미래창조과학부

Open Technet Summit 2017

오픈소스 보안 전략

숭실대학교 정보과학대학원 박재표

2017. 06. 21

nipa 정보통신산업진흥원 National IT Industry Promotion Agency

KOSSA 한국정보소프트웨어협회 Korea Open Source Software Association

디지털데일리

숭실대학교 Soongsil University

01 오픈소스 SW 시장 현황

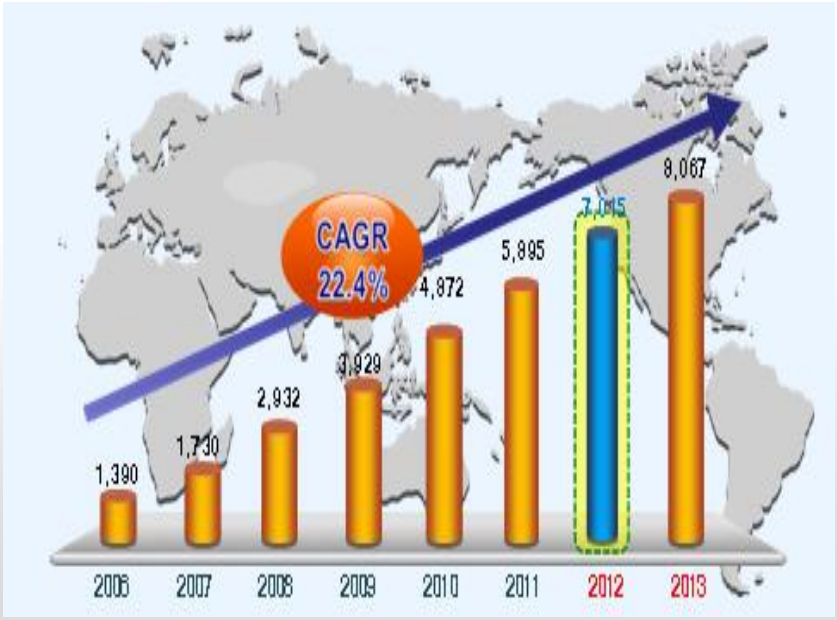
오픈 소스(Open Source)란?

소스코드를 공개하여 자유롭게 수정, 재 배포할 수 있는 자유로운 SW를 말함. 단, **저작권자에 의한 라이선스** 규정을 준수해야 하며, 공개 SW의 "Open"은 공짜가 아닌 소스코드 및 SW의 자유로운 사용을 의미

오픈소스 시장 규모

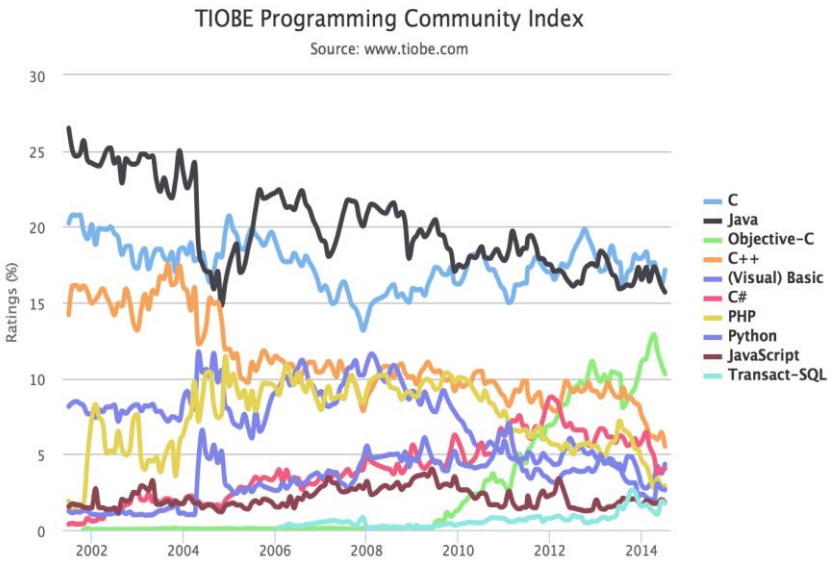
- 전세계 오픈소스 시장은 연평균 22.4%의 성장

(비공개 상용SW 시장은 연평균 7.6% 성장)



