SAMSUNG Research

안전한 공개 S/W 활용을 위한 취약점 분석 자동화 시스템

Samsung Research | Security Team | 황용호

2018.11.30

Contents

S/W 개발 Trend

소수 전문가에 의한 수직적 개발이 아닌,

집단지성으로 **다수**의 수평적 개발 더 중요

※ 앤드루 맥아피 / MIT 수석과학자 "인텔 Shift 2017" 기조 연설

[주요 오픈소스 프로젝트]

Apache HTTP server, Mozilla Firefox, Chromium, LibreOffice, GNU/Linux, Android, Tizen …

[외부 공동개발 활용 사례]

MS社 : 최대 Open Source 운영

- Closed → Open 개발환경으로 변화
- 1천 5백개 Repo 운영, GitHub 인수 발표 ('18.6月)

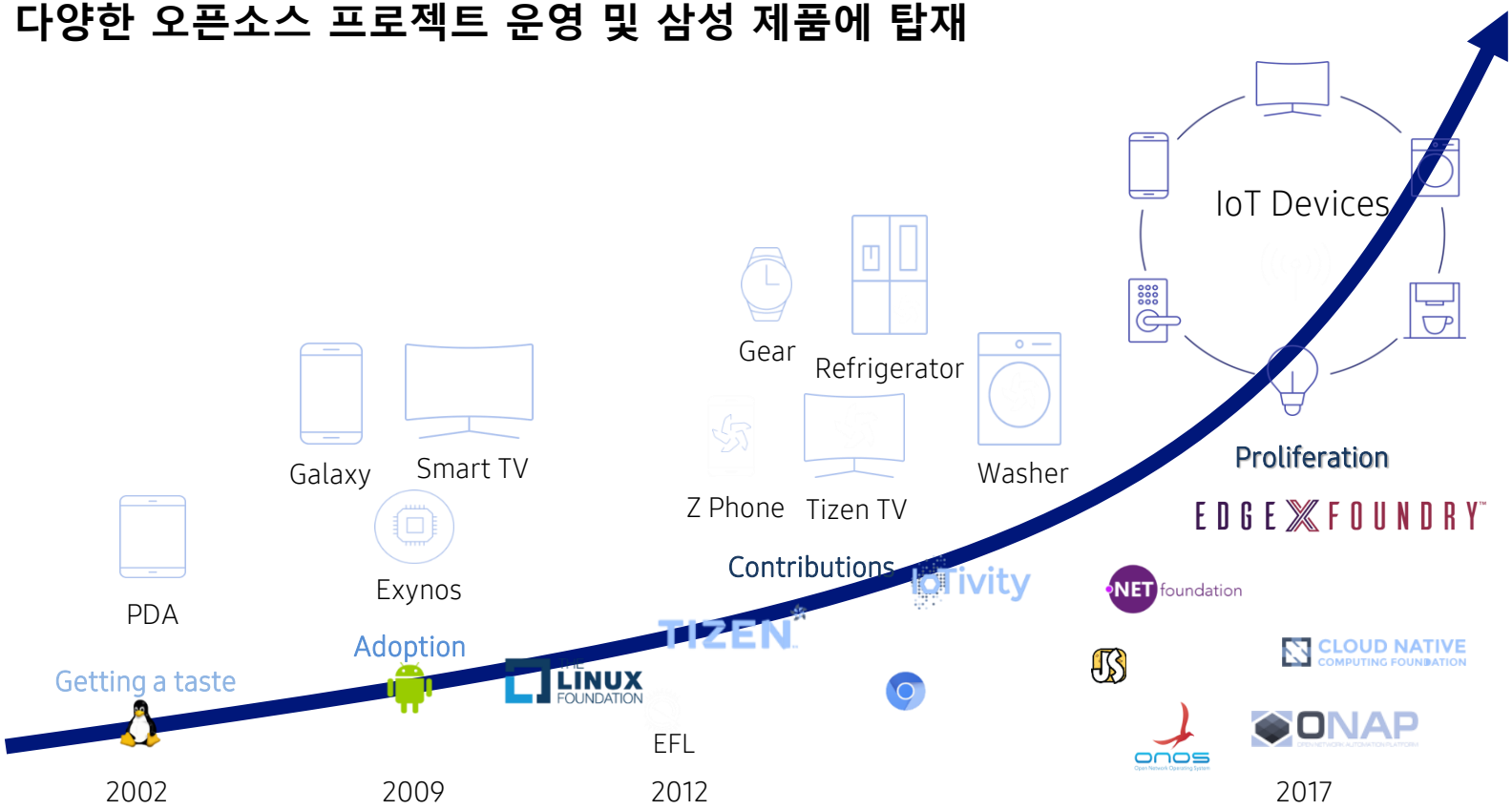
Satya Nadella
現 MS CEO
('14~)

Top 500 수퍼컴 OS, 100% Linux

- Open Source化 급증

Open Source in Samsung Research

√ 다양한 오픈소스 프로젝트 운영 및 삼성 제품에 탑재



Open Source vs. Security






Heartbleed	DROWN	FREAK	Ghost	ShellShock	Meltdown	Spectre
CVE-2014-0160	CVE-2016-0800	CVE-2015-0204 CVE-2015-1637	CVE-2015-0235	CVE-2014-6271 CVE-2014-7169 CVE-2014-7186	CVE-2017-5754	CVE-2017-5753 CVE-2017-5715 CVE-2018-3640 CVE-2018-3639 CVE-2018-3665 CVE-2018-3693

