1등급 GOOD Software

SolidStep CVE

## CVE 취약점 진단 자동화 솔루션

# 솔리드스텝 CVE 제품소개서

CVE 취약점 진단부터 권고, 조치 결과 확인, 보고까지 One-Stop으로 관리하는 CVE 취약점 진단 자동화 & 인벤토리 관리 솔루션입니다.

SSR (주)에스에스알
www.ssrinc.co.kr

SolidStep CVE

Automatic Security Vulnerability Scanner

# CONTENTS

# 01. SSR 소개

1. 회사개요
2. 주요연혁
3. 사업분야

# 1. 회사개요

## SSR(Security Strategy Research)

SSR(에스에스알)은 공공 및 대기업, 금융, 교육, 의료기관을 대상으로 취약점 진단, 정보보호 관리체계 수립, 개인정보보호 컨설팅 및 자체 개발 보안 솔루션을 제공하고 있는 **과학기술정보통신부 지정 '정보보호 전문서비스 기업'** 입니다.

취약점 진단 솔루션 및 컨설팅
핵심 기술을 자체 보유한
대한민국 대표 정보보안 기술 선도 기업

MENSA

고급 이상의 보안컨설팅 인력
대다수가 MENSA로 구성된
최상의 보안 전문가 집단

SolidStep
MetiEye

100% 순수 자체 기술과
컨설팅 노하우로 개발한
IT 보안 제품 시리즈

1st BEST

독보적 국내 시장점유율 1위인
취약점 진단 자동화 솔루션
(2016~2021년 조달 기준 평균 70%↑)

IPO

2018년
코스닥 상장

500,000+진단수행

전 산업분야 500,000회 이상
취약점 진단 및 컨설팅을 수행하며
다수 고객사 확보 및 빠른 성장세

# 2. 주요연혁

**2021**
- **12. SolidStep CVE GS 인증 획득**
- **11. SolidStep CVE 출시**
- 08. SolidStep CCE 출시 / SolidStep CCE GS 인증 획득
- 04. 신한은행과 보안취약점 자동조치 기능 개발 업무 협약 체결

**2020**
- 05. 인프라 취약점 진단 솔루션의 신규 버전 'SolidStep Portable' 출시
- 04. 보이스피싱 방지 방법, 방지 서버, 이를 위한 컴퓨터 프로그램 특허 획득

**2019**
- 10. 클라우드 시스템 취약점 진단 자동화 솔루션 'SolidStep for Cloud' 출시

**2018**
- 12. 수출유망 중소기업 선정(중소기업수출지원센터)
- **08. 코스닥 상장**
- **04. 정보보호 전문서비스 기업 지정**

**2017**
- 09. SolidStep Cloud 출시
- 07. 우수벤처 연구개발 부문 선정
  지란지교시큐리티 자회사로 편입
- 03. 솔루션 유럽 등 해외 수출

**2016**
- 10. 전자·IT의 날 국무총리 표창 수상
- 09. 서울형 강소기업 선정
- 08. 실행 프로그램 동적감시 특허 획득
- **05. SolidStep 특허 획득**
- 04. ICT INNOVATION 특별상 수상
  청년친화 강소기업 선정
- 02. SolidStep for PC 출시


**2015**
- 12. 정보보호산업 유공 장관상 수상
  인재육성형 중소기업 선정
- 09. 기술유출 방지 유공 장관상 수상
- 08. 개인정보 영향평가기관 지정
- 07. SolidStep PieLook 출시
- **04. SolidStep V2.5 출시**

**2014**
- **12. SolidStep CC 인증 획득**
- 11. 기술사업화 유공장관상 수상
  MetiEye 특허 획득
- 08. MetiEye CC 인증 획득
- **05. SolidStep GS 인증 획득**
- 04. 기술혁신형 중소기업(INNO-BIZ) 선정
- 03. MetiEye GS 인증 획득
  **지식정보보안 컨설팅 전문업체 지정**

**2013**
- 12. 펜타시큐리티 MOU 체결
- 04. ISO/IEC 27001 인증 획득

**2012**
- **12. SolidStep / MetiEye 출시**
  벤처기업 등록
- 09. ISO 9001 인증 획득

**2011**
- 12. 기술연구소 설립

**2010**
- 09. LG CNS 정보보호 컨설팅 특화업체 선정
- **08. ㈜에스에스알 설립**

# 3. 사업분야

정보보호 전문서비스 기업!
보안의 디테일을 연구합니다.

