Security Vulnerability Analysis! What will you use?

The first step to security!

Check with Secuguard SSE V7.0!

The system vulnerability assessment tool SSE, developed with domestic technology, automatically diagnoses various security vulnerabilities in computer systems, provides solutions for detected issues, and is a security software solution that protects and prevents hacking and computer crimes.

Detailed Features of SSE

Convenient User Interface

Intuitive user interface

SSE Manager provides a user interface in the form of a typical internet service, making it easy for anyone who has experienced general internet services to operate.

Easily accessible inspection history, progress, and inspection results screens, as well as reports

SSE stores inspection results in a database. Users can always check previous security vulnerability assessment results. Additionally, through reports, users can examine changes in agent security status from various perspectives.

Various Additional Features Provided

- Scheduled inspection function
- Real-time monitoring of agent operational status
- Continuous provision of the latest inspection modules by operating an in-house security team
- Vulnerability information link function
- Function to check the application of patches on servers
- Group-based agent management function
- Diagnostic resource usage limitation and notification support for agents
- Function to register the person in charge and detailed attributes for each asset
- Function to designate a person responsible for each identified vulnerability
- Personalized layout setting function for each user
- Support for various color skins and themes
- Responsive web UI feature

Fast and robust security vulnerability assessment.

Various inspection methods such as batch inspection, inspection by agent, and inspection by item.

Before initiating inspections on registered agents, SSE enables users to choose from various inspection methods.
It allows for either batch inspection of all inspection items across all agents or selective inspection of only specific agents.

Utilization of Scheduled Inspections and Inspection Results:

Users can utilize scheduled inspections to automatically perform periodic inspections.

Presentation of discovered security vulnerabilities, including risk level, content, impact, and mitigation measures.

Detailed information about security vulnerabilities discovered by SSE can be reviewed through the manager and reports. Detailed descriptions of security vulnerabilities, their risk levels, impacts on the system, and mitigation measures are presented according to recommended practices in compliance.

Other Key Features and Characteristics:

Encryption of Communications and Inspection Results:

The details of security vulnerabilities detected by agents are encrypted before being transmitted to the SSE Manager. This ensures that even if packets are intercepted on the network, the content of the security vulnerabilities remains unreadable, and the inspection results are encrypted. The system information collected for vulnerability assessments is encrypted and securely managed.

Expected Effects of SSE

Prevention of Security Incidents

By analyzing the security vulnerabilities of operational key information systems, it is possible to conduct activities aimed at preventing incidents.

Improvement in Security Level

Numerous security vulnerabilities can be understood through vulnerability analysis tools, and by incorporating these insights into management policies, an improvement in security levels can be expected.

Security Level Assessment Tool

Allows for the assessment of the current security status of information systems, supporting the safe operation of these systems based on this knowledge.

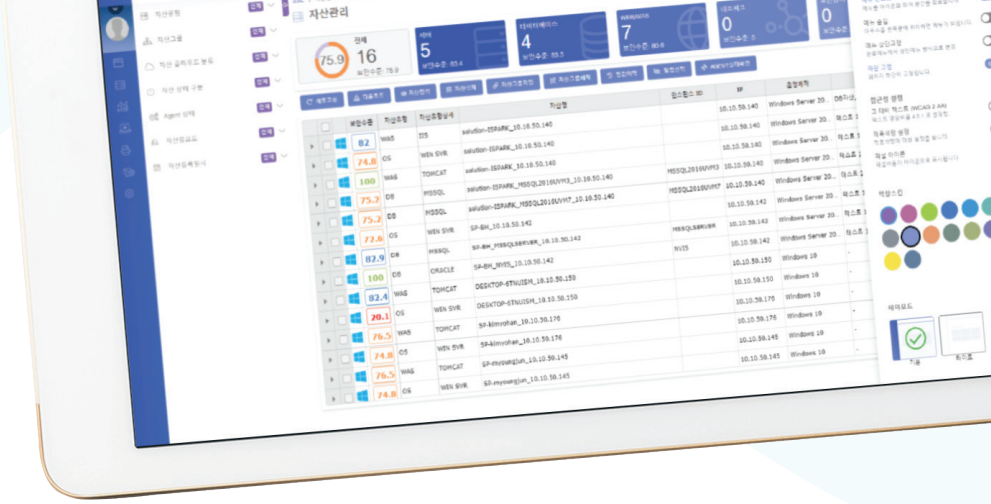
Disaster (Safety) Measures

The analysis and remediation of security vulnerabilities can help minimize damage in the event of failures in intrusion detection and intrusion prevention systems.