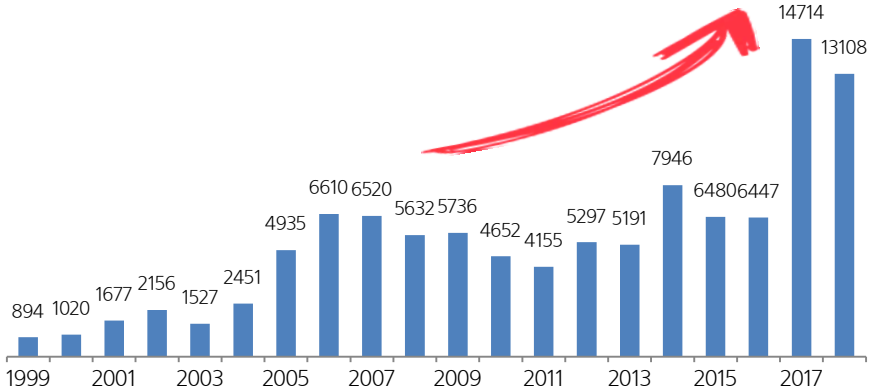
공유 개발 시스템에서 취약점 발생時,

사용하고 있는 **여러 제품**에서 **동시에** 취약점 발생 및 **해킹에 노출**

Open Source vs. Security

14,714

4,800



[공개된 취약점 현황]
from Synopsys Open source Security Report 2018

Common Vulnerabilities and Exposures (CVE)

√ CVE 란?

"A list of information security vulnerabilities and exposures that aims to provide common names for publicly known cyber security issues."

√ CVE는 어떻게 부여되나?

- CNAs (CVE Numbering Authorities)에서 CVE 여부 및 Numering 부여

Each CVE ID includes:

- CVE Identifier number (i.e., "CVE-1999-0067", "CVE-2014-10001", "CVE-2014-100001").
- Brief description of the security vulnerability or exposure.
- Any pertinent references (i.e., vulnerability reports and advisories).

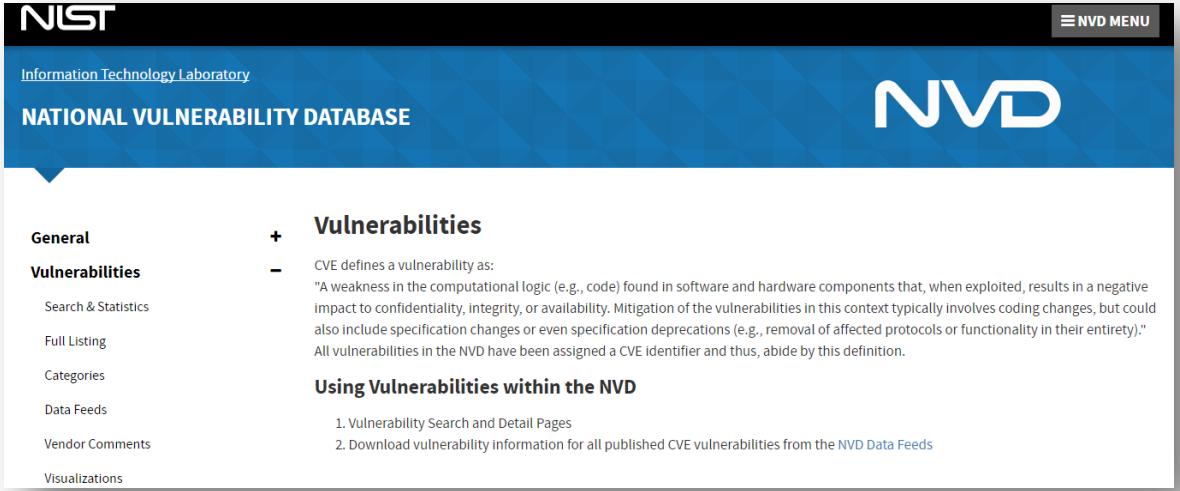
- 새로운 보안 취약점이 신고 되면, CVE Numbering Authority (CNA) 가 CVE ID 를 할당하고 CVE 웹사이트에 CVE 목록을 게재

CVE 관리

√ NVD (U.S. National Vulnerability Database)

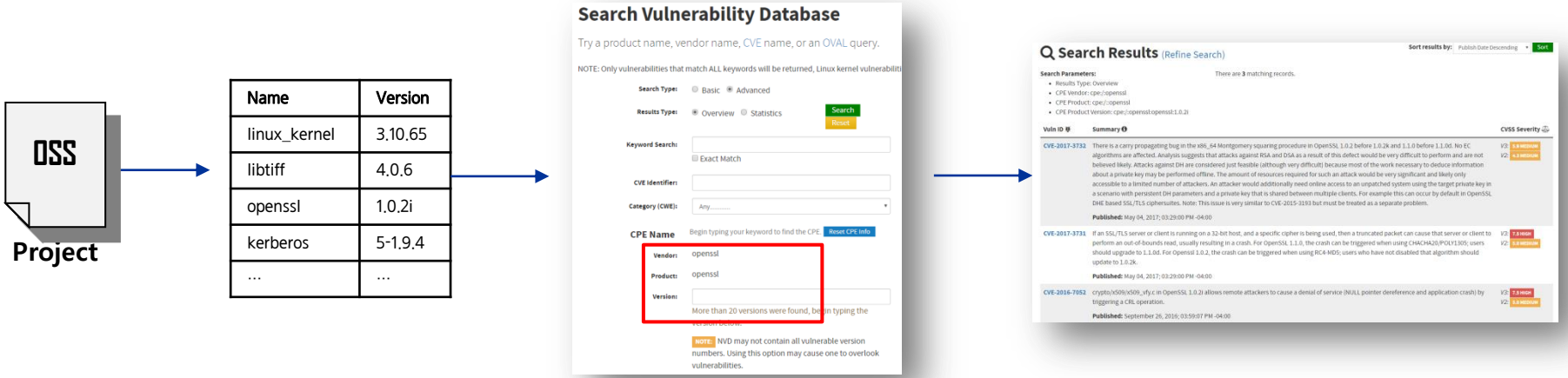
- CVE 목록이 미국의 National Vulnerability Database에 기입되고(NVD),