## 보안 컨설팅

### 정보보호 기술 컨설팅

- IT 인프라 취약점 진단 컨설팅
- 모의해킹 컨설팅
- 침해사고 분석 컨설팅

### 정보보호 관리 컨설팅

- 정보보호 법률 준수 컨설팅
- 정보보호 인증 관리 컨설팅
- 개인정보보호 컨설팅

## 보안 솔루션

### 보안 취약점 진단 자동화 솔루션

- CCE 취약점 진단 자동화
- CVE 취약점 진단 자동화
- PC 취약점 진단 자동화
- 단독형 PC, 폐쇄망 제어 PC 취약점 진단

SolidStep

### 웹 서버 보안 솔루션

- 실시간 웹쉘 탐지 및 차단
- Black, White List 방식 업로드 차단

MetiEye

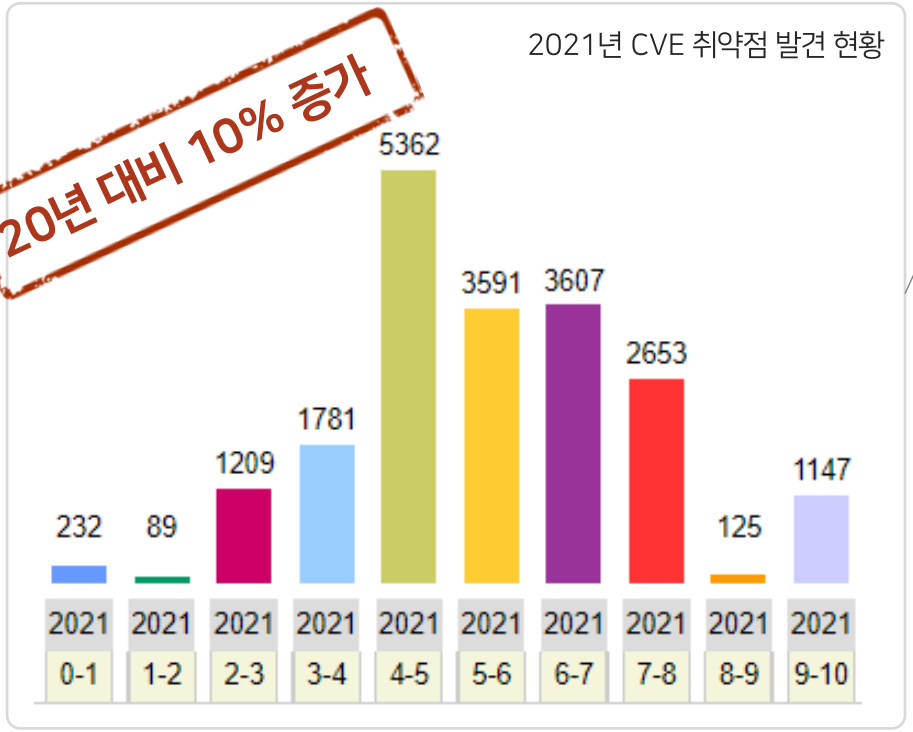
# 02. SolidStep CVE 제품소개

1. CVE 취약점 진단 필요성
2. SolidStep CVE 개발배경
3. SolidStep CVE 제품개요
4. SolidStep CVE 프로세스
5. SolidStep CVE 구성도
6. SolidStep CVE 특장점
7. SolidStep CVE 지원 환경
8. SolidStep CVE 도입효과

# 1. CVE 취약점 진단 필요성 (1/2)

## CVE 취약점이란?

CVE(Common Vulnerabilities and Exposures) 취약점은 **공개적으로 알려진 소프트웨어의 보안 취약점**을 말합니다.
CCE 취약점과 다르게 하루에도 수십 개의 CVE 취약점이 발견되고, CVE 취약점을 이용한 신종 랜섬웨어 공격도 늘고 있습니다.




2021년 보안 취약점 공동평가 시스템(*CVSS)에 따르면
CVSS 점수 7.0 이상 고위험 취약점이
21년도에만 3,925개가 발견(지속적인 증가 추세)

* CVSS(보안 취약점 공동평가 시스템)
- 어플리케이션 취약점(CVE 취약점)들의 심각성과 위험성을 평가하는 가장 보편적인 표준 시스템
- 보안과 관련된 각종 오류의 유형과 특징, 그 영향력들을 보다 간편하게 소통하고 공유하는 데 사용됨

# 1. CVE 취약점 진단 필요성 (2/2)

## CVE 취약점을 이용한 신종 공격들

대부분의 보안 솔루션은 알려진 랜섬웨어나 공격 수법을 탐지할 수는 있지만, Log4j(CVE-2021-44228)와 같이 CVE 취약점을 악용해 권한을 무시하는 해킹 기법을 사용하는 경우에는 즉각적인 방어가 어렵습니다.

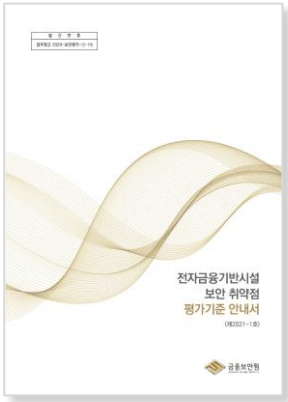
- 기존 **보안 솔루션들이 탐지하기 어려움**
- 이메일 첨부파일 열기 또는 악성 링크 클릭 등 사용자의 개입이 전혀 없더라도 감염 가능
- 예방을 위해서는 **SW 최신버전 업데이트, 취약점 진단 및 패치 관리 기능을 포함한 보안 제품 사용** 등의 조치 필요


- 패치를 주기적으로 업데이트 한다 해도 제조사에서 취약점에 대한 패치를 제때 하지 않으면 취약점에 그대로 노출
- 제조사의 신속한 패치도 중요하지만 제조사 패치에만 의존할 것이 아니라 신규 **CVE 취약점을 수시로 체크하여 내 자산이 위험에 노출되었는지 수시로 진단하는 것이 중요**

# 2. SolidStep CVE 개발배경

## 외산 솔루션에 의존하는 CVE 취약점 점검에 대한 국내 솔루션 필요

국내에도 보안 취약점 점검에 대한 다양한 법정 규제가 있지만 **CCE 취약점 위주**로 진행되고, **CVE 취약점에 대한 강제성이 미비**하여 신규 CVE 취약점 발생 시 즉각적인 대응을 못하고 있습니다. 많은 기관 및 기업에서 CVE에 대한 자체 분석 및 평가를 하고 있다고는 하지만 현실적으로는 많은 어려움을 겪고 있으며, CVE 진단 솔루션을 도입할 경우에도 외산 제품에 의존하고 있어 **국내 솔루션이 필요**합니다.




| 구분 | CCE (Common Configuration Enumeration) | CVE (Common Vulnerabilities and Exposures) |
|---|---|---|
| 진단 대상 | IT 인프라 설정의 취약점 (OS, Network, DBMS, WEB/WAS, PC 등) | 소프트웨어 자체 취약점 (펌웨어, 미들웨어, OS, 어플리케이션 등) |
| 진단 기준 | 주요정보통신기반시설, 전자금융기반시설 등의 기술적 취약점 분석평가 항목 등 | MITRE(NVD) CVE 항목 (KISA CVE 항목 포함) |
| 조치 방안 | 보안 규정에 맞게 관리자가 직접 수정 조치 | 제조사에서 제공하는 패치 적용 |
| 특징 | 정보통신기반시설 보호법 및 보안규정에 따라 취약점 진단, 조치 의무 | 제조사의 의존성으로 인해 법적 의무 없음 |
| 한계 | CVE 취약점을 이용한 신종 랜섬웨어, 어플리케이션 자체 취약점에 대한 신속한 대응 불가 | 매일 수십 개 씩 발견되는 취약점들을 관리하기 어려움 |

# 3. SolidStep CVE 제품개요

## CVE 취약점 진단 자동화 솔루션

SolidStep CVE는 국내 시장에 맞게 다양한 기능을 추가하여 CVE 취약점 진단 뿐만 아니라 자산별 상세 인벤토리 관리까지 가능한 CVE 취약점 진단 자동화 솔루션입니다.

