Secuguard SSE

Security Vulnerability Assessment! What should you do?

The first step to Information Security is Security Vulnerability Assessment.

Scan and Confirm with SSE!

The Secuguard SSE automatically scans for the system security vulnerabilities and provide remedies for the vulnerabilities found. It is a software solution for the preventing hacking and computer related crimes.

SSE uses an internal agent installed on the target to scan the system for known vulnerabilities and provides the user with remedies and additional information. It allows the system to maintain a high level of security integrity.

SSE generally scans for system password vulnerabilities, internal vulnerabilities, environmental vulnerabilities, file permission errors, etc. and since most of the vulnerabilities are scanned by the target server itself, the vulnerability information is relatively precise.

SSE Characteristics

✓ Common Vulnerability Exposure (CVE) Certificate

- Certificate of Common Vulnerability Exposure (CVE), The Standard for Information Security Vulnerability Names from MITRE

✓ Ease of Use and Installation

- Windows Explorer style user interface
- Detailed online help for installation and usage
- Real-time scan history, progress and result report

✓ Powerful Vulnerability Scanning Capability

- Reduces scan time by sharing information between modules using the Knowledge Base
- Powerful password cracking functions
- Various scan policies such as individual, group, operation system, etc
- Checks vulnerabilities for operating systems as well as user settings
- Integrity checks to find out access and modifications for major files
- Shows the risk level, description, impact, remedy, references, etc. for the found

✓ Ease of Vulnerability Management

- Simultaneous scans for multiple servers on one console
- Shorten scan time due to simultaneous scans

✓ Detailed Vulnerability Information

- Various vulnerability information provided by a assessment tool experts
- Vulnerability information sorted by group, operating system, risk level, etc

✓ Supports Most Operation Systems

- Most UNIX operating systems. Ex) Unixware, Solaris, AIX, HP-UX, Tru64, Linux, etc
- Supports Windows Server 2003, 2008, 2012, 2016

✓ Encryption of Communication and Result Data

- Encryption of communication messages between the console and server
- Only valid consoles and users can access scan results

✓ Online and Offline Update

- Updates scan modules, console module and vul-info db via the update server and internet
- Provides offline update option for users without internet access

✓ Various Result Reports

- More than 14 vulnerability reports sorted by group, risk level, etc.
- Various reports with various graphs and tables.
- Export reports to HTML, Word, Excel, PDF, RTF, Text, etc. formats

✓ Various Additional Features

- Scheduled scans allows automated scans and automatically sends email to each server administrator
- Real-time monitoring for agent live status
- Support scan modules and vul-infos of new vulnerabilities continuously
- Support infomation links of vulnerabilities
- Support scan for applying patch
- Support function to integrate with ESM
- Manage agents by group
- Ignore scanned vulnerabilities for report by user-setting

✓ Easy installation and Expansion

- Easy installation using Shell Script (UNIX) and InstallShield (Windows)
- Supports multiple consoles for load balancing

Benefit of Secuguard SSE

Preventing Security Incidents

Periodic vulnerability assessment for running system can prevent unexpected security incidents.

Vulnerability Assessment

Analyzing current system's security state. Promoting secure system operation based on analyzed security state.

Disaster Recovery Plan

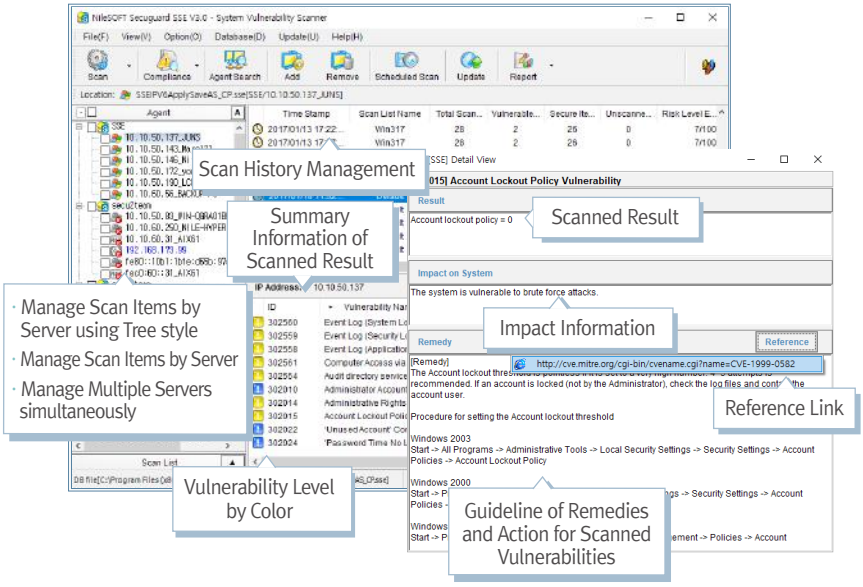
Periodic, daily security vulnerary assessment and action can minimize the damages from system's unexpected disorder and obstacles.

