry



Without understanding the real-world implications of an attack, financial, reputational, and legal, security teams will not know where they should focus their efforts. The need to remediate requires us to prioritize handling critical risks soon versus risks that can be placed on the "back burner" and dealt with in the next six months or a year. Prioritizing involves adding business context to the findings and ensuring they are understood in financial and operational terms.
Risk assessments incorporate threat modeling exercises and highly targeted business interactions to validate that the underlying vulnerabilities are exploitable and are to be considered as top security issues.

Building blocks of Continuous Assurance Program

Chart	Assess	Prioritize
Continuous mapping of the perimeter to ensure complete coverage	Understanding real-world exploitability of vulnerabilities, and apply the business context	Ensure focus is applied to fix the findings that carry the highest business risk

CAP creates an 'always-on' human pentesting capability providing the security team with an early warning view of vulnerabilities that merit genuine concern while filtering out the false positives.

Why HolistiCyber?

1. **Nation-state-grade expertise** - our staff of white-hat security experts is composed of former military and government offensive practitioners who can examine the attack surface from the vantage point of the attacker and not only from the company's vantage point. We have a solid grasp of the sophisticated tooling available to today's attackers and access to those attack tools.
2. **Holistic approach** - we tie compliance, remediation, and mitigation solutions to each company's unique business objectives and workflows. Security should complement productivity and growth and avoid hindering them.

"One of the reasons we like having HolistiCyber onboard is that they provide the expertise that would require hiring a large professional team to get the experience needed. In any case, it is almost impossible to assemble such a team, not to mention expensive.
These folks provide knowledge, expertise, and excellent customer service."

CISO, Financial Institution, USA