SolidStep CVE

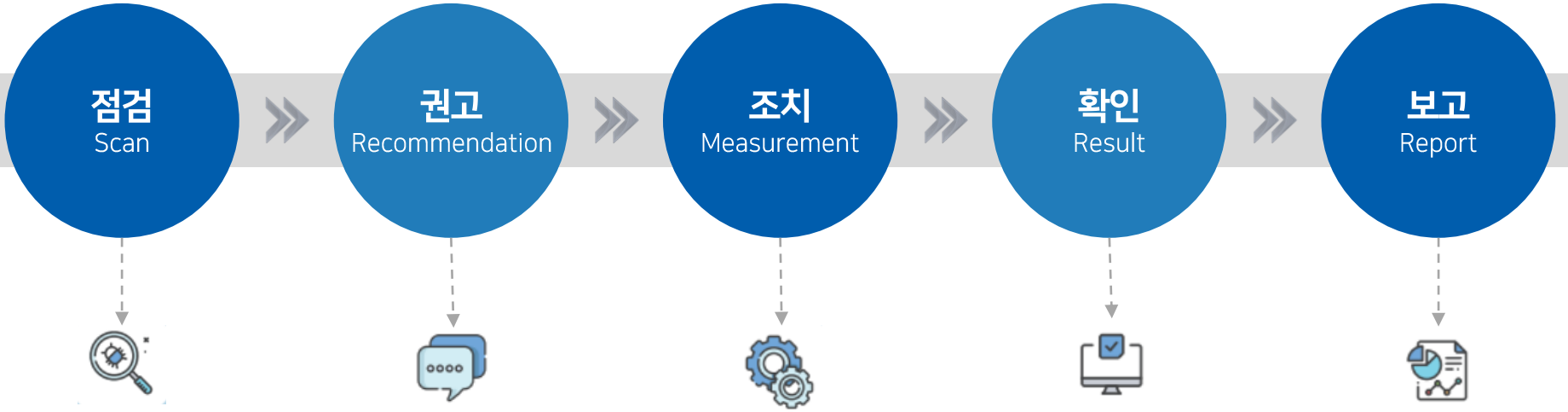

1등급 GOOD Software

- ☑ 검증된 기술력으로 자체 개발한 솔루션, GS1등급 인증 획득
- ☑ CVE 취약점 진단 + 인벤토리 관리 + 자산관리까지 원스톱 관리 가능
- ☑ 최신 CVE 취약점 정보 주기적인 반영으로 빠른 신규 취약점 대응
- ☑ 신속한 자동화 전수 진단 및 진단 결과에 대한 조치 관리 기능 제공
- ☑ 평가점수(CVSS) 전환 기능으로 고객사 평가 기준 최적화 반영
- ☑ 엑셀 형식의 다양한 결과보고서 제공

# 4. SolidStep CVE 프로세스

## 체계적인 One-Stop 취약점 관리

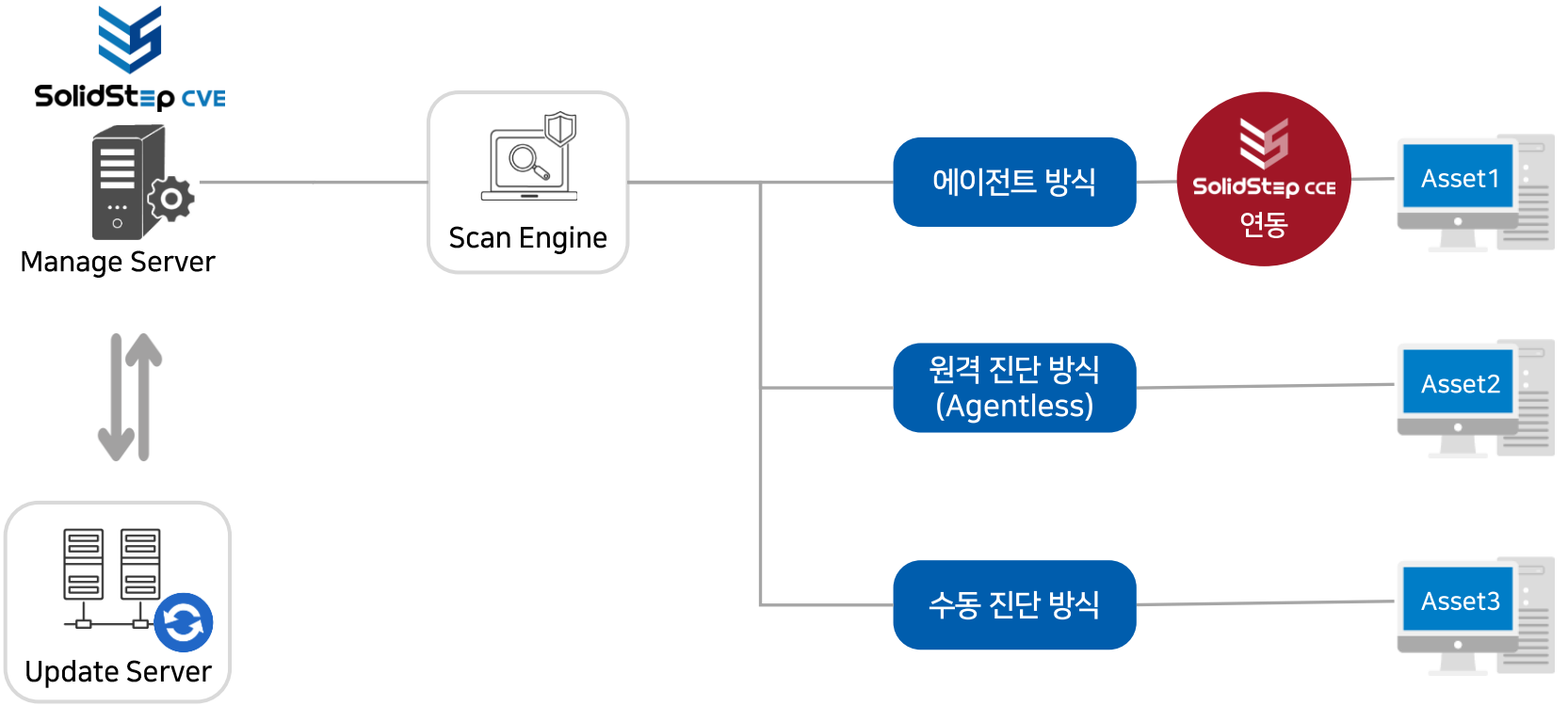
SolidStep CVE는 CVE 취약점 **점검부터 권고, 조치 결과 확인, 보고까지** 모든 과정을 체계적으로 관리합니다.
또한 최신 발표된 데이터를 주기적으로 반영하여 신규 취약점에도 신속하게 대응할 수 있습니다.



# 5. SolidStep CVE 구성도

## 고객 맞춤형 진단이 가능한 구성

SolidStep CVE는 **에이전트, 원격 진단(Agentless), 수동 진단 방식**을 지원하여 고객 맞춤 진단이 가능하며, 최신 CVE 정보를 주기적으로 업데이트 반영하여 최상의 진단 구성을 갖추고 있습니다.



# 6. SolidStep CVE 특장점

## 보안 전문기업이 만든 정확하면서도 쉽고 빠른 솔루션

보안 전문기업 SSR이 국내 시장점유율 1위인 자체 개발 CCE 취약점 진단 자동화 솔루션과 다년간의 보안 컨설팅 기술력으로 만들었습니다.
**신뢰할 수 있는 국산 CVE 취약점 진단 솔루션**으로 정확하면서도 쉽고 빠른 취약점 진단 및 관리가 가능합니다.

