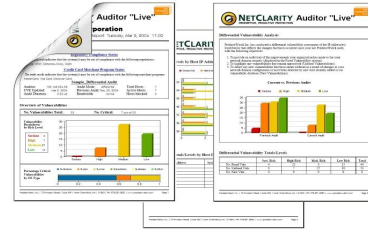




Auditor LIVE™ Services



The Problem: Your network may not be secure

You're vulnerable. Malicious attacks are on the rise and information is leaking from your organization. You don't know where or why it's happening.

Phishing, pharming, and information leaks are widespread concerns for many companies from financial institutions to insurance companies to health care providers and public companies.

Costs to hire a large consulting firm to evaluate your security implementation far outweigh the value of the services. You had nowhere else to turn – *until now!*

NetClarity Solution: External, Security Assessment Services

NetClarity can assist with your security implementation. Try our turnkey, external, Security Assessment Services for Vulnerability Management and Information Disclosure!

We'll show you where and how to harden your external brand, image, and security posture, and we'll help you comply with stringent government regulations.

NetClarity and our Channel Partners are exclusive worldwide providers of this powerful service based on our award-winning **Auditor** Enterprise appliances and proprietary security services.

Typically, a security assessment of this caliber could take up to one month and cost over \$100,000.

NetClarity **Auditor LIVE** Services offer the same assessments for a fraction of the cost and in five business days or less! And, you get a comprehensive, confidential 100-400 page report on your external security and compliance posture.

Isn't it time you had a more comprehensive, holistic view of threats, vulnerabilities, external network access, phishing, pharming, and information disclosure?

What are Auditor LIVE Services?

Auditor LIVE is an External, Security Assessment Service that consists of four components. **Auditor LIVE** helps you reduce risk and keeps your network safe from today's dynamic and evolving security threats. Key features include:

Anti-Phishing & Anti-Pharming Sweep

- Finds "knock-off" web page content as soon as it emerges on the web
- Locates site imitators infringing on corporate identities
- Detects duplicate pages with non-identical addresses and summarizes web page contents
- Tracks suspicious email solicitations and correlates with website sweep data

Website Review

- Tests strength of access controls for internal and external websites
- Places special emphasis on information security for electronic commerce
- Evaluates links, URLs, and transport protocols such as HTTP, SHTTP, and SSL

Network Perimeter Discovery and Information Disclosure Sweep

- Reveals confidential information that may compromise security and integrity of a corporate website or intellectual property
- Includes vulnerabilities revealing inside knowledge potentially allowing an attacker to find and exploit other vulnerabilities

External Vulnerability Assessment

- Evaluates strength of current security defenses from internal and external perspectives
- Conducts a series of non-destructive probes manually
- Focuses on system access and configuration controls, password files, Windows® Registry, and NetWare® bindery information.

Auditor LIVE Components

Anti-Phishing & Anti-Pharming Sweep

The Auditor LIVE Website Anti-Phishing & Anti-Pharming Sweep provides corporate web site monitoring using proprietary site sampling techniques.

Auditor LIVE finds web page content that is a “knock-off” of the monitored corporate site as soon as it emerges on the web. These copycat sites usually originate overseas and are typically involved in various cyber crime activities such as identity or intellectual property theft.

Sweeps detect duplicate pages with non-identical addresses and summarize web page contents for the returned results. Auditor LIVE also tracks suspicious email solicitations and correlates that with web site sweep data.

Auditor LIVE performs a review of Global Top Level Domains (gTLD) and Country Code Top Level Domains (ccTLD), any new registrations, and activations or changes to sites that may have suspicious properties.

This component includes functions that automatically track page changes and updates for the current online status of infringing sites. Auditor LIVE also provides corporate site route checking that maps routes to and from multiple locations throughout the world. This process reveals site misdirection techniques using DNS hijacking or cache poisoning techniques.

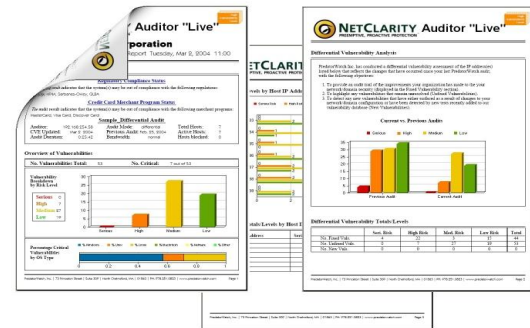
Auditor LIVE reports provide summary and detailed information typically displayed in the following categories. Others may be added or substituted based on findings.

- Duplicate Web site and page detection
- Suspicious eMail content review
- gTLD and ccTLD review with site registration change tracking
- Imitator site online status and site contact information
- DNS & Route analysis from multiple worldwide locations to corporate site(s)
- “Cousin Searches” for mistyped URLs infected with Malware
- Search-engine poisoning including imitator websites infected with Malware
- Recommended actions in the event of positive imitator detection

Website Review

The Auditor LIVE Website Reviews utilize active and passive security tools designed to identify a variety of security vulnerabilities including:

- Improper access control configurations
- Insufficient or non-existent passwords
- Improper system and network integrity
- Operating system & application software updates & patches



Network Perimeter Discovery and Information Disclosure Sweep

This report provides summary and detailed information typically displayed in the following categories. Others may be added or substituted based on sweep results.

- Availability of published web site analysis data
- Links that by-pass protected web pages without login/authentication mechanisms
- Jobs advertised looking for specific skills with technology and tool preferences
- Details on development tools and libraries used to build proprietary applications
- Descriptions of usage problems with development tools and libraries that might show release levels of current technology choices
- Posted system or network configuration data, e.g. ports used, IP addresses, logical network maps
- Descriptions of tools used to manage or monitor systems
- eMail addresses that may be used to find further details about employees and contractors or commit spoofing or masquerading attacks against the website
- Descriptions of techniques in use for security and integrity detection mechanisms

External Vulnerability Assessment

The most critical component in any good security program is the establishment of policies and procedures for use of external systems and network resources. Such guidelines are frequently under construction due to changes in business operations, rules, technology, or other variables in the environment. Unfortunately, the specialist resources required to validate those changes against the policies are seldom available.

For additional information about Auditor LIVE or other offerings, contact NetClarity, Inc.

Phone: 781-276-4555
 email: sales@netclarity.net
 Web: www.netclarity.net