오픈소스 Language 사용 현황

- 공개 SW 시장에서는 C와 Java의 활용도가 가장 높은 추세임. 하지만 Python, QT의 성장세도 점진적으로 높아질 것으로 예상됨

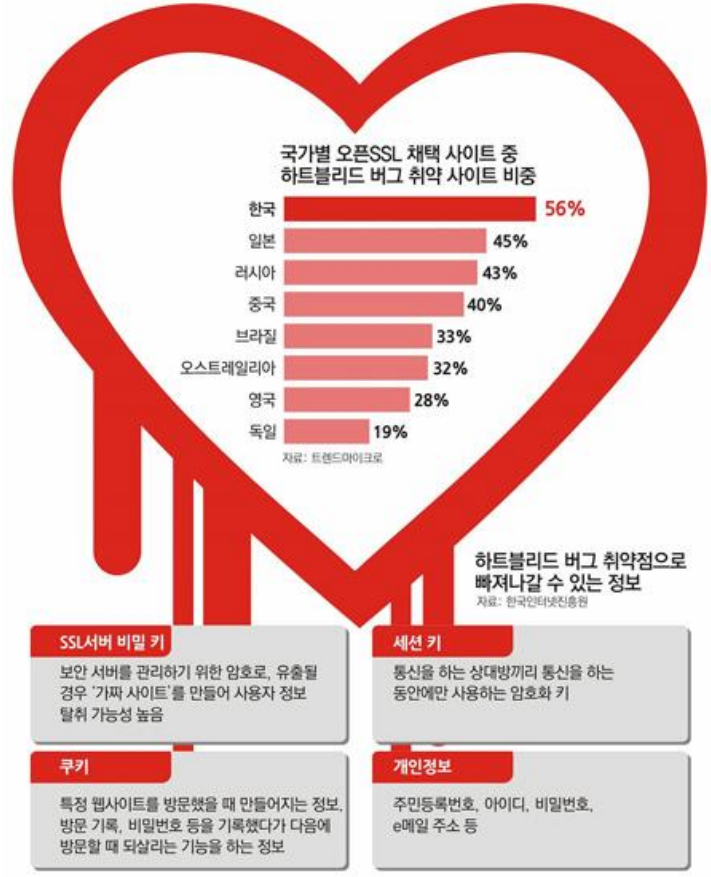


02 오픈소스 SW 취약점 분석의 필요성

대표적인 오픈소스 SW 공격 사례 (OpenSSL)

2014년도에 발견된 하트블리드는 오픈SSL의 핵심 프로토콜인 '하트비트(Heart beat)'에 영향을 미치기 때문에 붙여진 이름으로 해커들이 이 버그를 활용하면 오픈SSL을 설치한 웹 서버의 메모리에 침투해 모든 개인 정보를 탈취해 갈 수 있음

오픈소스 SW 소스코드의 취약점 분석 필요성



03 오픈소스 SW 취약점 분석의 필요성

HIDING IN PLAIN SIGHT: THE RELATIONSHIP BETWEEN APPLICATIONS AND CYBER THREATS

paloalto networks.

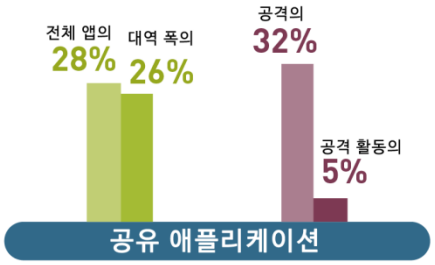
GLOBAL SUMMARY: **5,551** networks analyzed | **2,015** applications detected | **51.1** petabytes observed | **16,809** threats logged

Application Usage & Threat Report
11th Edition, June 2014
Download a copy at:
www.paloaltonetworks.com/autr

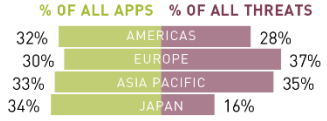
Social media, IM, email, video, file sharing

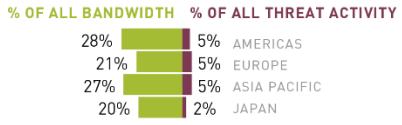
High in threat delivery, low in outbound threat activity