### 정확도 높은 진단 방식

- 전체 자산에 대한 원클릭 진단
- 에이전트 및 원격 스캔 진단 방식 제공
- CVSS 버전별 진단 및 전환 가능

### 자산/인벤토리 관리

- 자산별 취약점 현황 관리
- 자산별 상세 인벤토리 관리
  (Port, Service, Product, H/W 등)
- 자산관리대장 작성이 용이하고,
  자산 및 인벤토리 관리가 탁월함

### 쉽고 빠른 UI/UX 환경

- 직관적인 사용자 환경 제공
- Web UI에 최적화되어 있어
  빠른 속도 제공
- 사용자 권한 부여로 체계적 관리 가능

# 7. SolidStep CVE 지원환경

## 다양한 시스템 환경 지원

SolidStep CVE는 **운영 중인 다양한 시스템 환경**의 취약점을 진단합니다.

| 구분 | 상세 내역 | 비 고 |
|---|---|---|
| OS | • Windows<br>- 서버계열 : 2008/2008 R2/2012/2016/2019/2022<br>- PC계열 : 7/8/10/11<br>• Linux(Debian, RHEL, CentOS, Ubuntu, OpenSuse, Amazon Linux, ProLinux)<br>• Unix(HP-UX 11 이상, AIX 5.2 이상, Solaris 5.8 이상) | |
| Network | • CISCO, DELL, F5, Juniper, Huawei 등 글로벌 벤더사 모델 5,000개 이상 지원 | |
| Application | • Microsoft Exchange Server, Microsoft SQL Server, Microsoft Edge, Internet Explorer, Adobe Flash Player 등 500개 이상 지원 | |
| Developer Tools | • Microsoft .NET Framework, Microsoft Visual Studio, ASP.NET, Microsoft Silverlight, PowerShell 등 200개 이상 지원 | |
| Linux(Unix) Packages | • Samba, Openssh, Openssl, Bash, Glibc 등 1,200개 이상 지원 | |
| Microsoft Office | • Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Microsoft OneNote, Microsoft Outlook 등 200개 이상 지원 | |

※ 신규 플랫폼에 대한 지속적인 개발 및 지원

# 8. SolidStep CVE 도입효과

## 보안 체계 강화로 안정적인 시스템 운영

SolidStep CVE는 운영되고 있는 정보시스템의 CVE 취약점들을 상시 점검 및 분석하여 사고를 예방하고, 안정적인 운영과 관리 환경을 제공합니다.


### 01 취약점 진단과 자산관리의 자동화

- 자동화된 CVE 취약점 진단 및 자산 관리로 가시성 확보
- 자동화된 진단을 통해 지속적인 CVE 취약점 평가 가능

### 02 보안사고 예방을 통한 안전성 확보

- 주기적인 보안 취약점 분석을 통해 보안 위협을 사전에 예방하여 보안 사고 최소화 및 안전한 운영 가능
- 최신 발표된 CVE 데이터를 주기적으로 반영하여 신규 취약점에도 안전하게 대응 가능

### 03 신속하고 체계적인 보안관리

- 신규 취약점의 신속한 반영과 보안 진단 프로세스 개선을 통한 체계적인 보안 관리 가능
- CVE 취약점 관리를 위한 효율적인 통합된 업무 환경 지원

### 04 보안수준 향상 및 보안체계 강화

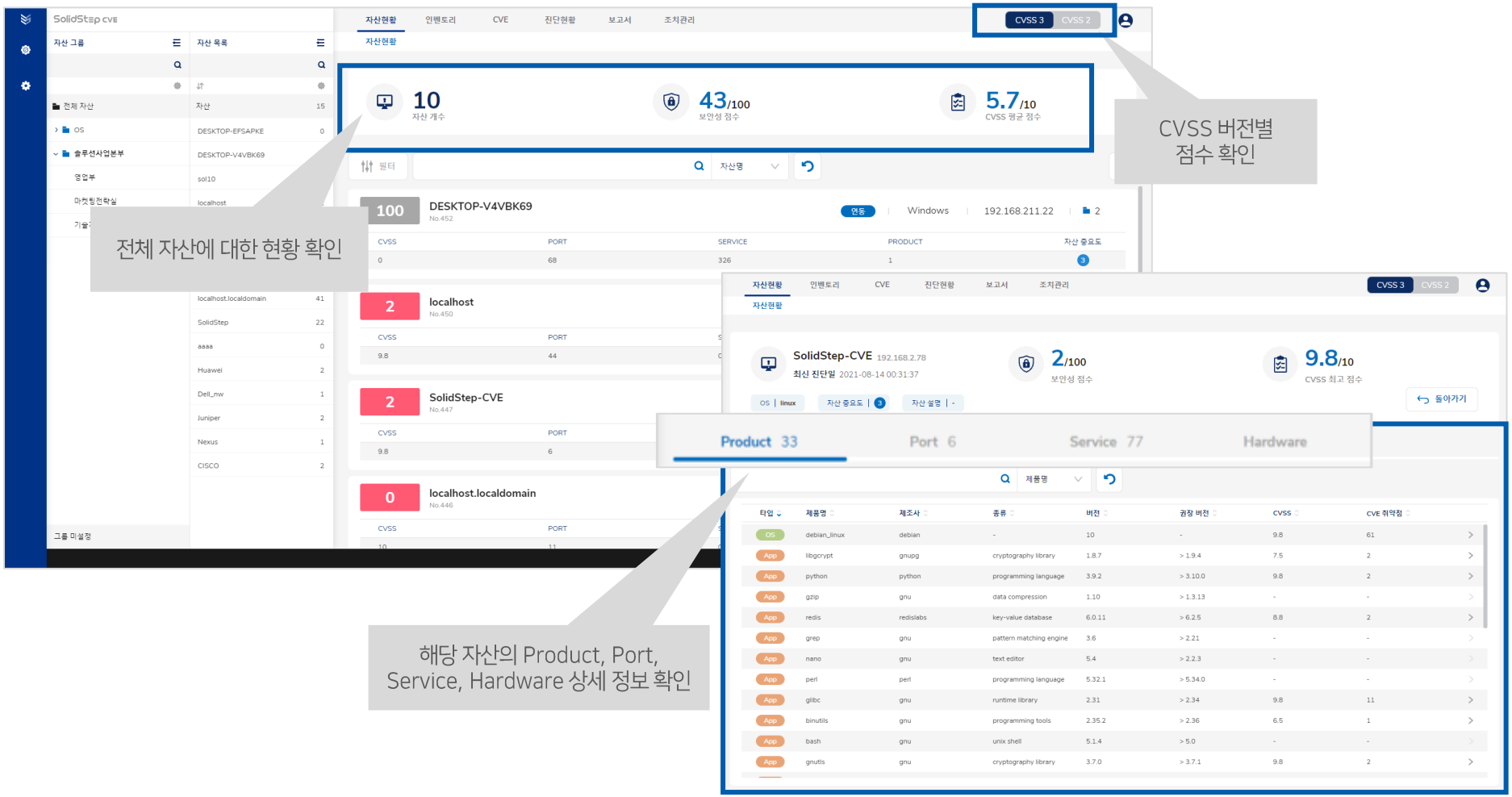
- 보안 관리 정책 강화를 통해 기업의 보안 수준과 경쟁력 향상 기대
- 정보시스템의 동일한 보안 수준 유지 및 보안 수준 향상을 위한 체계 확립 가능