  fix information, 및 severity scores, impact ratings 와 같은 CVE 정보가 함께 저장됨



CVE 분석 자동화 시스템 필요성

수동검사 방식 (1/2)



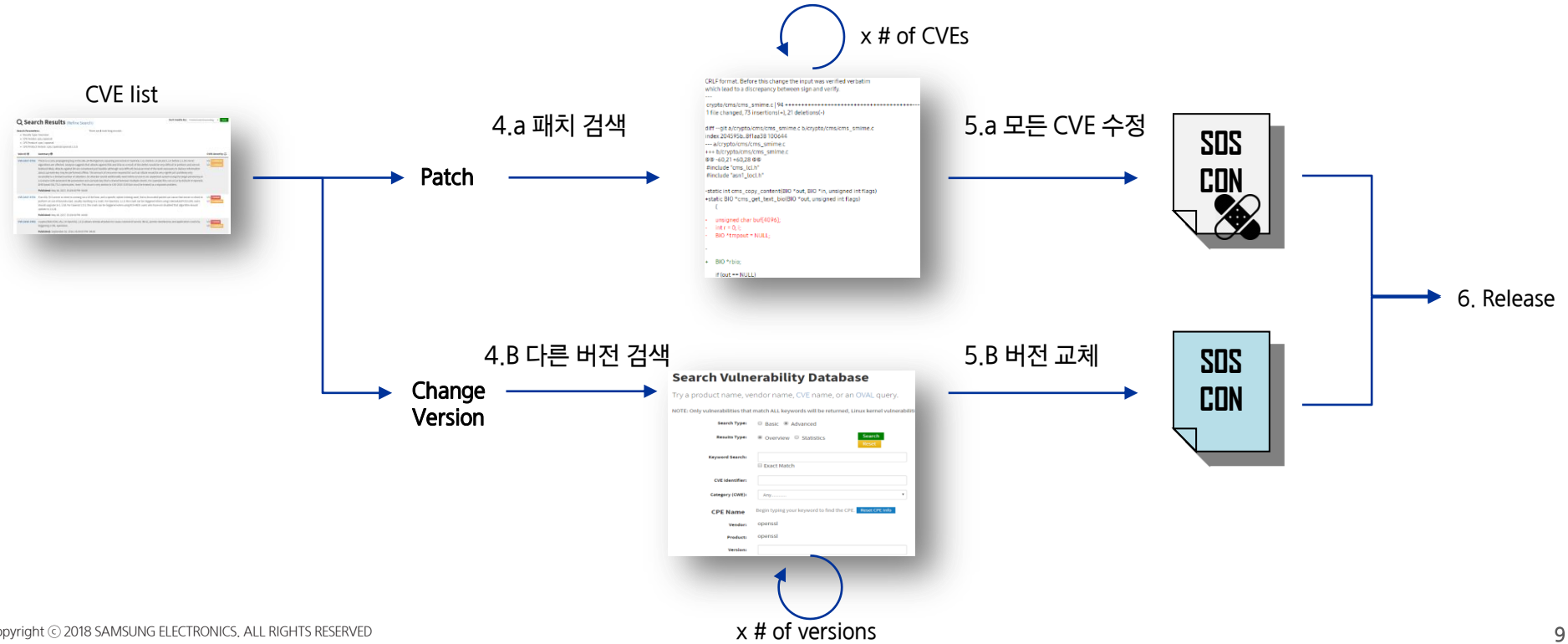
1. 오픈소스 식별

2. NVD에서 CVE 검색

3. CVE 리스트 확인

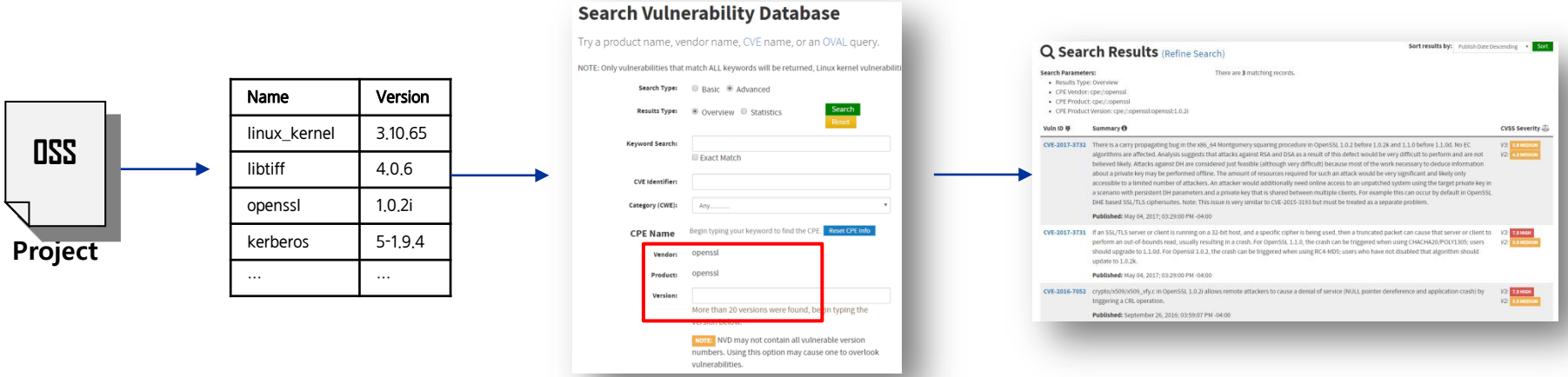
CVE 분석 자동화 시스템 필요성

수동검사 방식 (2/2)