애플리케이션 vs. 사이버 공격



REGIONAL BREAKDOWN

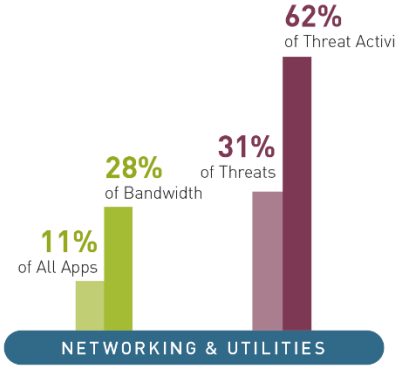




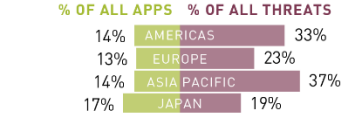
<< 공개 SW 보안 위협 노출 현황 >>

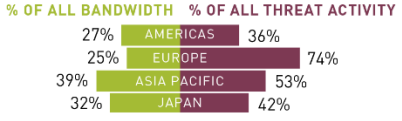
Networking and web utilities

High in outbound malware activity



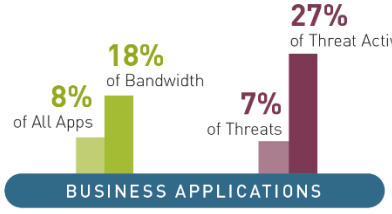
REGIONAL BREAKDOWN



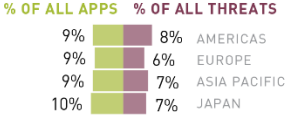


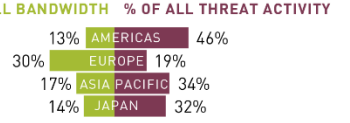
Business applications

Heavily targeted by brute force exploits



REGIONAL BREAKDOWN





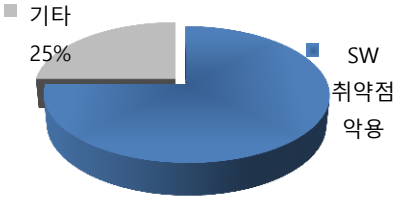
04 오픈소스 SW 취약점 분석의 필요성

시큐어 코딩(Secure Coding)이란?

소프트웨어의 개발과정에서 개발자의 지식부족이나 실수, 또는 각 프로그래밍 언어의 고유한 약점 등 다양한 원인으로 발생할 수 있는 취약점을 최소화 하기 위하여, 설계 단계부터 보안을 고려하여 코드를 작성하는 방식 권장

오픈소스 SW 소스코드의 취약점 분석 필요성

오픈 소스 S/W 취약점을 이용한 공격 증가



- ✓ 전 세계 사이버 공격 하루 평균 38만 건 발생 - IBM
- ✓ **사이버 공격의 75%가 SW 자체의 보안 취약점을 악용하는 공격**

시큐어코딩 법제화

- ✓ 사이버침해대응지 원센터 신설
- ✓ SW 진단 시범 사업 시작
- ✓ 20억 이상 규모의 공공정보화 사업
- ✓ 사업장 전체에 대해 시큐어코딩 의무화

2010 2012 2014 2015

- ✓ 소프트웨어 개발 보안에 관한 다양한 법률 제정
- ✓ 소프트웨어 개발 보안 (시큐어코딩) 관련 가이드라인 도출
- ✓ **정보화사업 전 분야에 걸쳐 의무화**

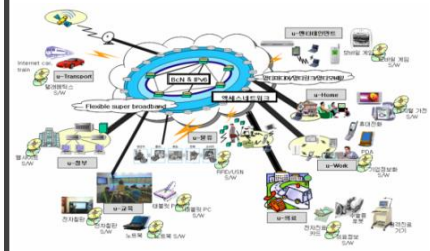
S/W 유지비용 감소

구분	에러 검출 영역				
	설계단계	코딩단계	통합단계	베타제품	제품출시
설계과정	1배	5배	10배	15배	30배
코딩과정	-	1배	10배	20배	30배
통합과정	-	-	1배	10배	20배

