SSR Security Strategy Research

취약점 진단 자동화 솔루션

# SolidStep V2.5

Brain Beyond Brands

# CONTENTS

# I

## 취약점 (Vulnerability)

# 1. 취약점(Vulnerability) 이란?

취약점이란 **소프트웨어나 정보시스템 상에 존재하는 보안상의 결점**으로서 프로그램을 본래의 기능과 다르게 동작하게 하거나, 허용된 권한을 초과하여 사용할 수 있게 하거나, 의도하지 않은 오류를 일어나게 할 수 있는 조건들 입니다.


- ✓ 악의적 크래커의 침투
- ✓ 내부 비인가자 통제 어려움

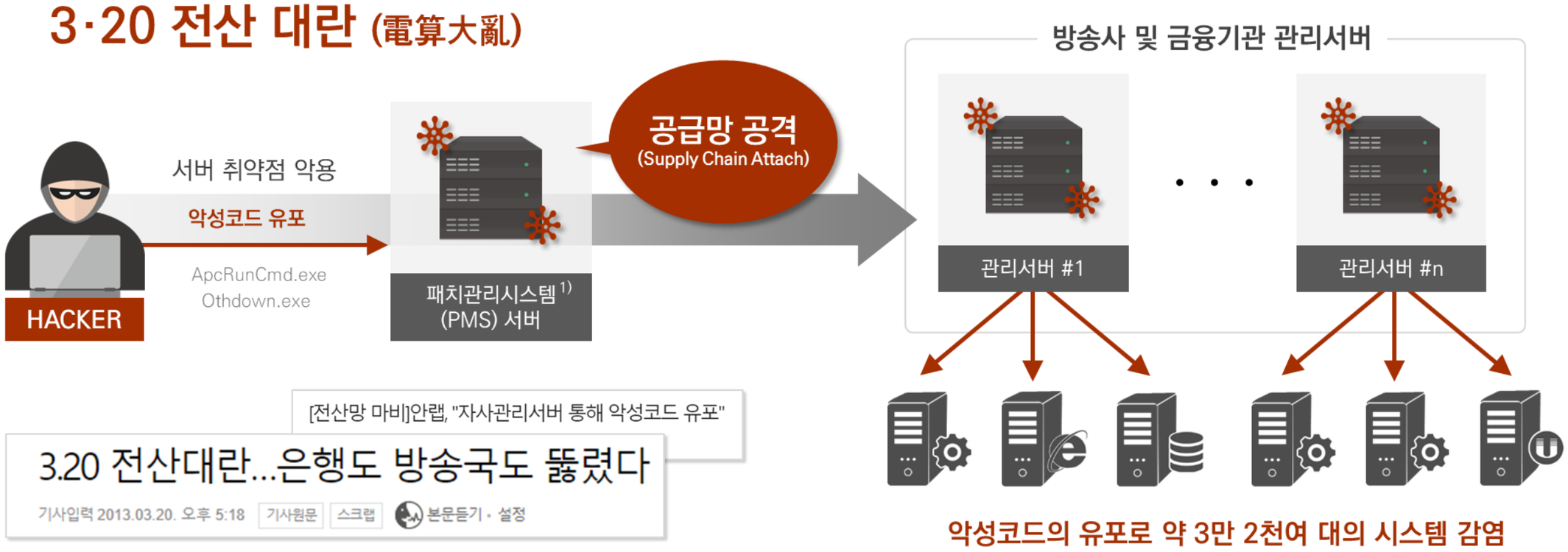
- ✓ 서비스 거부 공격 (DoS)
- ✓ 서비스 차단 (Interruption)

