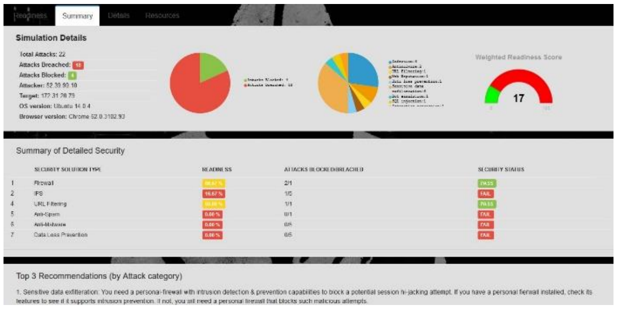
WhiteHaX Cyber-readiness Verification for Mid-tier Businesses

WhiteHaX – cyber-readiness verification: WhiteHaX is a cloud-hosted, automated, cyber-readiness verification (pen-testing) platform. The WhiteHaX cyber-insurance version provides a quick (under 15-min) verification of a business' cyber-readiness by simulating several threat scenarios against the business' deployed security infrastructure, including network perimeter defenses and endpoint security & controls. A few examples of these simulated threat scenarios include firewall attacks, user-attacks from internet such as drive-by downloads, email phishing/spoofing/spamming, ransomware, data-exfiltration attempts and others.

Measure cyber-readiness of deployed security controls: The primary focus of WhiteHaX cyber-insurance version is to verify the strength of your business' deployed security solutions and controls, using simulations of some of the most common and dangerous cyber threats/attacks. WhiteHaX simulations are performed to test security solutions and controls for - Firewalling (Network & Endpoint), Intrusion Prevention, Anti-Malware (Network & Endpoint), URL Filtering, Data Leakage Prevention, Ransomware prevention, User behavioral threats and OS & S/W vulnerabilities management.

WhiteHaX – verification process: WhiteHaX is a purpose-built platform, specifically designed for Cyber insurance policy-holder businesses. Using its patent-pending QIVE (Quick, Intelligent Verification Engine), it simulates many cyber security breach, exploits and attack scenarios, called Indicators of Prevention (IoPs) to quickly assess the readiness of the deployed security infrastructure solutions and their respective configuration policies against such threats. WhiteHaX utilizes the most recent and the most commonly used attack techniques and breach scenarios to verify how well your business withstands these threats in detecting and preventing them from compromising your internal assets.



Simulation Details

Total Attacks: 22
Attacks Breached: 18
Attacks Blocked: 4
Attacker: 52.39.99.10
Target: 172.31.20.79
OS version: Ubuntu 14.0.4
Browser version: Chrome 52.0.3102.93

Summary of Detailed Security

	SECURITY SOLUTION TYPE	READINESS	ATTACKS BLOCKED/BREACHED	SECURITY STATUS
1	Firewall	[illegible]	2/1	PASS
2	IPS	16.67 %	1/5	FAIL
4	URL Filtering	[illegible]	1/1	PASS
5	Anti-Spam	0.00 %	0/1	FAIL
6	Anti-Malware	0.00 %	0/5	FAIL
7	Data Loss Prevention	0.00 %	0/5	FAIL

Top 3 Recommendations (by Attack category)

1. Sensitive data exfilteration: You need a personal-firewall with intrusion detection & prevention capabilities to block a potential session hi-jacking attempt. If you have a personal ferwall installed, check its features to see if it supports intrusion prevention. If not, you will need a personal firewall that blocks such malicious attempts.

A unique login (through self-registration) or a URL for access to the WhiteHaX cloud-hosted platform, will be provided through your cyber-insurance broker or provider. This login will enable you to connect from any computer within your company's internal network to the Cloud-hosted WhiteHaX platform. Typically, you should either utilize a standard endpoint machine-image given to end-users or a standard server-image used in your infrastructure to connect to the WhiteHaX platform for your cyber-readiness verification.

Once the connection is established between your endpoint/server and the WhiteHaX platform, attacks are simulated bi-directionally either through the browser (which acts as a client) or a downloadable (no-install) self-destructing executable. Once all attack simulations are completed, WhiteHaX generates a comprehensive report for your review. The report includes:

- the *Executive Summary* outlining ratings of your overall cyber-readiness along with cyber-readiness of your security solutions and controls against simulated attacks (IoPs);
- the *Details* report showing the details of the executed threats and
- the *Resources* list to help you
    - remediate some of these threats,

  - perform more detailed risk analysis across entire network, servers and other assets, and
  - train your IT and end users on protection/prevention of most common threats.

WhiteHaX Verification – no-impact to your computers or infrastructure: WhiteHaX is designed to provide an internal cyber-readiness verification that is performed from inside-the-firewall of the business. This provides the business an opportunity to periodically self-assess its own cyber-readiness against some the most common, most recent and dangerous cyber threat, attacks and breach scenarios (IoPs).

- WhiteHaX Cyber-readiness verification (pen-test) is performed in less than 15 mins
- WhiteHaX cyber insurance version is specifically designed to run without impacting your infrastructure. WhiteHaX verification,
  - does not require a download if you use the browser based quick -assessment
    - the self-destructing executable provides deeper verification but requires just-in-time download
  - does not require install anywhere – neither for browser-based nor for self-destructing executable
  - does not impact any part of your production infrastructure (you may see security alerts from your deployed security solutions, if they are working correctly)
  - does not leave any footprint behind once it's done running
  - does not capture any proprietary data from your network or computers – not even your IP addresses.

WhiteHaX – Cyber Verification is free: Your cyber-insurance is making WhiteHaX cyber verification available to you free-of-charge. That means, you are getting a free pen-test to perform self-assessment of your business' deployed security solutions, controls and policies. Additionally, WhiteHaX cyber-readiness verification is available to you for periodic verification (multiple times a year) to allow you to self-verify your controls periodically e.g. on a quarterly basis. Please contact your cyber insurance broker or provider to check how often you can self-verify your business' security infrastructure.

WhiteHaX – Improve your cyber-readiness, gradually: Traditional pen-tests and vulnerability scanners produce a long, monolithic report listing large number of issues found. Such report can potentially overwhelm your IT security team resources. WhiteHaX on the other hand, provides a comprehensive report to with a thorough analysis and identification of weakness areas in security posture and potential attack surfaces. Additionally, the report offers recommendations on how to fix top three critical threats, such as which security solutions may need to be updated or deployed. This helps your business improver your overall cyber-readiness posture gradually, without overwhelming IT resources.

WhiteHaX – Keep up-to-speed against latest Cyber threats: WhiteHaX allows periodic self-verification of your deployed business security infrastructure and controls. Since WhiteHaX attack simulations and breach scenarios (IoPs) are adjusted frequently to include the recent cyber threats, it enables the business to verify the security controls against these new threats. AS a result, utilizing the opportunity to periodically self-verify your cyber controls, helps you keep your infrastructure up-to-date against such latest cyber threats.

For further information on how to self-register and other questions, contact your cyber insurance provider or broker. Alternatively send email to CybInsSupport@WhiteHaX.com with your business name & provider name.