# 03. SolidStep CVE 주요기능

1. 편리한 Web UI 방식의 대시보드
2. 자산 설정 및 자산 그룹 관리
3. 진단 실행
4. 인벤토리 관리
5. 상세한 진단 결과 보고서
6. 신속한 조치 관리

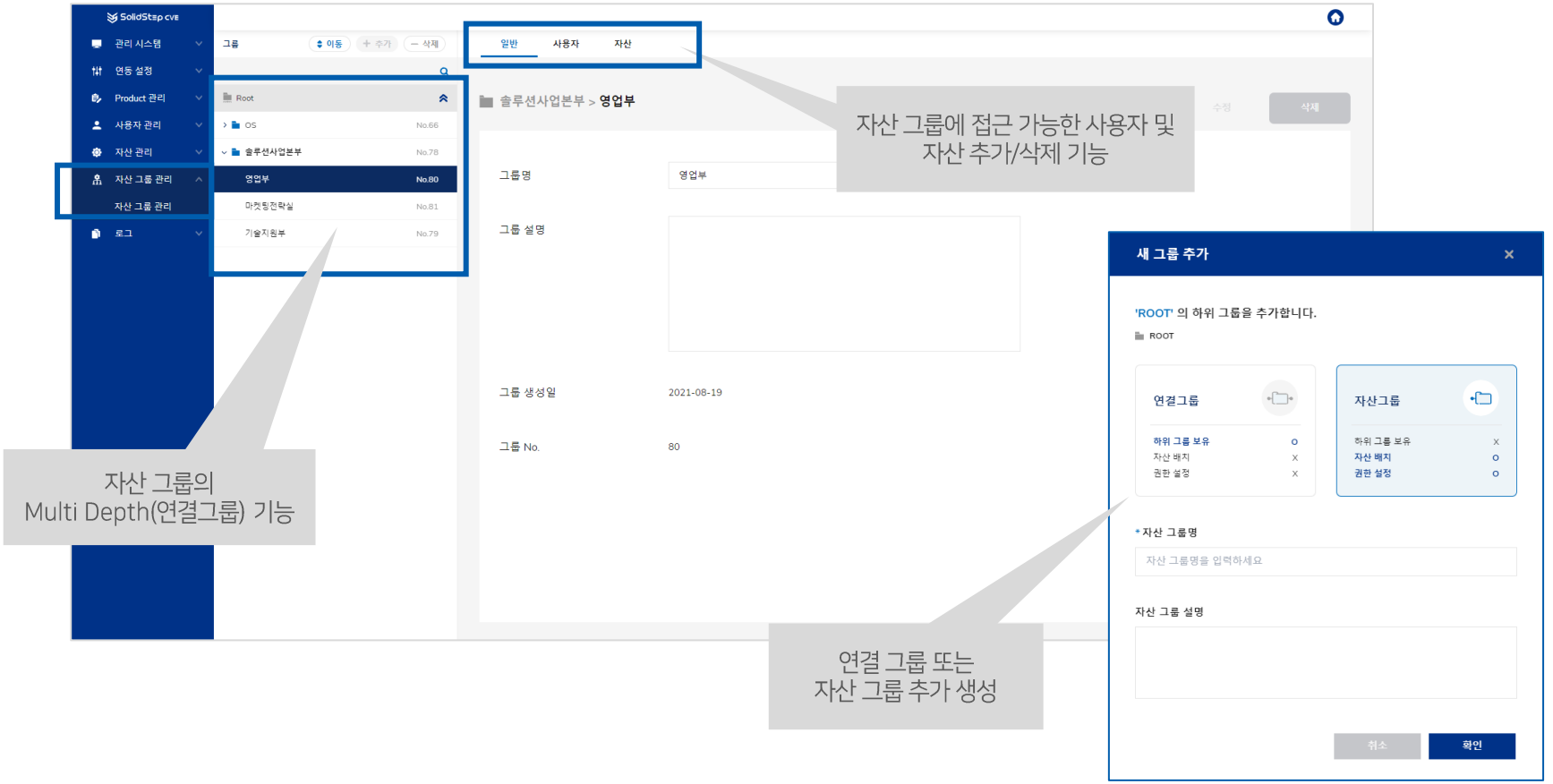
# 1. 편리한 Web UI 방식의 대시보드

SolidStep CVE는 전체 자산에 대한 현황 및 상세 정보, 인벤토리, CVE, 진단현황, 보고서, 조치 관리 등 다양한 현황 파악 및 관리가 편리하도록 사용자 접근성과 편의성을 고려한 Web UI 방식의 대시보드를 제공합니다.