CVE 분석 자동화 시스템 필요성

Pain points (1/2)



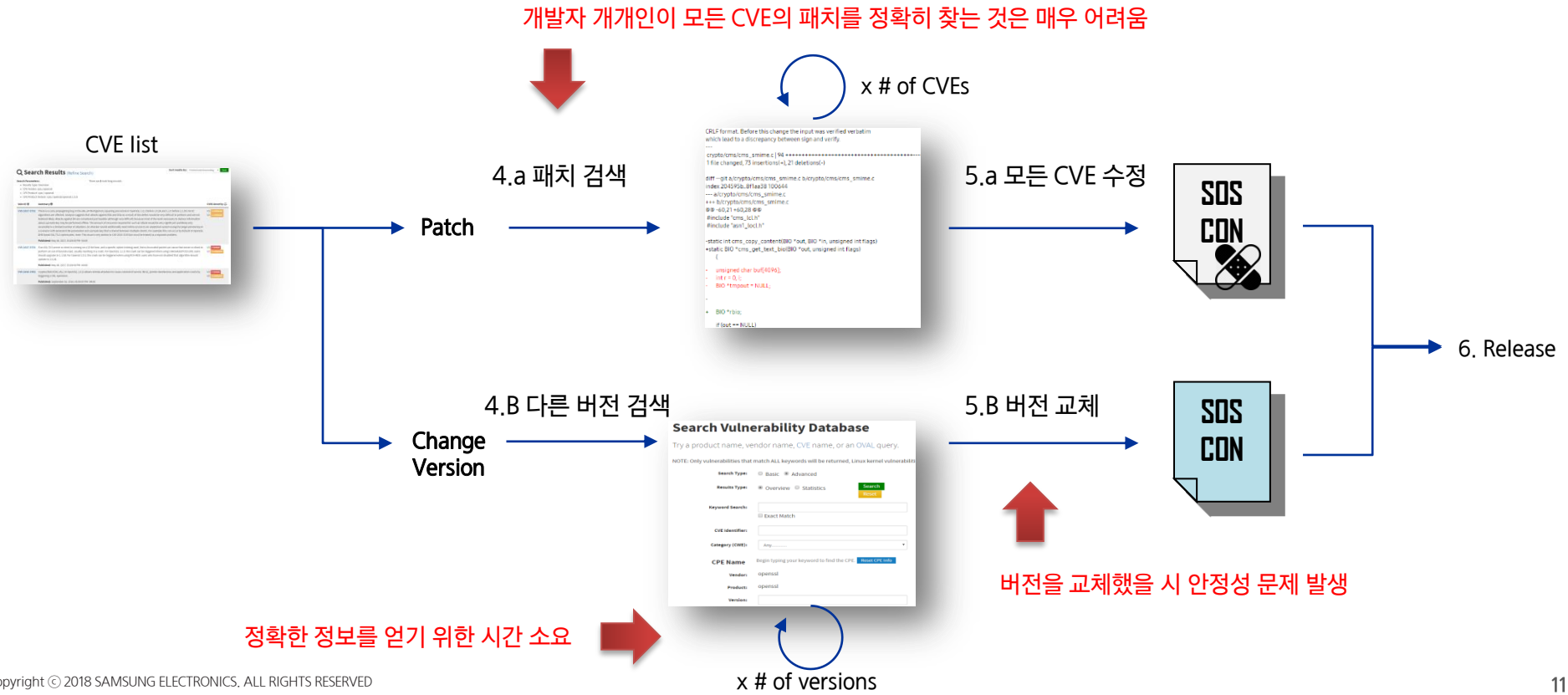
1. 오픈소스 식별
2. NVD에서 CVE 검색
3. CVE 리스트 확인

사용된 오픈소스 식별 어려움
- 프로젝트에 사용된 오픈소스에 대한 정보부족이나 관리 미흡

일반적이고 정형화된 오픈소스 명칭 부재
- linux_kernel, linux-kernel, linux, kernel …

CVE 분석 자동화 시스템 필요성

Pain points (2/2)