- ✓ 인사정보 및 기밀정보 유출

# 2. 취약점을 통한 해킹 피해사례

SolidStep

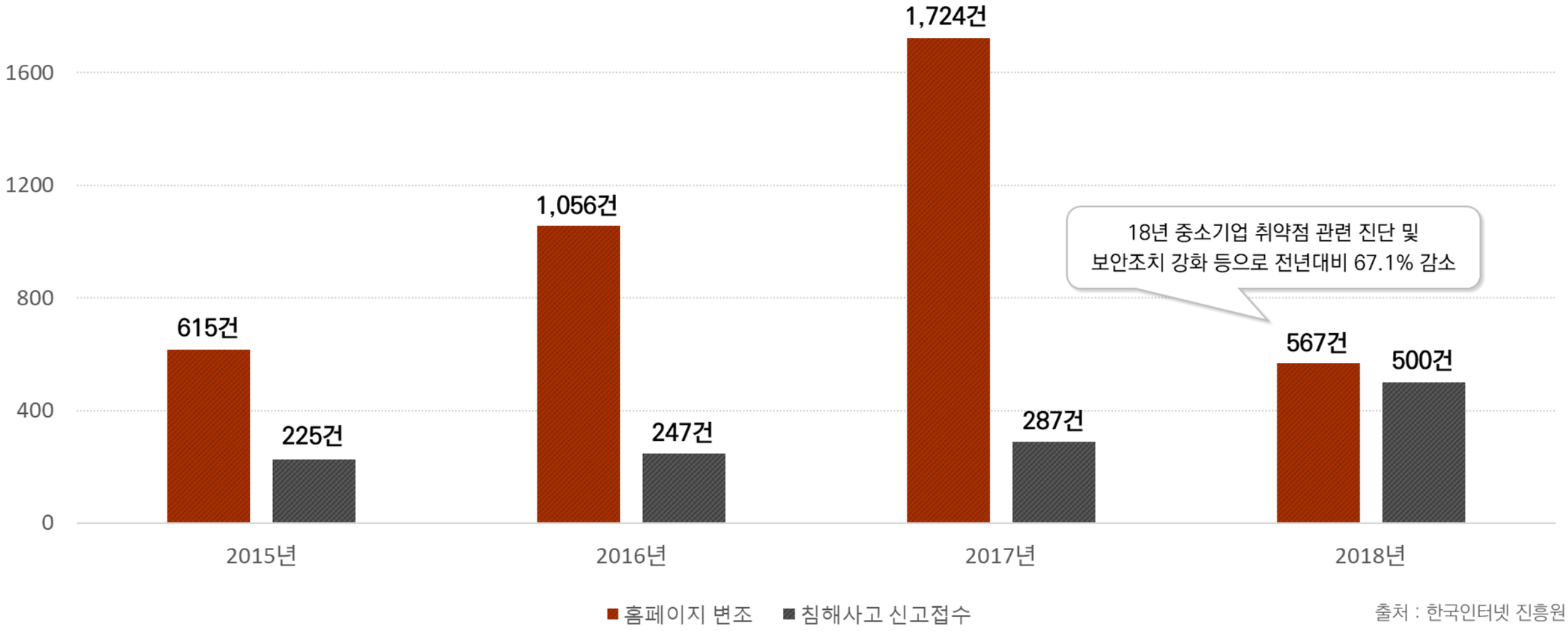
시스템의 취약점을 통한 악성코드의 배포로 2013년 3월 20일 대한민국의 주요 언론과 기업의 전산망이 마비되고, 수 만대의 컴퓨터가 악성코드에 감염되어 피해를 입은 사건이 발생했습니다.




1) 패치관리시스템(PMS) : 개별 PC의 소프트웨어 업데이트와 운영체제 패치 등을 관리하는 서버

# 3. 해킹 피해사고 건수

지속되는 해킹의 위협과 서비스 환경의 변화(보호 대상 영역의 확대)등에 따라 **취약점에 대한 이슈 및 피해 사례가 증가**하고 있으며, 취약점을 복합적으로 악용하여 악성코드를 유포시키는 방법이 지속될 것으로 전망됩니다.




출처 : 한국인터넷 진흥원

# 4. 취약점 관련 법령의 준수

취약점으로부터 발생하는 피해를 예방하기 위해 정보통신기반보호법, 전자금융감독규정 등 **정보보호 관련 법규 및 준수사항이 강화**되고 있으며, 운영 중인 내·외부 서비스는 정기적인 취약점 진단을 수행하도록 요구하고 있습니다.

