H www.lsware.com B blog.lsware.co.kr

Integrated Vulnerability Management Portal System

Omni-VM

Integration of Technical, Physical, and Administrative Vulnerability Management!!

Unified Management Process

Omni-VM is an integrated vulnerability management portal system that establishes the vulnerability management work process through a single interface by linking various vulnerabilitydiagnosis solutions and provides the security status with high visibility by calculating the security indices.

Overview

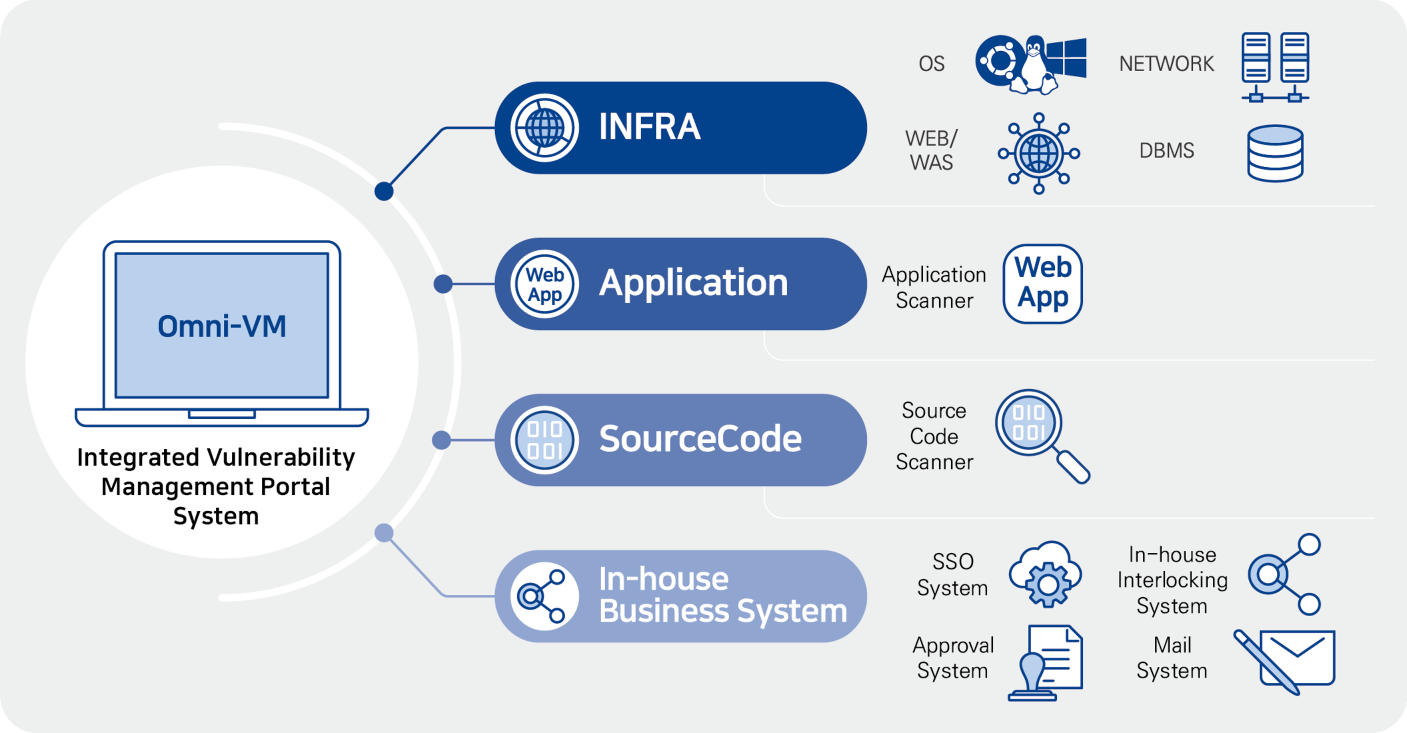
Change in Financial Security Regulation Paradigm from Heteronomous Regulation to Principle-centered Autonomous Regulation

- Enhancing the self-inspections/checks and responsibilities, and promoting the IT security competency improvement
- Establishing a private autonomous security review system and strengthening the regular monitoring system for financial security risks

Increased Need for Efficient Integrated Vulnerability Management

- Increase of management points for various diagnostic tools
- Increase of requirements for the quantitative expression with visibility on the company-wide vulnerability status
- Difficulty in calculating the security index by asset and importance for the diagnosis result
- Integrated vulnerability status screen/display required

