RansomSight

Protects your organization against targeted ransomware.

What is RansomSight?

RansomSight is a ransomware defense service designed to mitigate the wide-ranging effects of specific ransomware attacks on organizations. It includes penetration tests specifically targeting ransomware tactics, techniques, and procedures (TTPs) and pinpoints where cyber security vulnerabilities exist in an organization, and how a cyber offender would exploit them to carry out these ransomware attacks.

The service provides critical and actionable information allowing organizations to be prepared in the event of an actual attack. It is unique as it combines the use of people, process and technology, simulating the actions of a ransomware gang, and not just the tech they use. Nation-state grade defense experts provide tailored recommendations to close security gaps along with a clear priority list.

How does RansomSight work?

1. We focus on specific ransomware groups, known for their ransomware campaigns and map the commonly used TTPs (based on the Mitre ATT&CK Framework).
2. Our team scans for vulnerabilities, and creates a list of critical cyber risks and attack paths.
3. White hat experts simulate attacks on the organization’s IT systems, in different areas, including data, infrastructure, applications, endpoints and user IDs.
4. Activities are coordinated with the company's security operations (they can report which attempts they see as we step through each ransomware technique simulated).
5. Results are delivered in a user-friendly report indicating which TTPs were blocked, detected, executed, etc. with reference to full details on each TTP, allowing for remediation actions if needed. The report includes mapping to the Mitre ATT&CK framework, highlighting strong and weak areas in the organization’s resilience towards the TTPs.
6. 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?

- **Defense against potential ransomware attacks.**
- **Visibility to key attack vectors including most sophisticated ransomware attacks.**
- **Clear and simple presentation of testing results.**
- **Tailored recommendations from domain experts including straight-forward remediation and mitigation tactics and workflows.**
- **Fast: typically completed within a day or two when run for a single threat actor.**
- **Remote service with virtually no impact.**
- **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.**
- **Tests include all key domains; IT systems, applications, endpoints, user IDs, etc.**

What is our holistic approach?

HolistiCyber employs a holistic approach to each simulation and test, which includes technical findings together with a deep analysis of business needs. We use a phased approach:

Phase 1

Technical penetration testing
Execute ransomware group TTPS on client environment.

Phase 2

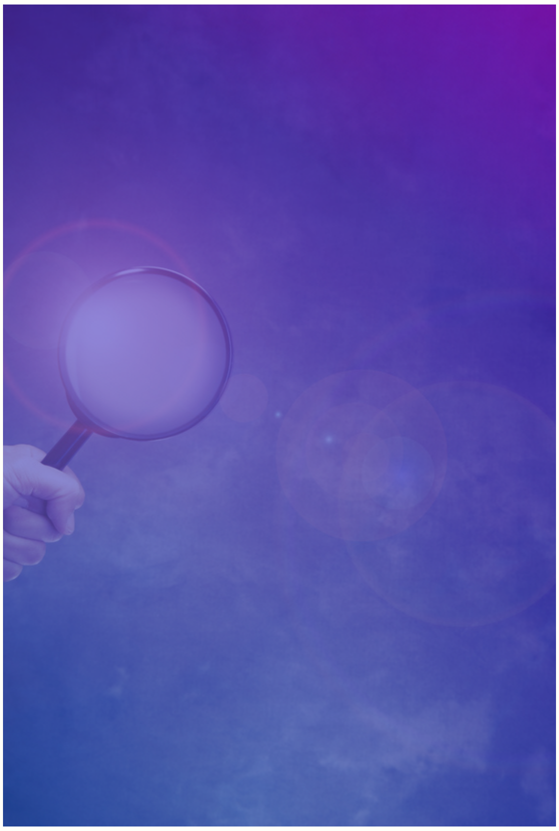
Environmental context & attack objectives
Includes network, attack sophistication, risk score, likely attack paths and capabilities mapped to infrastructure.

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)



Creating a robust line of defense against ransomware attacks.

Once these focused ransomware pentests are concluded, it will be clear which findings should be prioritized in terms of focus and action. The company will save time and budgets by fixing critical issues, and avoiding the futile attempt of attending to all cyber risks, which isn't possible in any case. Handling these crucial issues quickly will create a robust line of defense for your company against attacks that could otherwise cause catastrophic consequences such as devastating downtimes, with irrevocable financial and/or reputational losses.

Why HolistiCyber?

1. **Nation-state grade expertise** - our staff of white-hat testers, former military and government domain 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.

> ***"We know that ransomware attacks have been increasing over the past two years and it was a big concern for us. We brought in HolistiCyber to test our environments. It gave us a clear picture of where we stood and what was needed to shore up our defenses. I now have confidence in our ability to identify and stop a ransomware attack should one materialize in the future."***
>
> **CISO, US Commercial Bank**