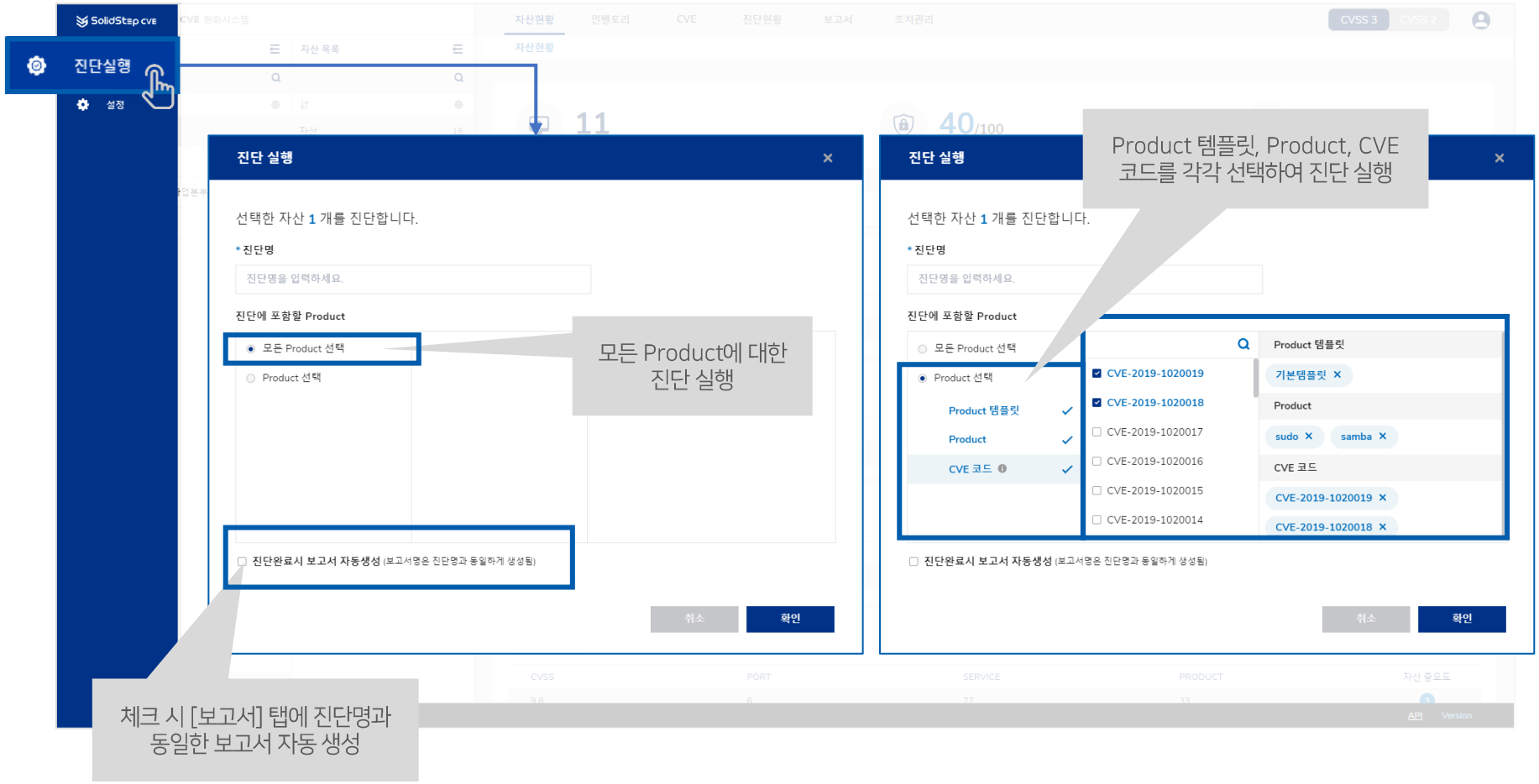
# 2. 자산 설정 및 자산 그룹 관리

자산별, 운영 부서별 다양한 그룹핑 설정으로 **물리적/논리적 그룹화 관리가 가능**하며, **관리자/사용자별 접근 권한 관리 기능**을 제공합니다.



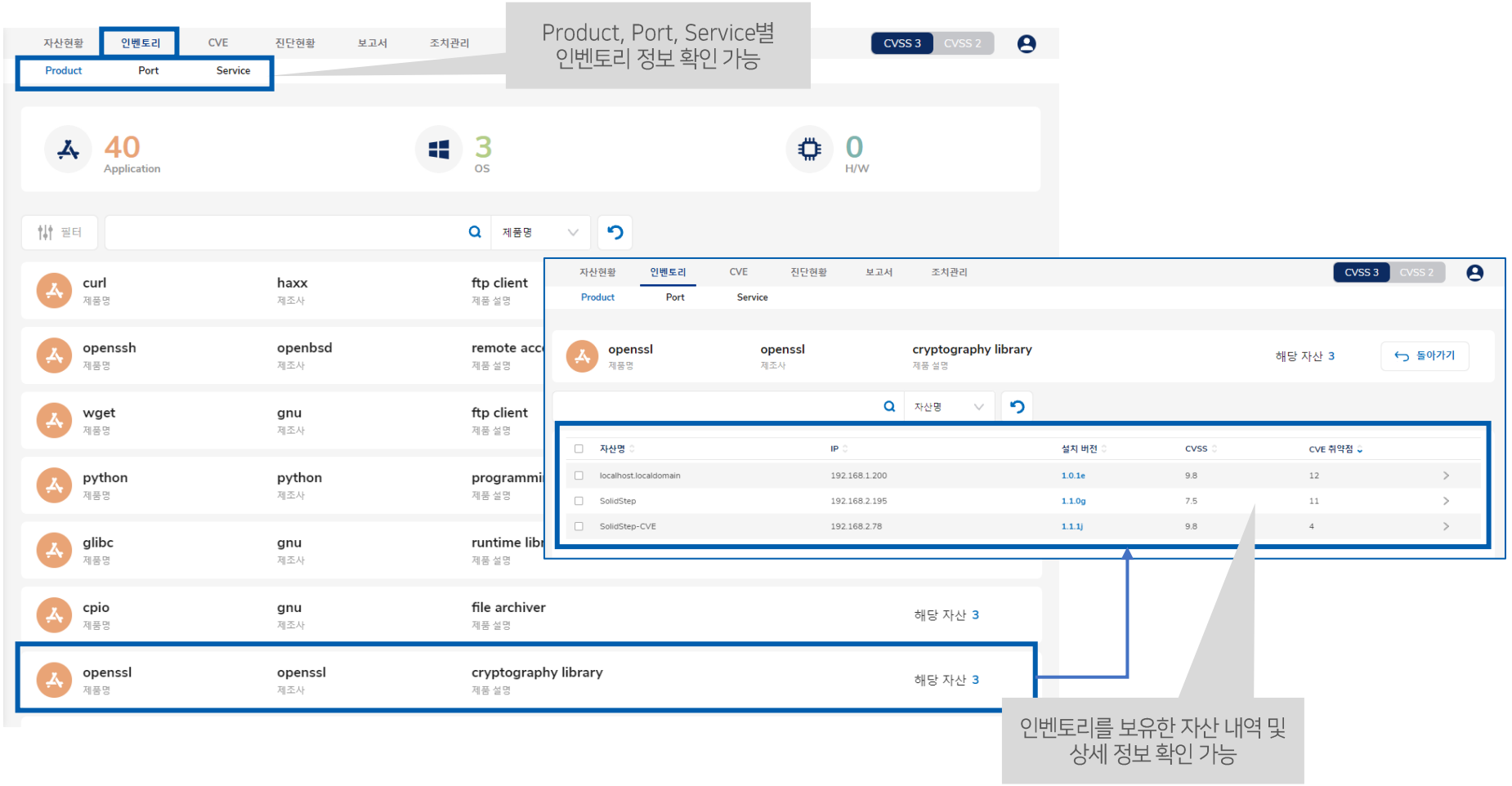
# 3. 진단 실행

**왼쪽 사이드바 [진단실행] 메뉴를 클릭**하여 편리하게 취약점 진단을 실행할 수 있습니다. 모든 Product를 선택하거나 사용자 요구에 맞게 Product, 템플릿, CVE 코드를 선택하여 진단할 수 있어 보다 유연하고 효율적인 진단이 가능합니다.



