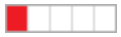
EHR 2.0 partners with industry leading edge continuous compliance monitoring provider, Qualys, Vulnerability Management platform to automate the lifecycle of network auditing and vulnerability management across your global business. Scan reports gives you visibility into your external-facing systems across your network, how they might be vulnerable to the latest Internet threats, and how to protect them. Scan reports by Qualys provides immediate access to your most critical vulnerability information.

Each vulnerability and possible threat is assigned a severity level. The following table describes the five (5) severity levels for vulnerabilities and potential vulnerabilities. Included in this report are a series of bar graphs showing vulnerabilities by severity, operating systems detected, and services detected, as well as detailed host and vulnerability data, sorted by host.

Severity	Level	Description
	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.