## 정보통신기반보호법

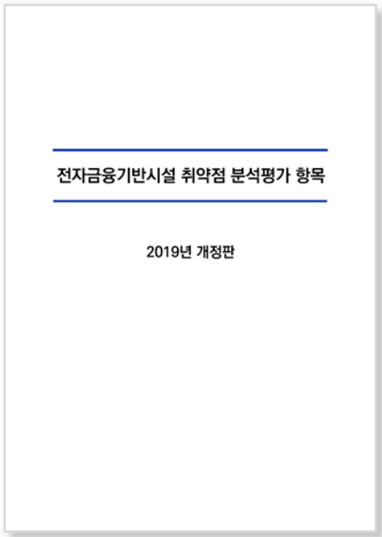
### 주요정보통신기반시설 기술적 취약점 분석·평가


- ✓ 관리기관의 장은 소관 정보통신기반시설이 주요정보통신기반시설로 지정된 때에는 지정 후 6월 이내에 법 제9조제1항의 규정에 의한 취약점의 분석 · 평가를 실시하여야 한다.
- ✓ 관리기관의 장은 제1항에 따라 소관 주요정보통신기반시설이 지정된 후 당해 주요정보통신기반시설에 대한 최초의 취약점 분석 · 평가를 한 후에는 매년 취약점의 분석 · 평가를 실시한다.

**주요정보통신기반시설은**
**매년 취약점 분석/평가를 실시하여야 함**

## 전자금융거래법

### 전자금융기반시설의 취약점 분석·평가




- ✓ 전자금융거래법 제21조3(전자금융기반시설의 취약점 분석, 평가) 1항
- ✓ 전자금융기반시설의 취약점 분석·평가는 총자산이 2조원 이상이고, 상시 종업원 수 300명 이상인 금융회사 또는 전자금융업자이거나 「수산업협동조합법」, 「산림조합법」, 「신용협동조합법」, 「상호저축은행법」 및 「새마을금고법」에 따른 중앙회의 경우 연 1회 이상 실시하여야 한다.

**전자금융기반시설은**
**매년 취약점 분석/평가를 실시하여야 함**

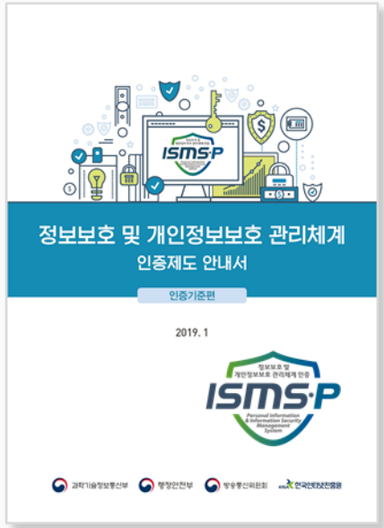
# 5. 정보보호 인증 컴플라이언스 준수

SolidStep

정보보호 및 개인정보보호 관리체계(ISMS-P) 및 정보보안경영시스템 등 다양한 인증 관리 시 내부 **정보시스템에 대한 상시적인 취약점 진단 및 조치를 요구**하고 있습니다.

## 정보보호 및 개인정보보호 관리체계 인증

### 2.11.2 취약점 진단 및 조치




- ✓ 정보시스템의 취약점이 노출되어 있는지를 확인하기 위하여 정기적으로 취약점 점검을 수행하고 발견된 취약점에 대해서는 신속하게 조치하여야 한다. 또한 최신 보안취약점의 발생 여부를 지속적으로 파악하고 정보시스템에 미치는 영향을 분석하여 조치하여야 한다.
- ✓ 개인정보 보호법 제29조(안전조치의무)
- ✓ 정보통신망법 제28조(개인정보의 보호조치)
- ✓ 개인정보의 안전성 확보조치 기준 제6조(접근통제)
- ✓ 개인정보의 기술적, 관리적 보호조치 기준 제4조 (접근 통제)