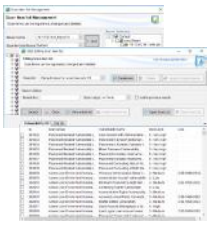
Security improvement

Deep understanding of system with provided various security vulnerability assessment. This can be adapted by Operation policy. It can be used and help increasing higher security system.

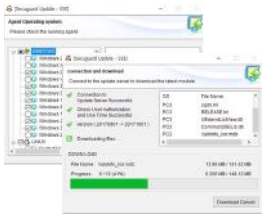
SSE Screen Shots and Features

▲ Screen of Scanning Process





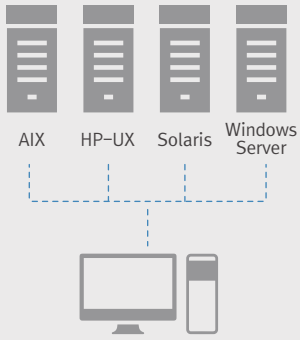
▲ Edit Scan Items



▲ Online and Offline Update

▲ Scheduled scans and Scan by Category or Item

SSE Architecture and Scan Category



SSE Architecture

Host based Vunerability Assessment Tool Process

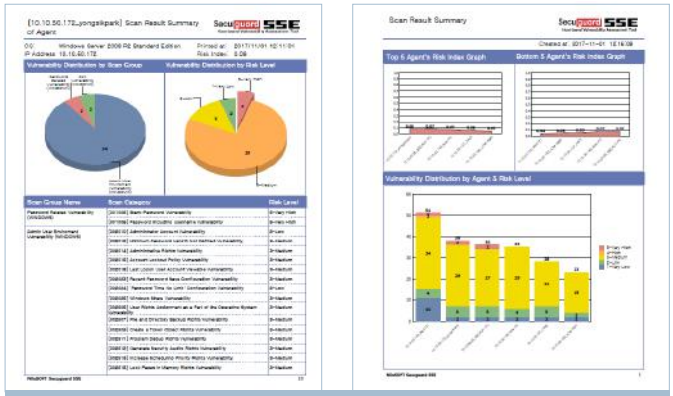
Security Vulnerability Scan Category (UNIX/Linux)

- Password Related Vulnerability
- X Windows Related Vulnerability
- Administrator and User Environment Vulnerability
- Utility Vulnerability
- File System Vulnerability
- DB Vulnerability
- Daemon Vulnerability
- Special File Vulnerability
- FTP Vulnerability
- SMTP and Mail Related Vulnerability
- RPC Vulnerability
- WWW/HTTP and CGI Vulnerability
- DNS/BIND Related Vulnerability
- Remote Access Command Vulnerability
- Packet Related Vulnerability
- Network Related Command Vulnerability
- NIS/NIS+ Vulnerability
- Firewalls/Filters/Proxies Vulnerability
- Port Vulnerability
- Backdoors Vulnerability

Security Vulnerability Scan Category(Windows)

- Password Related Vulnerability
- Administrator and User Environment Vulnerability
- File System Vulnerability
- DB Vulnerability
- Special File Vulnerability
- Server Services Vulnerability
- Other Server Service Vulnerability
- Application Vulnerability
- Other Application Vulnerability
- Exchange server Vulnerability
- Registry Vulnerability
- WWW/HTTP and CGI Vulnerability
- Packet Related Vulnerability
- Firewalls/Filters/Proxies Vulnerability
- Port Vulnerability
- Internet Explorer Vulnerability
- Internet Information Server Vulnerability
- SMTP and Mail Related Vulnerability
- Backdoors Vulnerability

SSE Various Reports



▲ Summary Report

▲ Detailed Report

NileSOFT
Kolon Digital Tower Billant 10th Fl. #1004, 30, Digital-ro 32-gil, Guro-gu, Seoul, 08390, South Korea
TEL. +82-2-783-0961 FAX. +82-2-783-0963 e-mail. nileman@nilesoft.co.kr
www.nilesoft.co.kr/eng