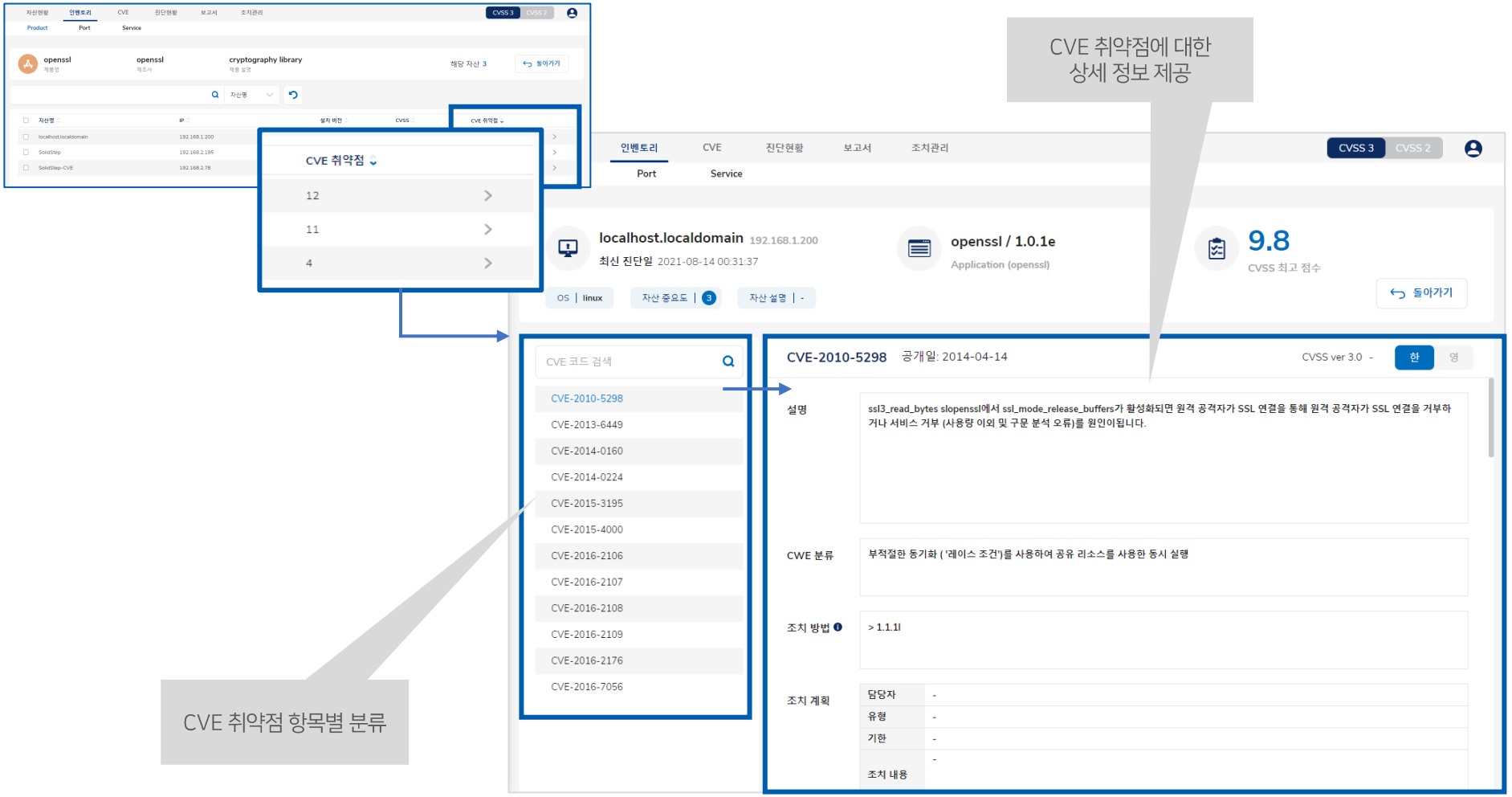
# 4. 인벤토리 관리 (1/2)

**인벤토리별 취약점 점수,** 인벤토리를 보유한 **자산 내역 및 상세 정보 확인**이 가능합니다.



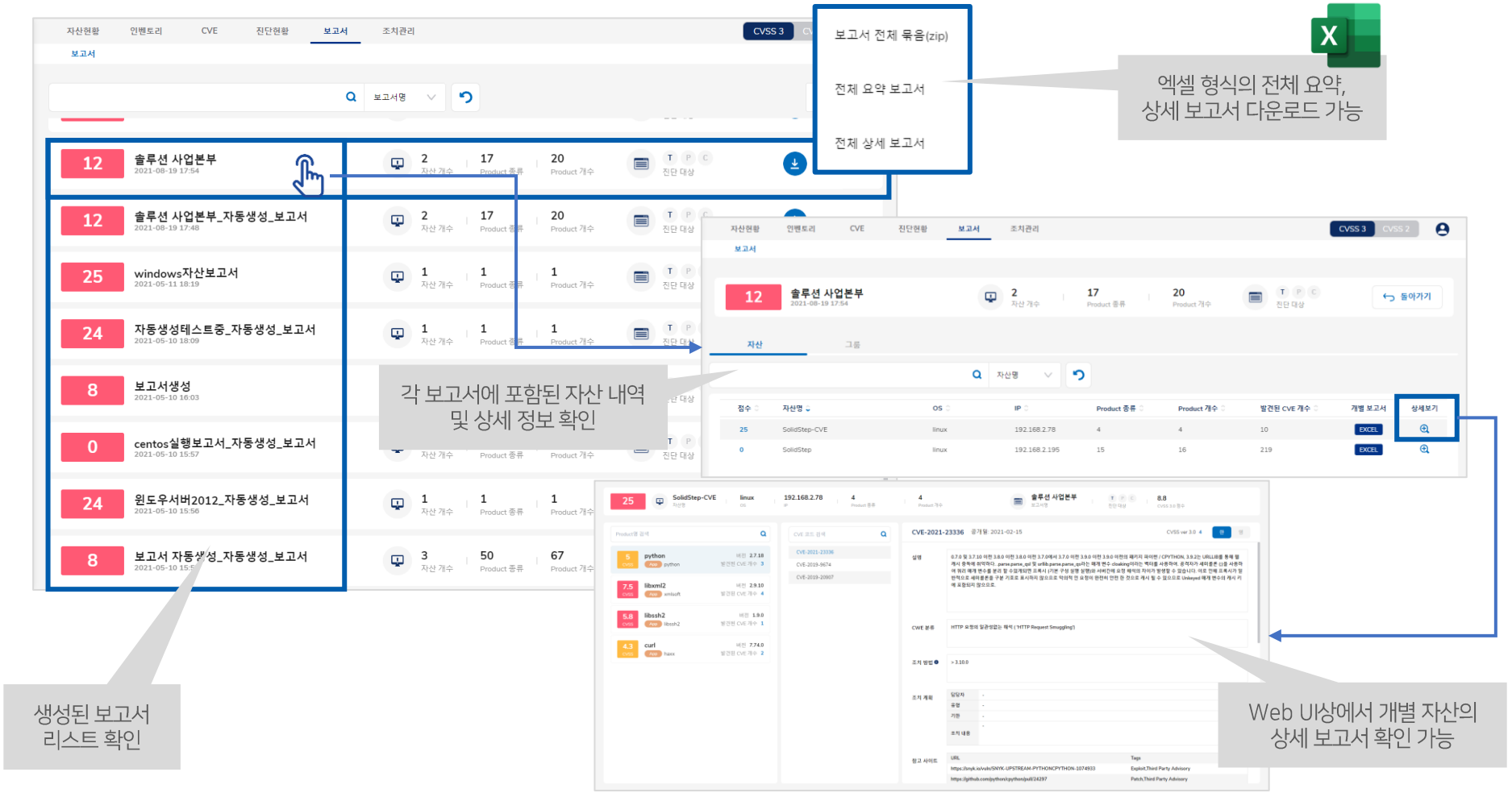
# 4. 인벤토리 관리 (2/2)

