Frequently Asked Questions (FAQ)
About WhiteHaX

Q1: What is WhiteHaX?

A1: 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 a number of common threat scenarios against the business' deployed security infrastructure including network perimeter defenses and endpoint security & controls. Some of these simulated threat scenarios include firewall attacks, user-attacks from the internet (such as drive-by downloads), email phishing/spoofing/spamming, ransomware, data-exfiltration attempts and others.

Q2: What does it test?

A2: The primary focus of WhiteHaX cyber-insurance is to verify how strong are your business' deployed security solutions and controls against 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 Controls (Network & Endpoint) & Ransomware prevention;
- Web and other types of Filtering;
- Data Leakage Prevention;
- Protection against User Behavioral Threats (through emails and web-browsing) and
- OS & S/W vulnerabilities management.

WhiteHaX simulates different threats, attacks and breach scenarios to verify if these controls on your network and endpoints adequately protect your assets against such cyber-threats.

Q3: How does WhiteHaX work?

A3: WhiteHaX provides a unique login (through self-registration) or URL to each business customer through your cyber-insurance provider. This login will enable you to connect from any endpoint within your company's internal network to the Cloud-hosted WhiteHaX platform. Once the connection is established between your endpoint and 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, a comprehensive report is generated for your review with :

- an executive summary outlining ratings of your overall cyber-readiness along with the cyber-readiness of your security solutions and controls against simulated attacks;
- a details report showing details of executed threats; and
- a list of resources to help you,
    - remediate some of these threats,

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

You have an option to email or print the pdf report, once the attack simulation is completed.

Q4: How much does it cost?

A4: Not a penny. WhiteHaX cyber insurance cloud-hosted verification is provided to you at no-cost, by your cyber insurance carrier to help you assess, understand and potentially remediate some of the cyber risks you may face. The goal is to help you improve your business' overall security posture over time to stay current against the most common and dangerous cyber threats that your deployed security controls may encounter.

Q5: Will it impact – my machines/servers, or my production infrastructure?

A5: No, WhiteHaX cyber insurance version is specifically designed to run without impacting your infrastructure. It

- does not require a download if you use the browser based quick -assessment,
- does not require install on any of your endpoints, servers or other infrastructure,
- does not impact any part of your production infrastructure except potential alerts from your deployed security solutions,
- does not leave any footprint behind once it's done running, and
- does not capture any proprietary data from your network or endpoint – including your IP addresses.

Finally, it doesn't require any major commitment from your business – only requires 15 minutes or less of your time and a computer to run it from.

Q6: Why should I run WhiteHaX to test our business cyber-readiness?

A6: WhiteHaX is provided as a free service from your cyber insurance provider, CNA, to help you assess, understand and potentially remediate some of the immediate cyber risk your business may have, with a focus on your perimeter defenses and endpoint security & controls. WhiteHaX provides you a good visibility in to the cyber readiness of your business against a number of common and dangerous threat scenarios, without any major involvement from your side, impacting your production infrastructure or requiring any specific assets from your infrastructure. WhiteHaX not only provides you an overall cyber readiness visibility but also a better understanding of your network and endpoint defenses The detailed report generated by WhiteHaX, as outlined in Answer #3 above, provides you details needed to identify, remediate and improve overall cyber readiness of your business infrastructure.

Since WhiteHaX attack simulations change frequently, by testing your security & cyber-readiness periodically through WhiteHaX, you will have a good understanding of potential areas of risks and how

to remediate them. WhiteHaX helps you self-assess your cyber-readiness and gradually improve your overall security posture – all at no cost to you.

Q7: Are our test result data shared with cyber insurer/broker?

A7: First of all, WhiteHaX does not collect any proprietary data from your computer, network or other assets – therefore there is no risk of proprietary data collection or sharing either with WhiteHaX or your cyber insurer. Second, no WhiteHaX data will be shared with your insurance provider, CNA. It is your choice (as an Insured business) whether to share the results with CNA or your broker.

Q8: Will my business be penalized for bad cyber-readiness score?

A8: As outlined in Answer #7 above, no data is shared with your insurance provider, CNA, unless you choose to do so. There is no intention of CNA to penalize yours or any business regardless of how good or bad are your cyber-readiness results from WhiteHaX verification. The WhiteHaX service is provided to you as a valued customer and policy holder of CNA cyber insurance, purely to help you identify, remediate and continue to improve your cyber readiness posture.

Q9: What's the data privacy and security policy of WhiteHaX?

A9: As pointed out in Answer #5 above, WhiteHaX does not collect any proprietary information from your business network, computers or other assets. The only data that is collected is various cyber-readiness scores and test results, which are used to provide a trend of how historically your cyber-readiness has been in the past. For the full information on WhiteHaX data collection, privacy and security, please refer to WhiteHaX Service Agreement on the landing page of the WhiteHaX link that has been provided to you through an email.

Q10: What else can WhiteHaX do to help improve my cyber security?

A10: As outlined in the resources page of the detailed report generated by WhiteHaX, there are recommended next steps which can help you further solidify your overall security posture. These next steps include conducting full cyber-readiness verification and penetration testing of your network assets, application servers and endpoint golden images. The Enterprise version of WhiteHaX can help perform more extensive set of security verification such as a full-scale network pen-test. By providing a set of WhiteHaX versions and partnerships with well-know security solutions and services vendors, WhiteHaX can help you evaluate, understand and remediate weaknesses across your entire security infrastructure. Please refer to Resources page in the report generated by WhiteHaX for more information.