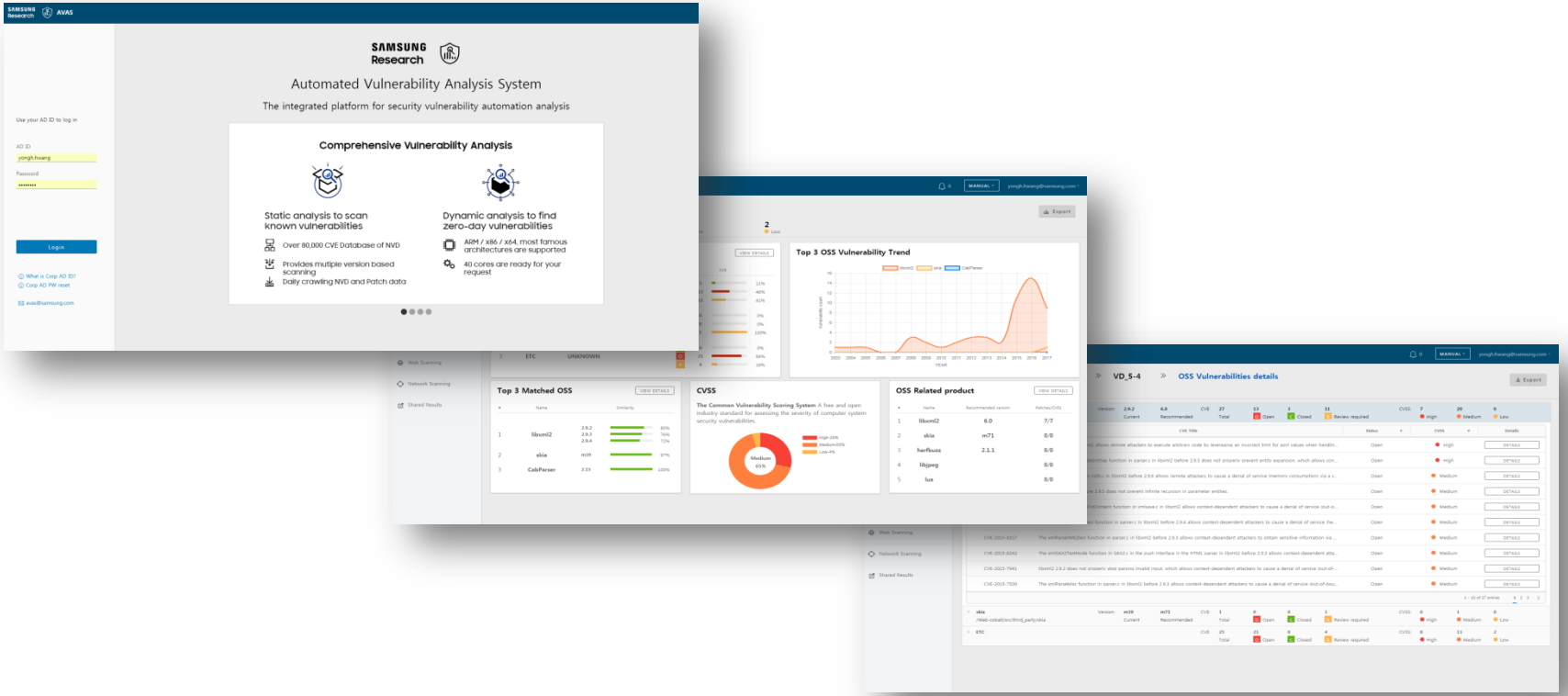
개발자들을 위해 무엇이 필요한가?

Requirements for scanning CVEs

- 자동화된 시스템
- 낮은 false positive
- 오픈소스 명과 버전 관리 불필요
- 적절한 수정을 할 수 있도록 CVE의 위치 제공
- 발견된 취약점들 수정을 위한 패치 정보 제공

Automated Vulnerability Analysis System (AVAS)