인벤토리별 CVE 취약점 항목에 대한 상세 내용을 확인할 수 있습니다.



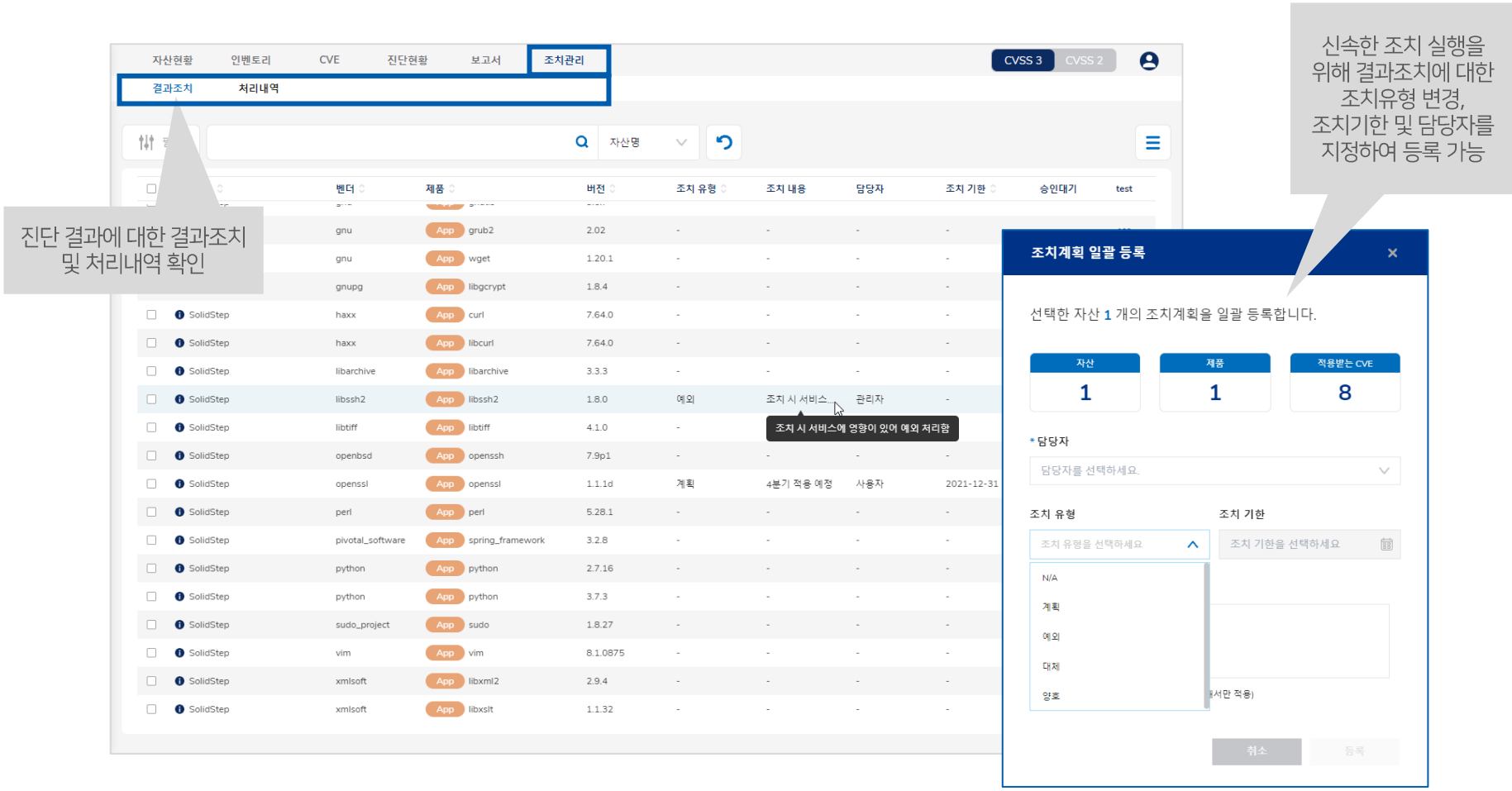
# 5. 상세한 진단 결과 보고서

취약점 진단 후 **생성된 보고서 확인 및 엑셀 파일**로 다운로드를 할 수 있습니다. 각 보고서를 클릭하면 **Web UI상에서** 해당 보고서의 자산 및 그룹정보, **개별 자산의 상세보기**가 가능합니다.



# 6. 신속한 조치 관리

진단 결과에 대한 **신속한 이행 조치를 위해 결과 조치** 기능을 제공합니다. 즉시 조치가 불가능하거나 장기적인 계획이 필요한 항목에 대해서는 사용자가 요청한(NA/계획/예외/대체/양호) 결과로 변경 가능하며, **항목별 담당자, 조치 기한 등의 지정**이 가능합니다.



SCAN ME

# 보안 취약점 진단 자동화 솔루션

Automatic Security Vulnerability Scanner

SolidStep CVE

www.ssrinc.co.kr

(주)에스에스알

Address. 서울특별시 구로구 디지털로 26길 111, 1606호 (구로동, JnK디지털타워)

TEL I 02.6240.6000 / FAX I 02.6959.0130 / 제품문의 I biz@ssrinc.co.kr