<소프트웨어 개발단계별 결함수정 비용 분석>

- ✓ 소프트웨어 개발 단계에서 보안 취약점을 제거하는 것이 가장 효과적
- ✓ 보안취약점을 유지 보수하는 것에 시간과 비용 등 많은 어려움이 발생
- ✓ **시큐어코딩 적용 시 약 25배 이상의 비용 절감 효과**

공개 S/W 이용범위 증가



- ✓ 다양한 분야(컴퓨터, 스마트단말, 기차, 자동차, 디지털 가전기기, 의료기기 등)에서 소프트웨어를 이용
- ✓ SW 개발 환경에서도 Redmine등 다양한 오픈소스SW를 활용하고 있음

2014. 09. 16

오픈소스 소프트웨어의 안전성 점검이 가능한 보안 취약점 분석 기술과 발견된 취약점에 대한 자동 패치가 가능한 소프트웨어 취약점 분석 플랫폼 개발

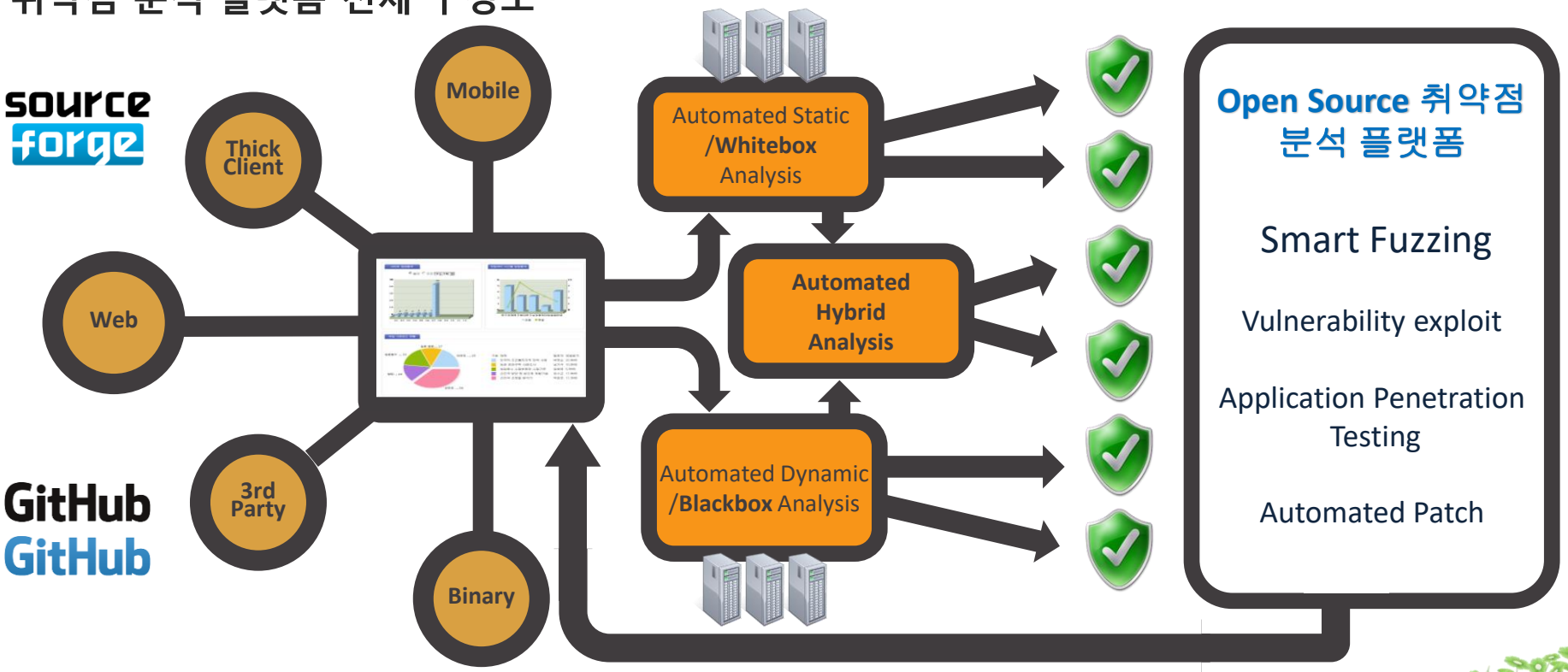
ENKISOFT Evenstar 숭실대학교 Soongsil University

05 오픈소스 SW 취약점 분석 플랫폼 개요

취약점 분석(Vulnerability)이란?

