netVigilance
assurance has arrived

Network Vulnerability & Risk Assessment.

Structured Test profile for SecureScout™ to ensure HIPAA Security Standards Compliance for Health Information

Meeting regulatory compliance standards concerning the protection of customer information is a daunting and resource-intensive task. The ever-increasing frequency and destructiveness of cyber attacks puts mounting pressure on the CISO to protect vital Patient Health Information and avoid legal action.

Comprehensive reporting to keep all levels of the organization informed on your Information Security posture. From Executive level summaries to detailed remediation procedures; your institution works efficiently and intelligently to demonstrate audit requirements. Visibility to assess the information security posture and performance of individual divisions, offices and branches.

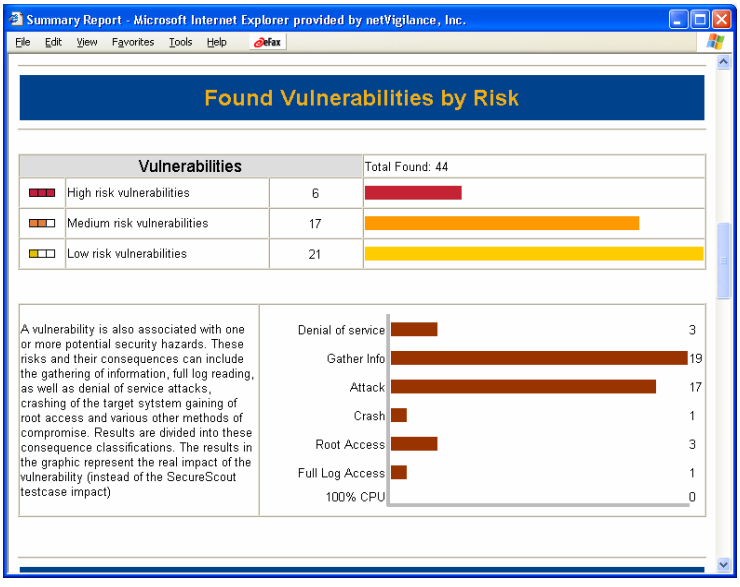
Delivering the highest degree of risk assessment, the most efficient scanning engine; coupled with the revolutionary distributed architecture, HIPAA Safe Scan enables You can demonstrate that you are proactively protecting your digital assets and avoiding a breach of customer information systems.

HIPAA Safe Scan

Risk	Vulnerability Name	Description
	Microsoft SQL Server Weak Authentication Vulnerability	Your Microsoft SQL Server is using an authentication scheme that is using weak encryption.
	First Reported: 2004-01-21 19:21:13	Port: 1433
	NetBIOS Null Session Vulnerability	Outsiders can access information on the target system without authentication.
	First Reported: 2004-01-21 19:21:13	
	Users in the Admin Group Vulnerability	Some users are unexpected members of "Administrators" group.
	First Reported: 2004-01-21 19:21:13	
		+ Extended Info
	SSL Server Allowing Weak Ciphers Vulnerability	An attacker could decrypt your communications.
	First Reported: 2004-01-21 19:21:13	
		+ Extended Info
	Microsoft SQL Server Monitor 0X0A DOS Vulnerability	Your SQL Server could be DOS'd by sending crafted packets to its monitor port.
	First Reported: 2004-01-21 19:21:13	Port: 1433
	ICMP Timestamp Reply Vulnerability	An attacker can flood the local network with undesirable packets.
	Insufficient Password History Length Vulnerability	The value that your security policy specifies on the length of password histories less than 3.
	First Reported: 2004-01-21 19:21:13	
		+ Extended Info

Number of vulnerabilities in 192.168.1.100: 33

Administrator's Report



Vulnerabilities by Risk Report

netVigilance, Inc. • 503.524.5758 • 17937 SW McEwan Rd. Suite 250
Portland, OR 97224

netVigilance
assurance has arrived

- **A Solid Partner for Compliance Audit**

With the best performance, lowest number of false-positives, highest number of found vulnerabilities; the SecureScout scanning engine is the best risk assessment solution available on the market today. Our Security expects have a collective experience base of over 72 years.

- **Strong, Unified front for regulatory compliance**

With over 2000 customers worldwide and growing; You benefit from the collective experiences of thousands of your colleagues around the world. Leverage the experiences of all of these organizations sharing the same concerns for protecting patient health information.

- **Automated updates**

netVigilance security experts continually research information sources for new vulnerabilities, so you can focus on other core tasks and can be confident that you are scanning for the most recently discovered vulnerabilities. Through differential reporting, you can easily benchmark your security level at various points in time and document that flaws have been eliminated.

- **Concurrent test Case Database**

Your SecureScout Vulnerability scanning engine is updated weekly with the latest tests for the most recent vulnerabilities. Our Security Operations Experts vigilantly monitor every emerging threat to ensure that your network is protected from malicious intent.

HIPAA Specific Vulnerabilities

- Root Access
- Execution Arbitrary code
- Directory traversals
- Default / Weak passwords
- File uploading
- Trojans/backdoors
- Possible sniffer (ARP Promiscuous)
- Data reading/alteration/deletion
- Creation of new user accounts
- Escalation of authorized user privileges
- kazaa/Morpheus/Shareaza/Yahoo IM vulnerabilities
- File/Folder/share mounting/viewing
- Outdated Virus Definitions
- Cross-Site Scripting (XSS)
- Hotfixes to Excel, outlook, Internet Explorer, etc
- Web site source code access
- Anonymous FTP and writable FTP
- HTTP Directory listing
- Database test cases