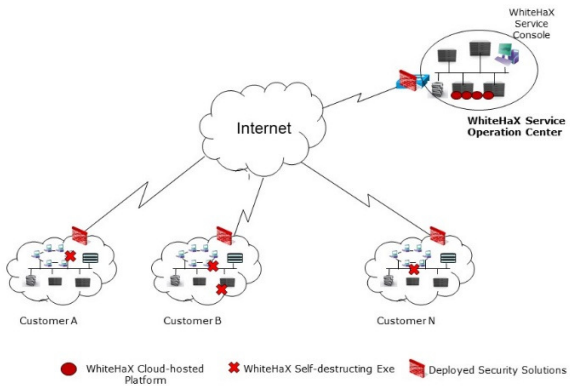
Business Cyber-readiness : With increasing threats of cyber attacks and data breaches, businesses have to be ever so vigilant about ensuring the security & protection of their business assets. Periodically verifying that your business is adequately protected should at least involves two steps and possibly many more. The two important steps though are a) to determine whether your deployed security products and controls are adequately protecting assets from most recent and most dangerous threats, and b) to ensure that if in case there is a breach, that the breach remains contained to single machine and doesn't propagate to other business assets. IronSDN has purpose-built its WhiteHaX platform to allows businesses to periodically verify cyber-readiness and network-readiness of their security infrastructure and to help them stay up-to-date against latest cyber threats.

WhiteHaX – cyber-readiness verification: WhiteHaX is a cloud-hosted, automated, cyber-readiness verification (pen-testing) platform. The WhiteHaX ensures that the business cyber-readiness is adequate by simulating multitude of threat scenarios against the 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.

WhiteHaX – network readiness verification: While WhiteHaX cyber-readiness verification focuses on security controls and infrastructure verification, WhiteHaX network readiness focuses on evaluating security of the business assets (computers) connected on the business network. It performs an extensive scanning of the business network to a) take inventory of network accessible machines and classifying them, and b) identify Vulnerabilities associated with those machines. The network readiness is a crucial aspect of business security as most ransomware, worms and other types of breaches propagate through the network by exploiting vulnerabilities present on network connected machines.

WhiteHaX – network verification process: WhiteHaX is a purpose-built platform, specifically designed to provide no-install, no-impact, automated verification. A simple self-registration process for your business in to the WhiteHaX cloud-hosted platform provides you a unique login and password. This login will enable you to connect from any computer within your company's internal network to the Cloud-hosted WhiteHaX platform. Once the connection is established between your local computer and the WhiteHaX platform, a downloadable, no-install, self-destructing executable runs on your computer and starts verifying your network readiness.



For network readiness, WhiteHaX first takes inventory of machines on the network to determine which machine allows what types of service access. It then uses that information to identify OS, applications and services running on the machine as well as whether these machines are update-to-date on their latest OS releases. WhiteHaX then classifies each machine as either an endpoint or a server, based on the type of services accessible on each. Next, utilizing the inventory, WhiteHaX identifies potential network-exploitable vulnerabilities on each of them. Determining exploitable vulnerabilities allows the security-admin to work through and fix the most dangerous ones quickly.

Once WhiteHaX readiness verification is completed, it generates a comprehensive report for your review. The report includes:

- the Executive Summary outlining ratings of your overall network-readiness along with readiness of servers and endpoints on your network;
- the Details report showing the details of the inventory of machines and detected threats on each; and
- the Resources list to help you
    - remediate some of these vulnerabilities quickly,
    - 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 has No-impact on your Computers or Infrastructure: WhiteHaX is designed to provide an internal cyber and network readiness verification that is performed from inside-the-firewall of the business. This provides the business an opportunity to periodically self-assess its own security infrastructure and controls against some the most common, most recent and dangerous cyber threats, identify potentially exploitable vulnerabilities on computers across the business and help quickly fix them. WhiteHaX verification does not require any install, doesn't impact your network, computers or other infrastructure, doesn't leave any foot-print once it completes nor does it run persistently to consume resources on any of your business assets.

WhiteHaX Comprehensive Cyber and Network Readiness Verifications: The WhiteHaX cloud-hosted platform is a unique, all-automated solution, which from a single platform allows your business to periodically verify your security readiness by evaluating deployed security infrastructure and controls as well as your network-readiness of servers and endpoints. It allows your business to not only run simulated attack and breach scenarios but also inventory control and vulnerability scans at once. This makes a smaller IT team much more efficient in evaluating security threats and provides some of the same level of security verification performed by very large companies using their red-team, blue-team approach without the cost, planning or resource impact.

WhiteHaX keeps you Up-to-speed against latest Cyber Threats: The WhiteHaX attack simulations, breach scenarios and vulnerability checks are adjusted frequently to include the recent cyber threats, enabling your business to verify the security controls against new threats periodically. Thus it provides you the opportunity to self-verify your readiness and helps you keep your infrastructure up-to-date against latest cyber threats.

WhiteHaX Pre and Post-Breach "Betterment" Verifications: The business can best prepare and protect itself by at least performing infrastructure cyber-readiness along with network readiness verification to avoid any potential security breach situation. WhiteHaX is a comprehensive solution to help your business do so. However in case if a breach occurs, it is imperative to make the dual verification a standard practice in your IT security verification process. Post-breach. the dual-verification WhiteHaX "Betterment" service can help the business identify potential weaknesses in the cyber security infrastructure, endpoints and servers and by eliminating them, continuously improve their overall security posture.

For further information on WhiteHaX readiness verification, visit www.WhiteHaX.com or send email to SalesDev@WhiteHaX.com.