보안 취약점은 해킹 등 외부 공격으로 시스템의 보안 정책을 침해하여 보안 사고의 실제 원인이 되는 시스템 상의 보안 허점과 프로그램의 품질을 저하시키는 품질 취약점을 포함하며, 이는 외부 공격자가 정보를 악용하도록 함.

취약점 분석 플랫폼 전체 구성도

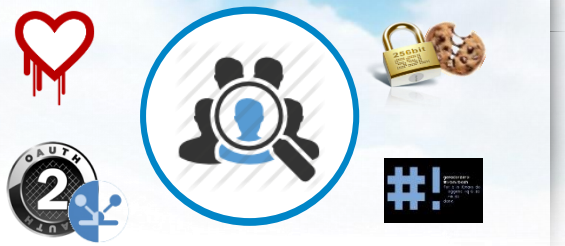


06 오픈소스 SW 취약점 분석 플랫폼

취약점 분석 플랫폼 전체 구성도

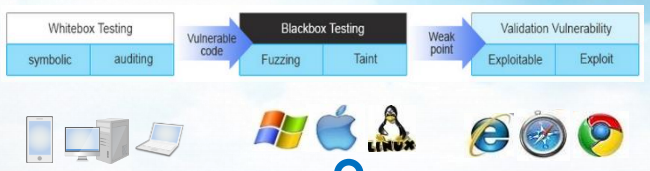
1. 오픈소스 수집 기술

위험성을 기준으로 오픈소스 소프트웨어 자동 수집 및 대상 예측



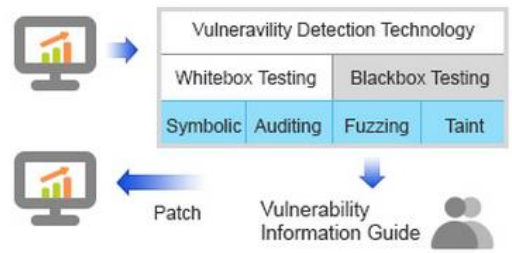