Scope of Interlocking by Omni-VM



Key Features of Omni-VM

Integrated Vulnerability Management

- Interlocking various vulnerability diagnosis solutions
- Linking with the asset system
- Registering and managing administrative/ physical vulnerabilities and consulting details
- Providing vulnerability check results in a single interface

Vulnerability Diagnosis

- Automatic diagnosis of various diagnostic solutions through the web portal
- Handling exceptions by setting a specific reason and period
- Alarming for delayed/missing tasks
- Managing vulnerability diagnosis results and implementation details

Establishment of Vulnerability Management Process

- Providing a process covering from the phase of vulnerability check to the phase of action implementation
- Establishing the management system for various compliances
- Defining the role for each vulnerability management business process
- Supporting the vulnerability management for each project (security review)

Provision of Security Vulnerability Status

- Providing company-wide security indices based on diagnosis results
- Providing vulnerability reports of individual diagnostic tools
- Providing the status of vulnerability diagnosis results in charts and various formats
- Providing statistical data for each major situation

Advantages of Omni-VM

User Aspect

- Improving security work productivity by minimizing repetitive manual tasks
- The establishment of the inspection and action processes clarifies the roles and responsibilities of the security and system operators
- Providing UI for each user role and authority (privilege) through the web

Admin Aspect

- Establishing a unified security vulnerability management work process suitable for the nature of the organization
- Reducing the management points by integrating various systems
- Minimizing the delays and omissions through periodic notifications/reminders

Functional Aspect

- Performing inspections and checking the results centrally without the scanner access
- Establishing the management system linked to the in-house business system (Mail, SSO, approval , etc.)
- Managing the history of diagnosis execution, results, and action implementation

Mapping for Core Elements, Laws, and Guidelines

Core Elements	Key Certification Guidelines
Electronic Financial Transactions Act	• Article 21-3(Analyzing and Assessing Vulnerability of Electronic Financial Infrastructure) ①To ensure the security and reliability of electronic financial transactions, a financial company and an electronic financial business entity shall analyze and assess the following matters with respect to its or his/her electronic financial infrastructure and report the findings therefrom to the Financial Services Commission. 21-4 ② A financial company and an electronic financial business entity shall establish and implement a plan to take necessary complementary measures based on the findings from analysis and assessment of vulnerability in the electronic financial infrastructure under paragraph (1).
Comprehensive Measures to Reinforce Financial Institution's Data Security	• The vulnerability checks and complementary measures shall be thoroughly implemented under the responsibility of the CEO. • A system shall be established to ensure that complementary measures against vulnerabilities are thoroughly implemented, such as preparing implementation procedures corresponding to the findings of the vulnerability checks • The vulnerability checks and security control shall be expanded to the extent of non-financial computer systems • The security checks on internal business support systems, such as the website for education and PR, and the groupware, other than electronic financial infrastructure, shall be mandatory.
Protection Guidelines on Critical Information and Communications Infrastructure	• Article 13 (Analysis and Evaluation of Vulnerabilities) ① In accordance with Article 9 of the Act, when the head of the management organization has conducted the first vulnerability analysis and evaluation on the critical information and communications infrastructure under his/her jurisdiction he/she shall analyze and evaluate the vulnerabilities of critical information and communications infrastructure each year. ③ The head of the management organization shall establish and implement the plans necessary for the specific implementation of the vulnerability analysis and evaluation, such as the target, period, procedure, method, and budget formation and execution of vulnerability analysis and evaluation, in consideration of the criteria for the analysis and evaluation of vulnerabilities under Article 9 (4) of the Act.
Information Security Management System (ISMS)	• The certification system for the comprehensive management system, such as technical and physical protection measures established and operated to ensure the security of information and communications networks • Article 18-11 (Operational Security) In order to check whether the information system is exposed to known vulnerabilities, technical vulnerability checks shall be carried out regularly, and actions shall be taken against the identified vulnerabilities.

※ Relevant laws and regulations

Financial Services Commission "Electronic Financial Transactions Act", "Comprehensive Measures to Reinforce Financial Institution's Data Security"
Ministry of Science and ICT (Former Ministry of Science, ICT and Future Planning) "Protection Guidelines on Critical Information and Communications Infrastructure," "Notification on Information Security Management System Certification, etc."