

Vulnerability Assessment Service www.clone-systems.com

Prevention is Better than a Cure

In all likelihood, your enterprise is inspected more often by hackers than by your security staff. As such knowing the vulnerabilities of your enterprise can be a proactive means to safeguard your network. To that end, Clone Systems offers CG-VAS, a managed vulnerability assessment service that entails scanning all web applications, databases, networks, operating systems and other network-resident software to detect threats, assess their risk and devise a remediation plan to quickly mitigate them. It enables IT and security groups to implement a measurable and proactive vulnerability management process that eliminates security weaknesses in your network before the network is penetrated and sensitive information is compromised.

CG-VAS is a managed service, meaning that it is performed on a one-time basis by our expert staff of security engineers.

Clone Guard® CG-VAS Solution

Clone Systems' vulnerability assessment is based on industry best practices we have developed and refined over hundreds of engagements remotely and at client sites. The assessment includes tests for SQL injection, cookie manipulation, access control weaknesses, session state, and cross-site scripting. Upon completion of the assessment, our security engineers review the results with your organization and discuss potential remediation tactics. Full documentation of the assessment is provided in a series of customized reports designated by your company.

Multi-Vendor Support



CG-VAS Features

An economical means to verify your network's security posture for security compliance frameworks (PCI-DSS, ISO 27001, SOX, HIPPA, COBIT).

Validates your enterprise's security for online transaction processing benchmarks.

Achieves the following benefits for your organization:

- **Building and broadening awareness** by directing senior management's attention to IT security.
- **Establishing or evaluating against a baseline** to gauge the improvement or deterioration of an organization's security posture.
- **Identifying vulnerabilities and subsequent responses**, which can help drive the development of a unified risk-management process.
- **Categorizing key assets and driving risk-management practices**, and implementing a consensus hierarchy of assets.
- **Promoting network security action**, for targeting specific and systemic security problems.