2. 취약점 탐지 기술

정적·동적·자동 검증을 통한 스마트 탐지 원천 기술의 확보

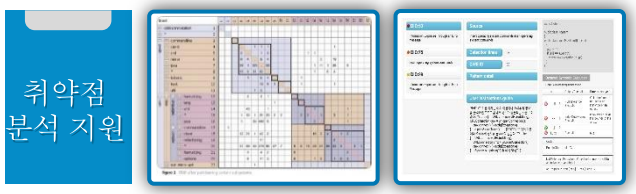


3. 취약점 패치 기술

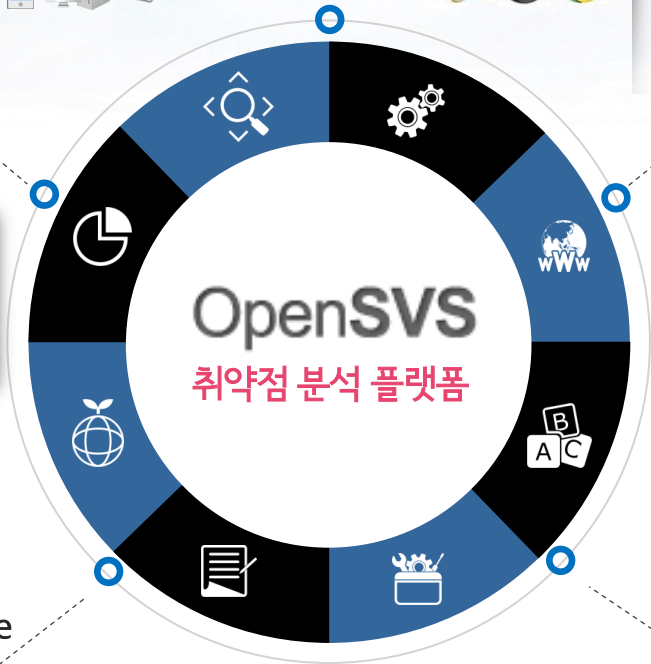
취약점 분석 업무의 효율화를 위한 자동 패치 가이드라인 및 리포팅 기술



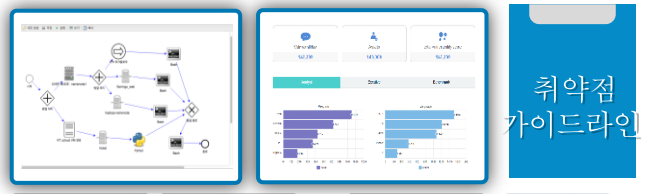
전문가 Analysis Service



전문가 Collaboration Service



Automatic Exploit Generation

