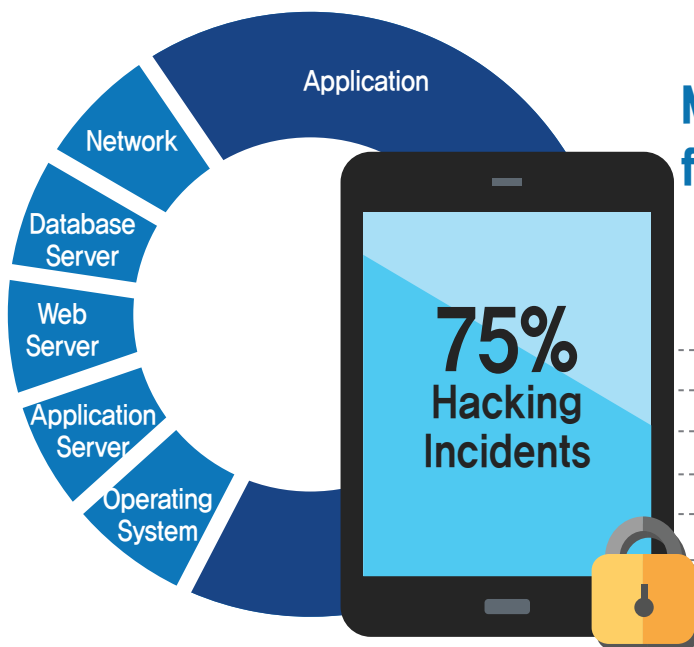# CodePolice

Static Code Analysis solution to eliminate security vulnerabilities and develop secure software

CodePolice is the most convenient solution for developers, which detects security weaknesses through code analysis and eliminates the detected weaknesses automatically.

Most security incidents occur from Application SW

75%
Hacking Incidents

- Application
- Network
- Database Server
- Web Server
- Application Server
- Operating System

- Injection
- Broken Authentication
- Cross Site Scripting
- Security Misconfiguration
- Sensitive Data Exposure
- Error Handling

Key Features

Active Code Assistant(ACA)
- Remove existing security weaknesses in the source codes with only one–click

Active Incremental Scan(AIS)
- Selectively analyze only affected parts by modified source codes, providing rapidly decreased detection time
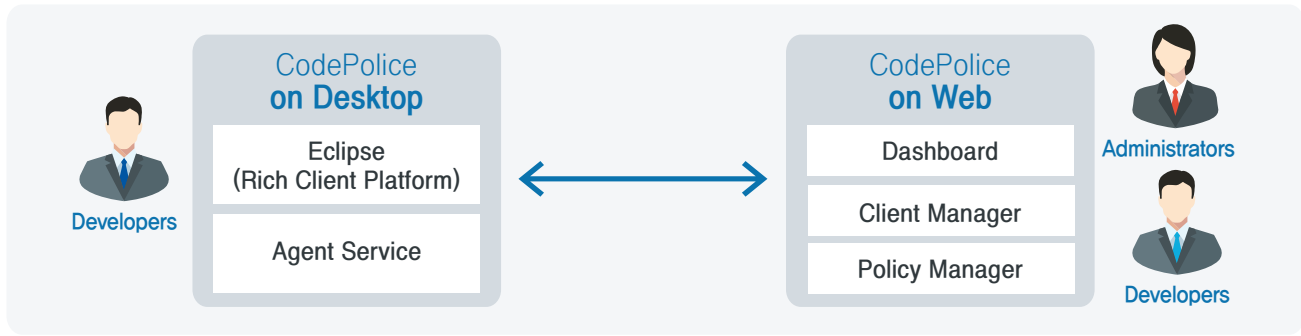
Active Pattern Search(APS)
- Analyze pattern of security weaknesses and manage grouping

Active Flow Trace(AFT)
- Provide detailed tracing information of security weaknesses from cause to result for fast analyzing environment

PHP
JAVA
XML
C++
CSS
CMS
</CODE>

Configuration

CodePolice on Desktop

- Eclipse (Rich Client Platform)
- Agent Service

Developers

CodePolice on Web

- Dashboard
- Client Manager
- Policy Manager

Administrators

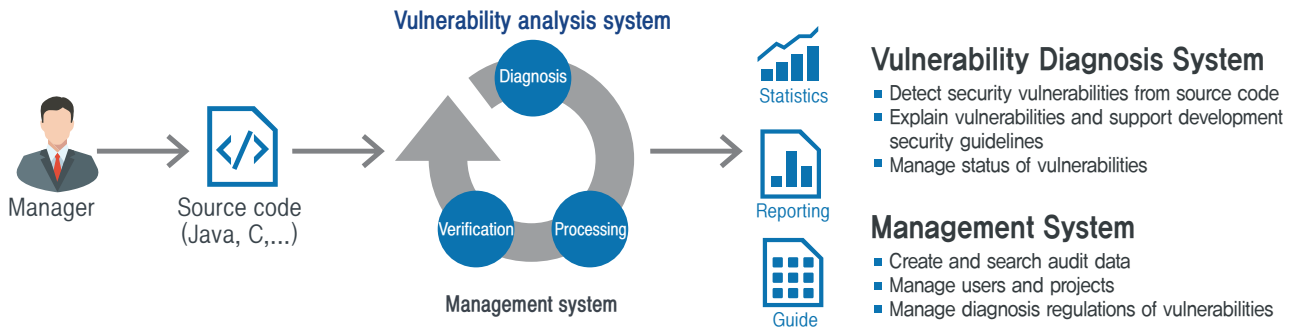**Developers**

A system for developers
- Detection of existing security weaknesses in the source codes
- Elimination of detected security weaknesses

A system for administrators
- Dashboard for collaborative works
- Diverse statistics and reports
- Centralized policy management
- Integrated server inspections

System Architecture

Manager → Source code (Java, C,...) →

Vulnerability analysis system
- Diagnosis
- Verification
- Processing

Management system

Statistics

Reporting

Guide

Vulnerability Diagnosis System
- Detect security vulnerabilities from source code
- Explain vulnerabilities and support development security guidelines
- Manage status of vulnerabilities

Management System
- Create and search audit data
- Manage users and projects
- Manage diagnosis regulations of vulnerabilities

Specifications

	CodePolice on Desktop(Plug-in)	CodePolice on Web
Supported languages	JAVA, JSP	JAVA, JSP, C, C++, Android JAVA, Objective-C, PHP, ABAP(SAP), ASP.Net, C#
Report formats	PDF, Word, Excel, RTF (Hancom Office and MS Office supported)	PDF, Word, Excel, RTF (Hancom Office and MS Office supported)
OS	Windows7(32Bit, 64Bit) or later (Windows10 – 64Bit or later recommended)	Windows, Linux, Unix (Server OS supporting JAVA 1.7)
CPU	Min. x86 2.4GHz dual-core (3.0GHz quad-core or higher recommended)	Min. x86 2.4GHz dual-core (3.0GHz quad-core or higher recommended)
Memory	Min. 4GB (8GB or above recommended)	Min. 8GB (16GB or above recommended)
HDD	Min. 250GB (SSD – 250GB or above recommended)	Min. 500GB (SSD – 500GB or above recommended)