

# External ASSESSMENT

“Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.”

*Source: 2000 Computer Crime and Security Survey*

In many cases companies are trying to create secure systems without understanding what assets they are trying to protect, and the threats, vulnerabilities, and risks to which they are exposed. Although security and business functionality are on opposite ends of the spectrum, you must provide a secure enterprise under which employees can still do their jobs. While companies may already have sound security mechanisms in place, they may still be unknowingly exposed to threats from improper configuration, poor security design, or malicious misuse. Today’s common attacks exploit vulnerabilities inherent in networking protocols and services and operating systems to gain system administrator privileges, access to unauthorized accounts, etc.

SEC’s **External Vulnerability Assessment** measures and analyzes an organization’s susceptibility to outside threats by verifying the integrity of the existing security infrastructure. Our assessment methodology identifies vulnerabilities, advises on their severity, and provides prioritized corrections, allowing you to effectively secure operations in a dynamic environment. This is a technical review from an outsider’s point of view that does not consider physical, personnel, procedural, or legal security issues. SEC’s engineers will:

- Perform scans of all selected network sites, segments, and subnets
- Categorize vulnerabilities by severity
- Research and document the type of action to be taken

- Make additional recommendations regarding global changes to improve overall security
- Provide guidance for implementation.

This approach structures the sometimes large quantities of vulnerability data exposed by this assessment and provides logical recommendations that can be managed and tracked throughout implementation.

SEC’s assessment includes three levels of reporting designed to provide a basis for management decisions as well as facilitate resolution of security vulnerabilities. These levels are summarized below:

- Executive summary – High-level overview of your company’s security posture; non-technical reviewers can easily see and understand test results
- Information gathering report – Information about devices within the test scope, including operating system types and revisions, and applications and services that are running; also includes public information such as Whois and ARIN search results
- Detailed vulnerability report – Description of vulnerabilities grouped by severity, detailed instructions for implementing the fix, and a list of all devices subject to the vulnerability.

A final report will be delivered to key personnel on-site after the data collection process is completed.