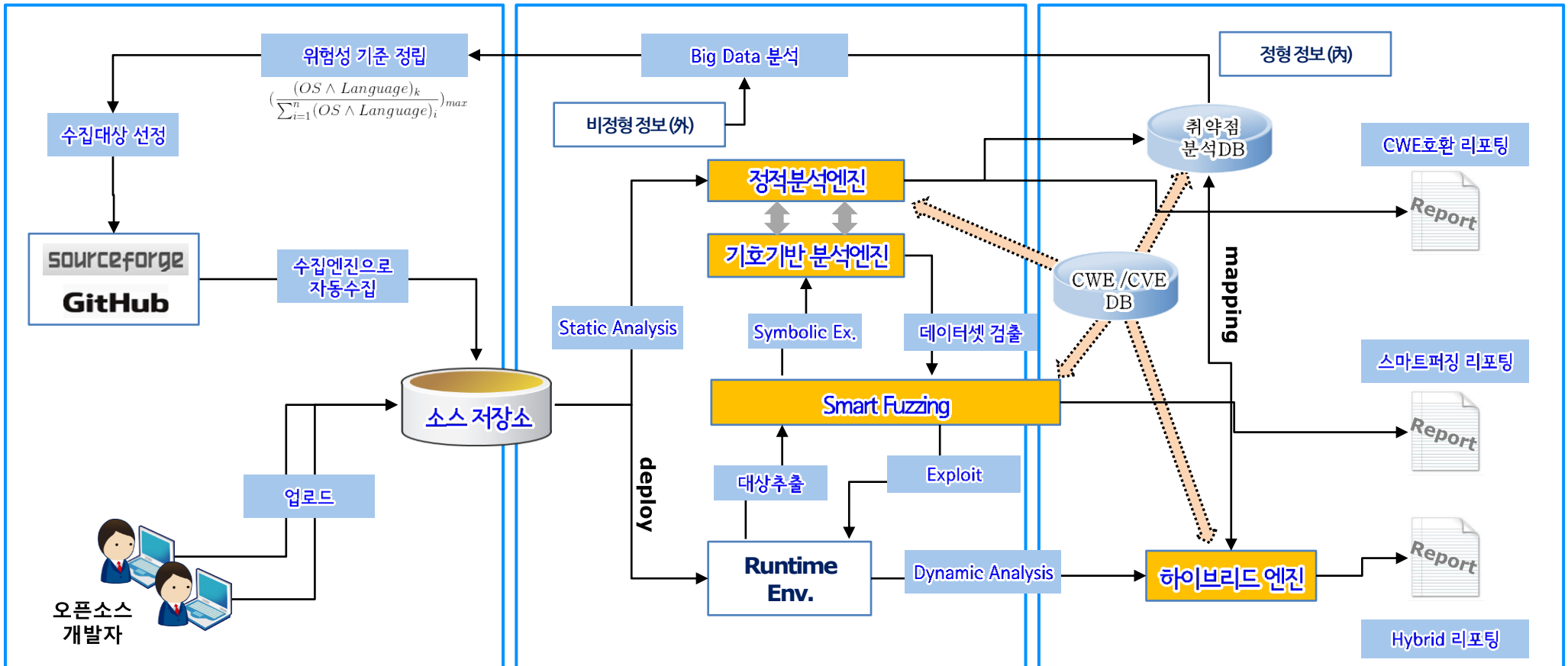


취약점 Scoring Service

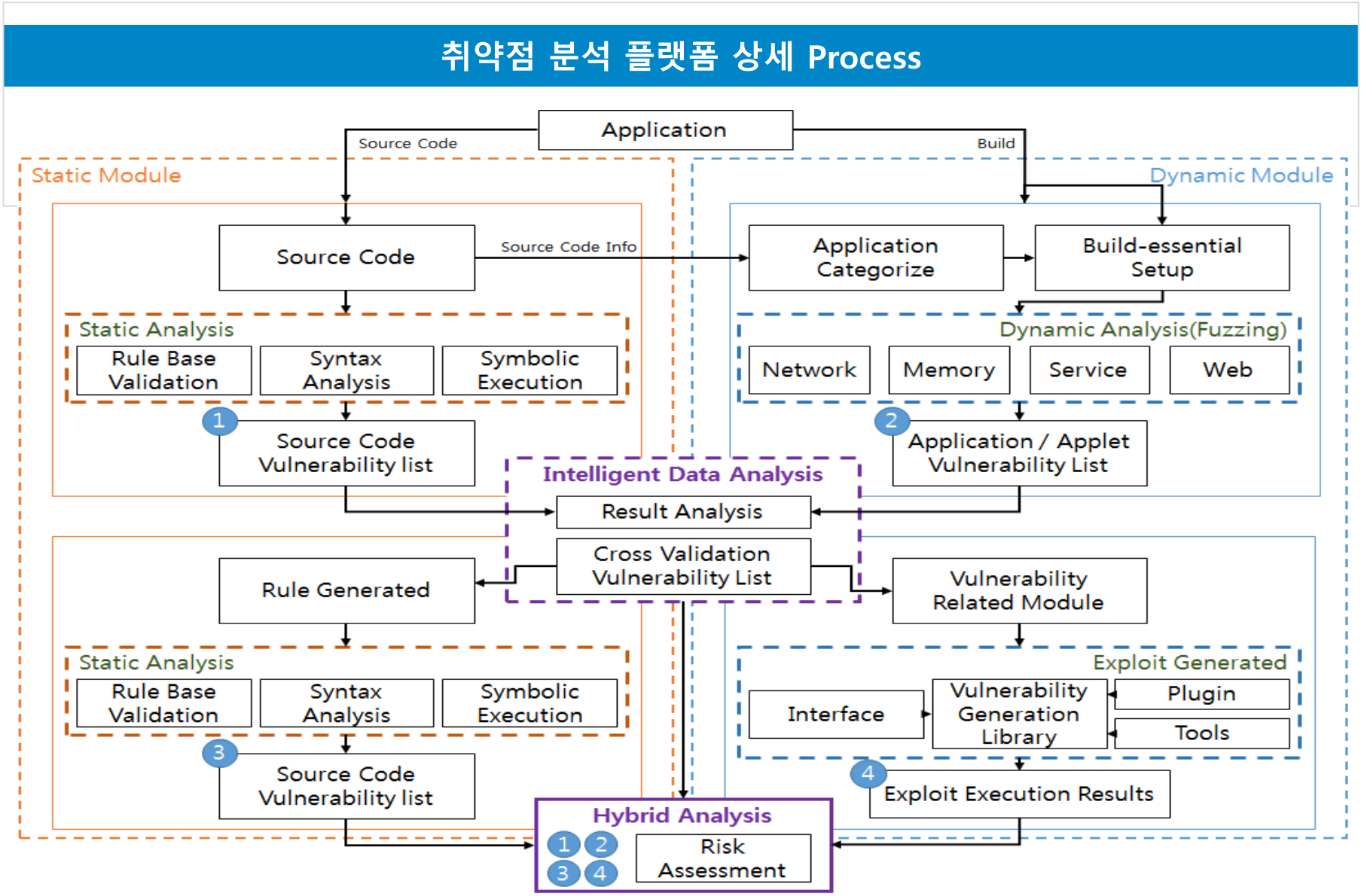
07 오픈소스 SW 취약점 분석 플랫폼 메가 프로세스

취약점 분석 플랫폼 Processing Cycle

오픈소스 수집 단계	취약점 탐지 단계	취약점 패치 제공 단계
Big Data기반 위험성 기준도출 소스 자동 수집기	기호기반 정적 분석기 스마트 퍼징, 하이브리드 분석기	CWE 호환성 패치 리포트 하이브리드 통합 패치 가이드



08 오픈소스 SW 취약점 분석 플랫폼 상세 프로세스



08 오픈소스 SW 취약점 분석 플랫폼

NEXT

질의응답