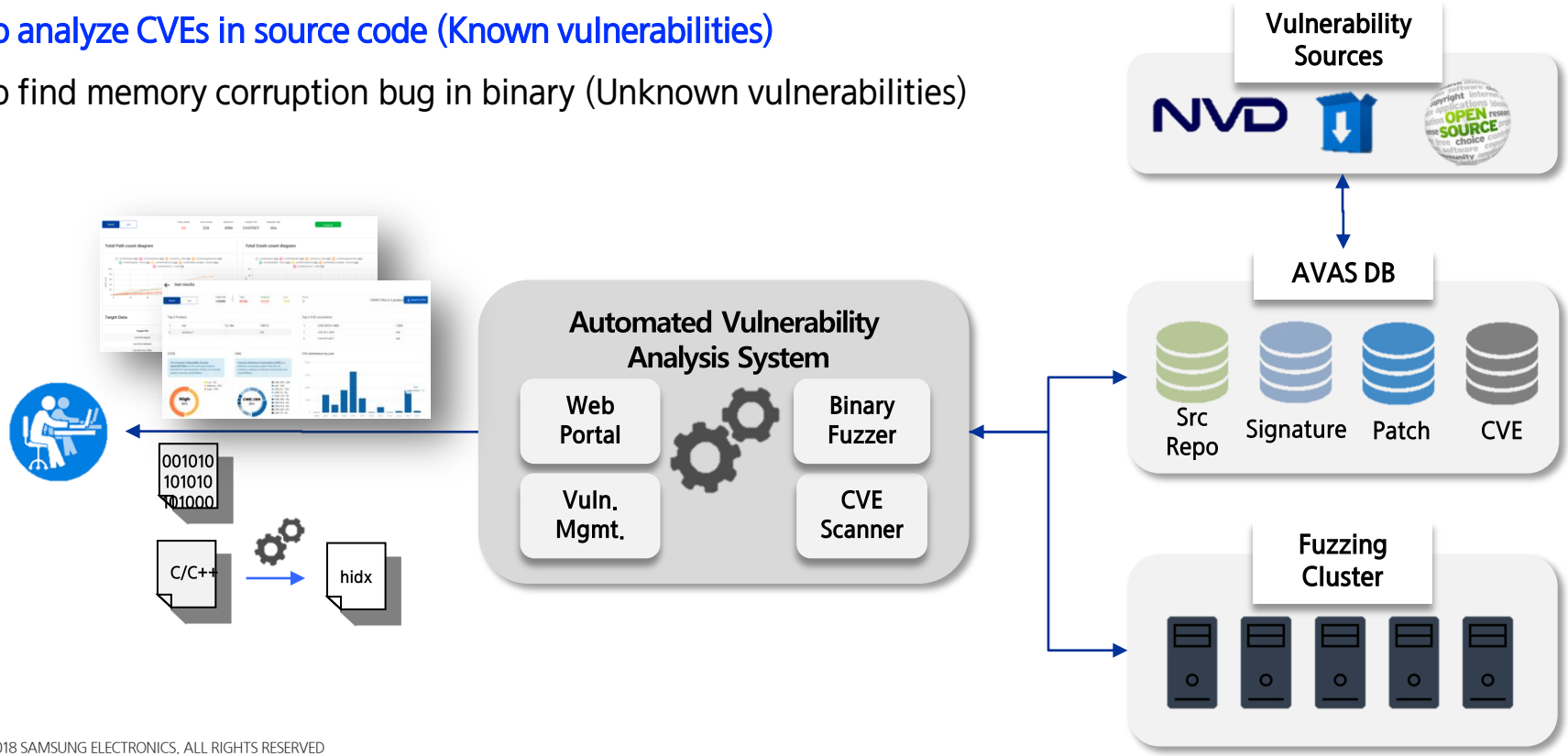
Easy-to-use web-based system



Automated Vulnerability Analysis System (AVAS)

Easy-to-use web-based system

- to analyze CVEs in source code (Known vulnerabilities)
- to find memory corruption bug in binary (Unknown vulnerabilities)

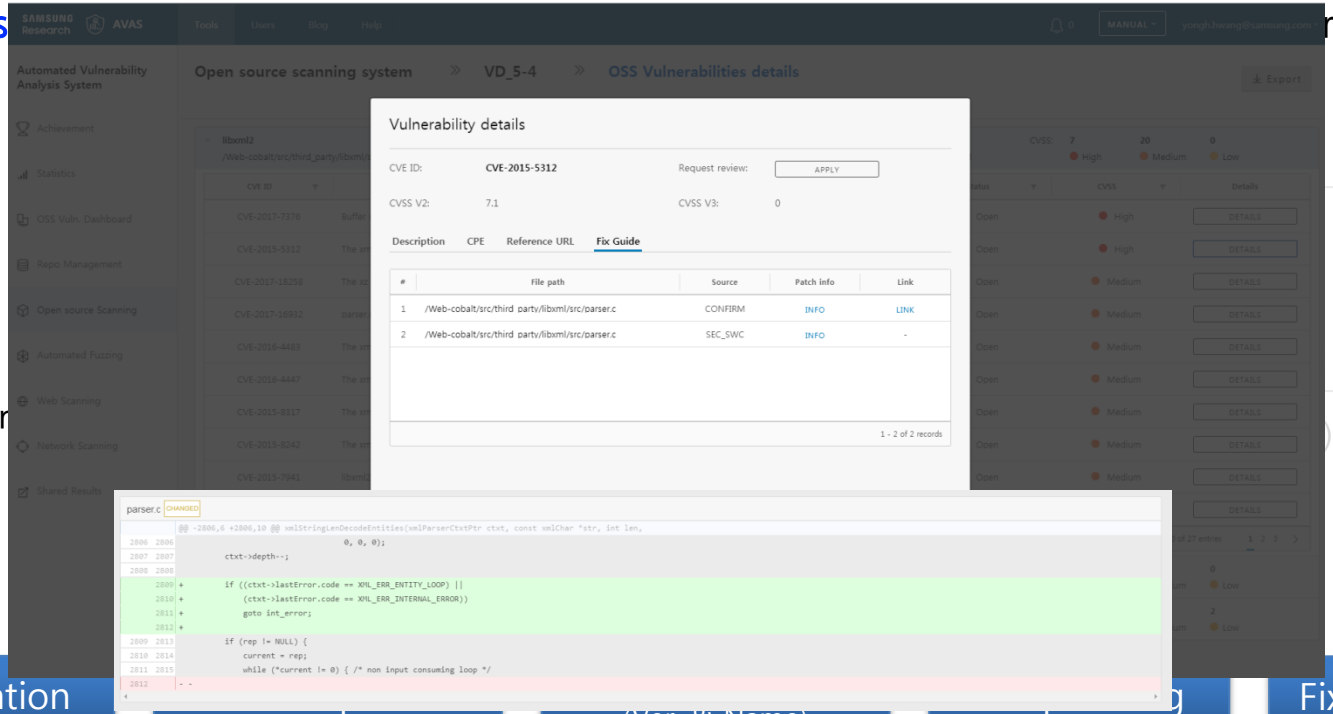


Automated Vulnerability Analysis System (AVAS)