Secuguard SSE V7.0

GS Certification Achieved:
Achieved Level 1 rating

First in the country to obtain the CVE
(Common Vulnerability Exposure)
certification mark



Key Features of SSE

Compliance with Various Domestic and International Standards

- ✓ Targets major information and communication infrastructures, Ministry of Trade, Industry and Energy, Financial Security Institute, etc.
- ✓ Diagnosis of CVE (Common Vulnerabilities and Exposures) Items

Support for Various Diagnostic Methods

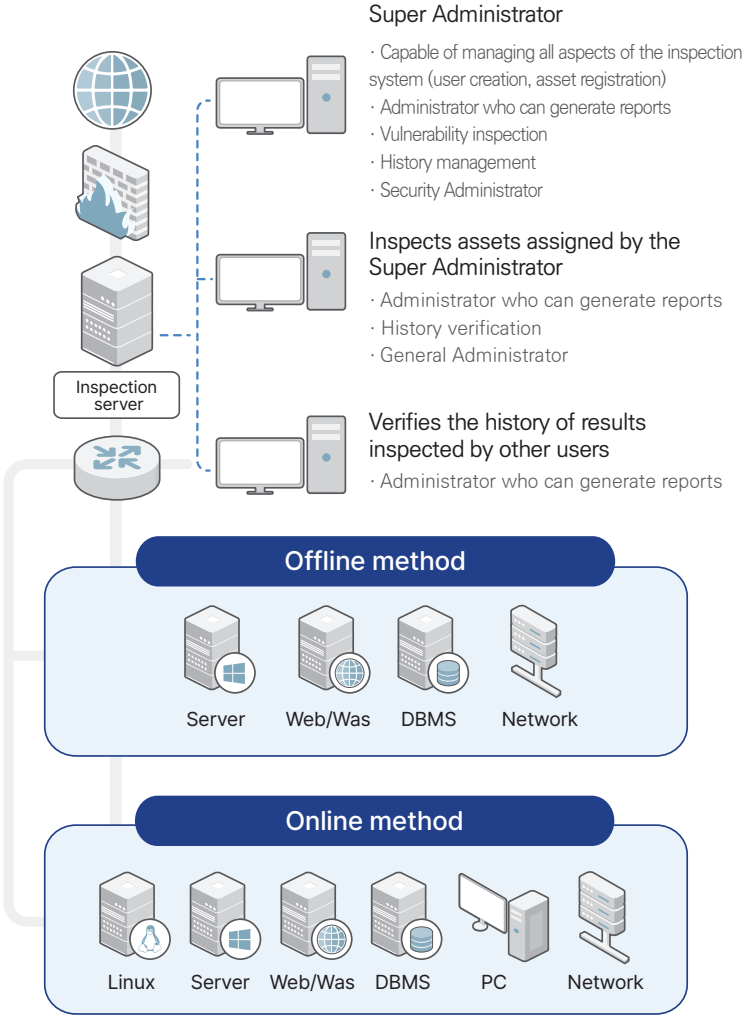
- ✓ Multiple Diagnostic Approaches: Provides options for agent-based, agentless, and manual inspections.
- ✓ Support for Closed Networks: Offers manual script methods for environments without network connectivity.
- ✓ Customizable Inspections: Adaptable to fit the operational environments of the target systems, ensuring that checks are thorough and appropriate.

Support for various features

- ✓ Vulnerability Assessment Planning and Scheduling: Enables users to organize and schedule vulnerability scans effectively.
- ✓ Comprehensive Coverage: Checks vulnerabilities across operating systems, databases, web servers/application servers, and network equipment.
- ✓ Vulnerability Remediation and Compliance Tracking: Facilitates the tracking and implementation of remediation actions for identified vulnerabilities.
- ✓ Secure Data Management: Encrypts and securely stores data collected by agents.
- ✓ Compli ance and Vulnerability History Management: Maintains a detailed history of compliance-related vulnerability findings and checks.

Supports various diagnostic methods

- ✓ Operating Systems, Database Management Systems (DBMS), WEB/WAS, Networks, etc. (Refer to the table)



Platforms capable of supporting SSE

OS	UNIX(LINUX), WIN SVR, WIN PC
DB	ORACLE, MSSQL, MYSQL, SYBASE, DB2, ALTIBASE, POSTGRES, TIBERO, SYBASEIQ, MARIADB, INFORMIX, CUBRID
WAS	APACHE, WEBTOB, JEUS, TOMCAT, WEBLOGIC, WEBSPHERE, ORACLE HTTP SERVER, JBOSS, IPLANET, JBOSS2, NGINX, IIS, SUNONE, IBM HTTP SERVER, JRUN, LENA, JETTY, Resin
NETWORK	CISCO, JUNIPER, ALTEON, F5, A10, AVAYA, BROCADE, EXTREME, UBIQUOSS, PUMPKIN, HPE, 3COM, ALCATEL_TIMOS, DASAN, PIOLINK, ALCATEL_OMNISWITCH, HanDreamNet, Enterasys, NetGear, Array, Citrix, ALCATEL_OMNISTACK, HP_Provision, Vyatta, SAN, NETKTI
SECURITY	FORTIGATE, NETSCREEN, SECUI, XGATE, NEXG
ETC	RHEV, XENSERVER, VSPHEREESXI, PowerVM, HPUXVM

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
Popularization of Information Security! NileSOFT will go together.