CVE Scanner

- provide s matically

[Oper



in cooperation with CSSA
Center for Software Security and Assurance

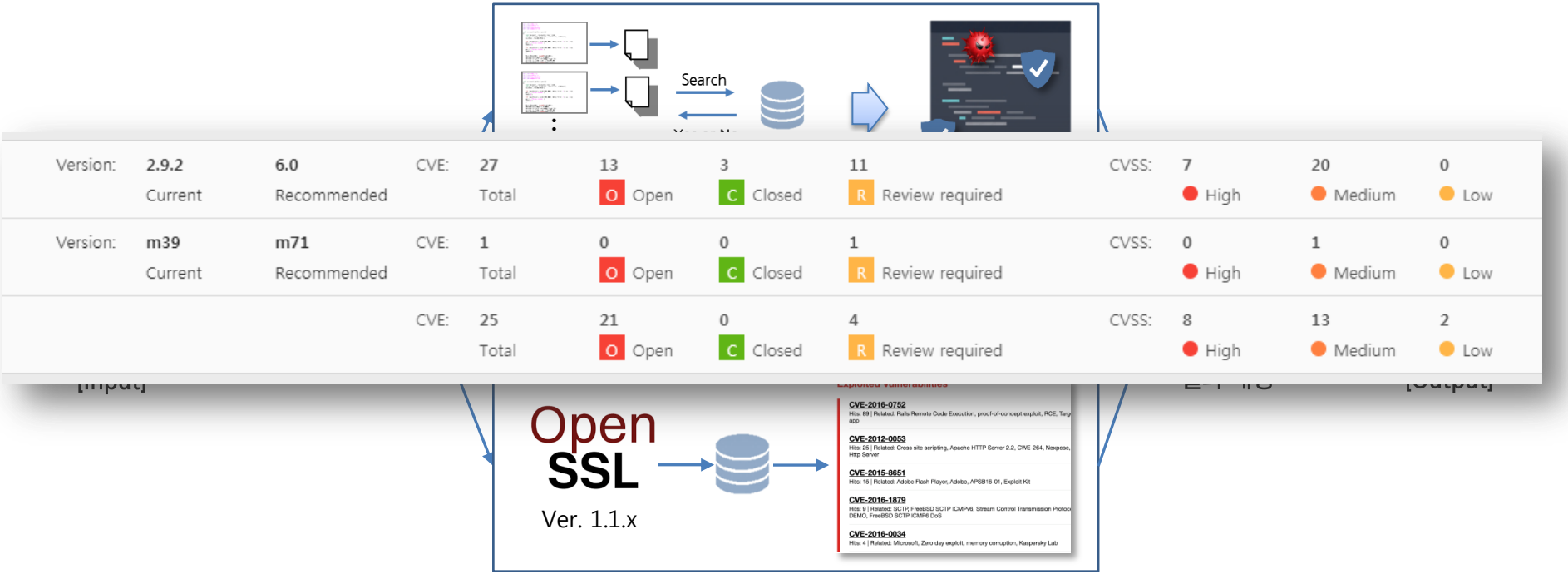
Automation

(Ver. & Name)

Fixing information

Automated Vulnerability Analysis System (AVAS)

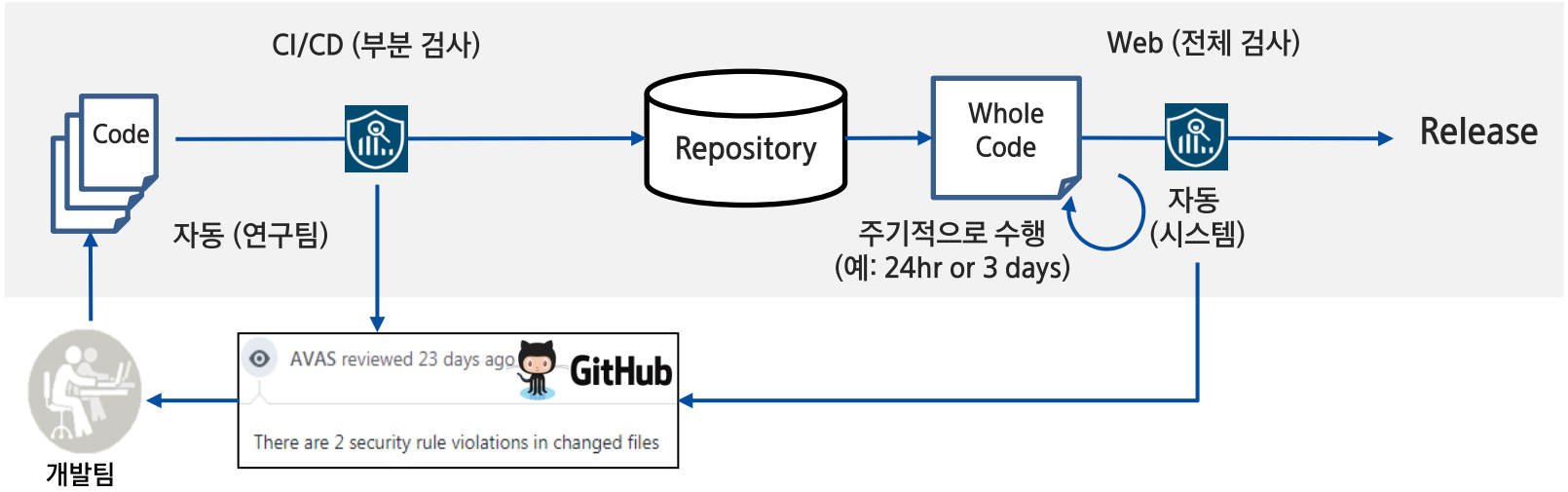
CVE Scanner Flow



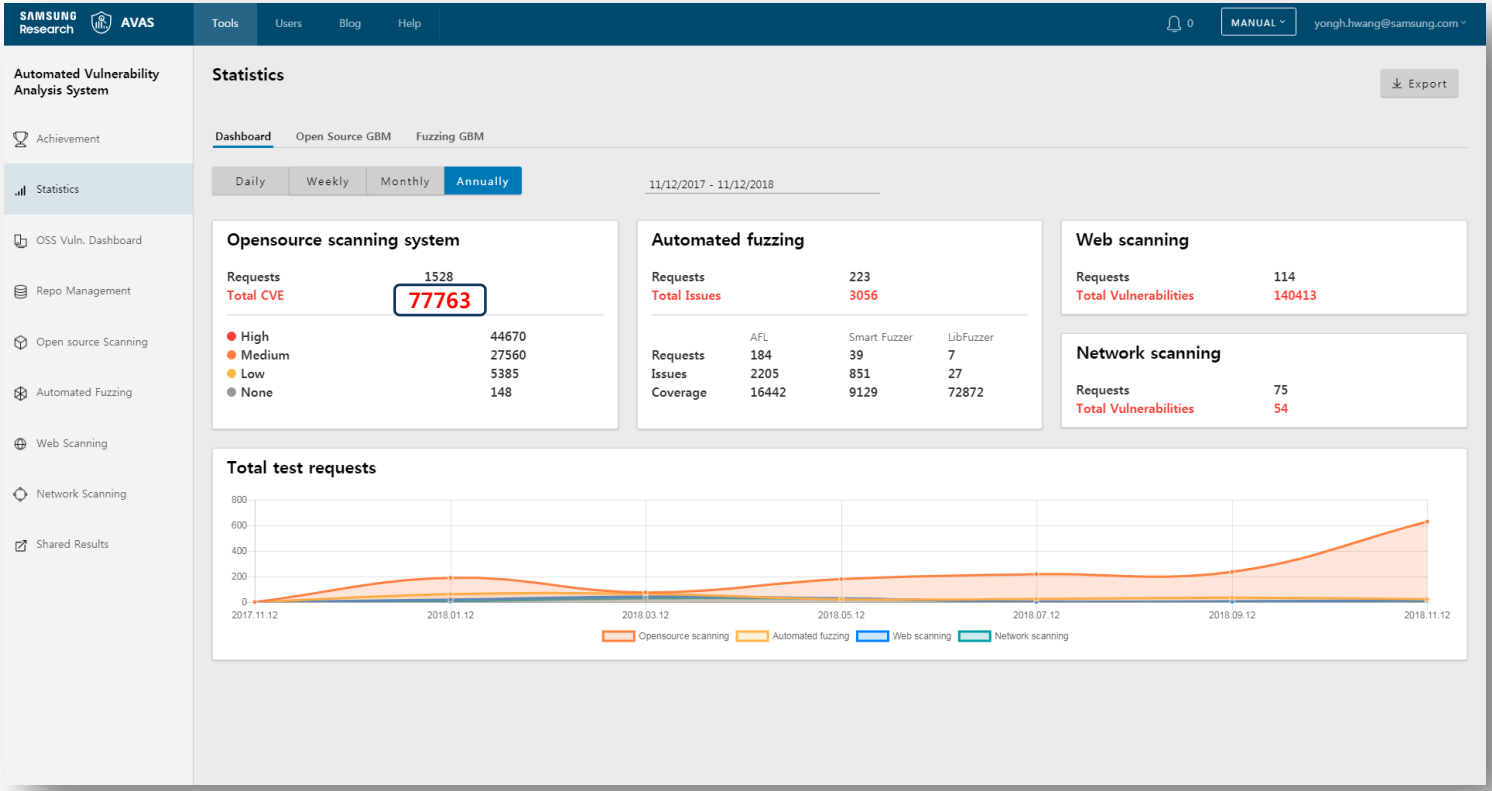
Version:	2.9.2 Current	6.0 Recommended	CVE:	27 Total	13 O Open	3 C Closed	11 R Review required	CVSS:	7 High	20 Medium	0 Low
Version:	m39 Current	m71 Recommended	CVE:	1 Total	0 O Open	0 C Closed	1 R Review required	CVSS:	0 High	1 Medium	0 Low
			CVE:	25 Total	21 O Open	0 C Closed	4 R Review required	CVSS:	8 High	13 Medium	2 Low

Version 기반 전체 CVE 목록 탐지

AVAS in USE



AVAS: Statistics



Infographic for AVAS

CVE Scanner

CVE

OVER
111,000

NVD

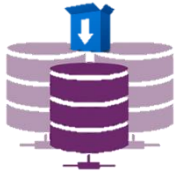
OSS Recognition Accuracy

91.49%

TIZEN

Patch

23,000



CVE Detection Accuracy

92.17%

Crawling

24h

Supported Languages

11

C/C++

Java

php

‘18.09月 기준

Summary

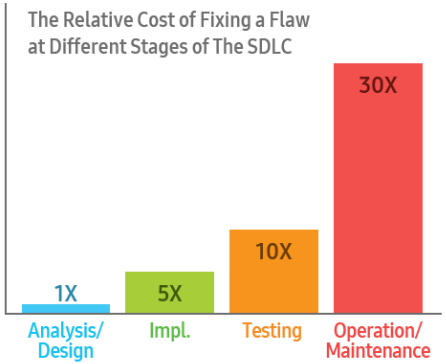
√ 공개 S/W의 활용은 필연적이나, 취약점 발생 시 공격에 쉽게 노출

√ S/W 개발 단계에서 체계적인 보안검증 활동 필요

- 출시前 **알려진 취약점들(CVE 등) 제거** 필요

√ 보안개발 프로세스에 대한 **시스템화**

- 체계적인 보안 활동 가능, 분석 및 대응 현황 제공



√ 보안 **검증 자동화**

- Manual 검증은 매우 제한적이기 때문에 자동화 기능 연구/개발 반드시 수행되어야 함

THANK YOU