## 정보보안경영시스템(ISO/IEC27001)

### A.12.6.1 기술적 취약성 통제


- ✓ Management of technical vulnerabilities
- ✓ 12.6.1 사용 중인 정보 시스템의 기술적 취약성에 대한 정보를 시의 적절하게 확보하고, 조직이 그러한 취약성에 노출된 사례를 평가함으로써 관련 위험을 해결하기 위한 적절한 조치하여야 한다.
- ✓ 12.2.1 악성코드로부터 보호하기 위해 탐지, 예방 및 복구 통제를 이행하고 사용자가 적절히 인식할 수 있도록 한다.

# Ⅱ

# 취약점 진단 방식 및 개선방안

# 1. 취약점 진단의 유형

취약점의 진단 항목의 유형은 크게 **CCE, CVE, CWE** 등이 있으며, 국내에서는 자체적으로 개선이 가능한 **CCE, CWE 취약점 항목에 대해 법률적 통제(Compliance)로 의무화 및 조치를 권고**하고 있습니다.

Compliance

## CCE 취약점

(Common Configuration Enumeration)

사용자에게 허용된 권한 이상의 동작,
허용된 범위 이상의 정보 열람, 변조, 유출
등을 가능하게 하는 설정상의 취약점

**자체개선 가능**
(운영자 조치 가능)

**Infrastructure 취약점 진단**

IT Infra Configuration 진단
(OS, Network, DBMS, Web/Was, PC 등)

## CVE 취약점

(Common Vulnerabilities and Exposures)

컴퓨터 하드웨어 또는 소프트웨어의
결함이나 체계, 설계상의 허점

**자체개선 불가능**
(제조사 공식 패치 의존)

**Application 취약점 진단**

어플리케이션 취약점 진단
(Microsoft, Adobe, Open SSL, Java 등)

Compliance

## CWE 취약점

(Common Weakness Enumeration)

다양한 소프트웨어 언어(C, C++, Java 등)
뿐만 아니라 아키텍처, 디자인 설계, 코딩 등
개발 단계에서 발생 가능한 취약점

**자체개선 가능**
(개발자 수정 가능)

**Web 취약점 진단**

웹 서버의 소스 진단
(HTML, ASP, JSP, PHP 등)

## 기타 보안취약점

정보시스템의 위변조 감지,
개인정보 유출, 악성코드 및 피싱 위협,
모바일 보안 등의 취약점

**기타 취약점 진단**

컨설팅 수동진단, 모바일 보안진단 등
다양한 주요 정보시스템의 보안 취약점

# 2. 취약점 진단의 방법

SolidStep

대부분의 고객사에서는 **정보보호 컨설팅이나 내부 보안감사를 통한 연간 위험관리 활동** 또는 **솔루션 도입을 통해 취약점을 상시 관리하고 있으며,** 운영 중인 보안 조직의 인원 및 기술역량, 정보자산의 규모 등을 고려한 적절한 선택이 필요합니다.

## 1안. 정보보호 컨설팅

- ✓ 운영 중인 정보자산이 소규모(10대 미만)이거나,
- ✓ 매년 정보자산의 변동이 없는 경우
- ✓ 단기간에 높은 수준의 취약점 진단을 필요로 할 때
- ✓ 관리 인력의 부재로 내부 관리가 어려운 경우

| 구분 | 내 용 |
|---|---|
| 장점 | • 외부 컨설팅 전문가의 취약점 진단으로 높은 전문성<br>• 상세하고 세밀한 취약점 진단이 가능 |
| 단점 | • 1회성 진단으로 매번 비용이 소요<br>• 취약점의 조치 후 이행진단 필요 시 컨설턴트를 통한 추가 비용 발생<br>• 인력에 의한 작업으로 취약점 진단 과정 및 결과에 오류 발생 가능<br>• 컨설팅 전문가의 숙련도에 따라 진행 속도 및 결과 보고가 상이함 |

## 2안. 취약점진단 솔루션 도입

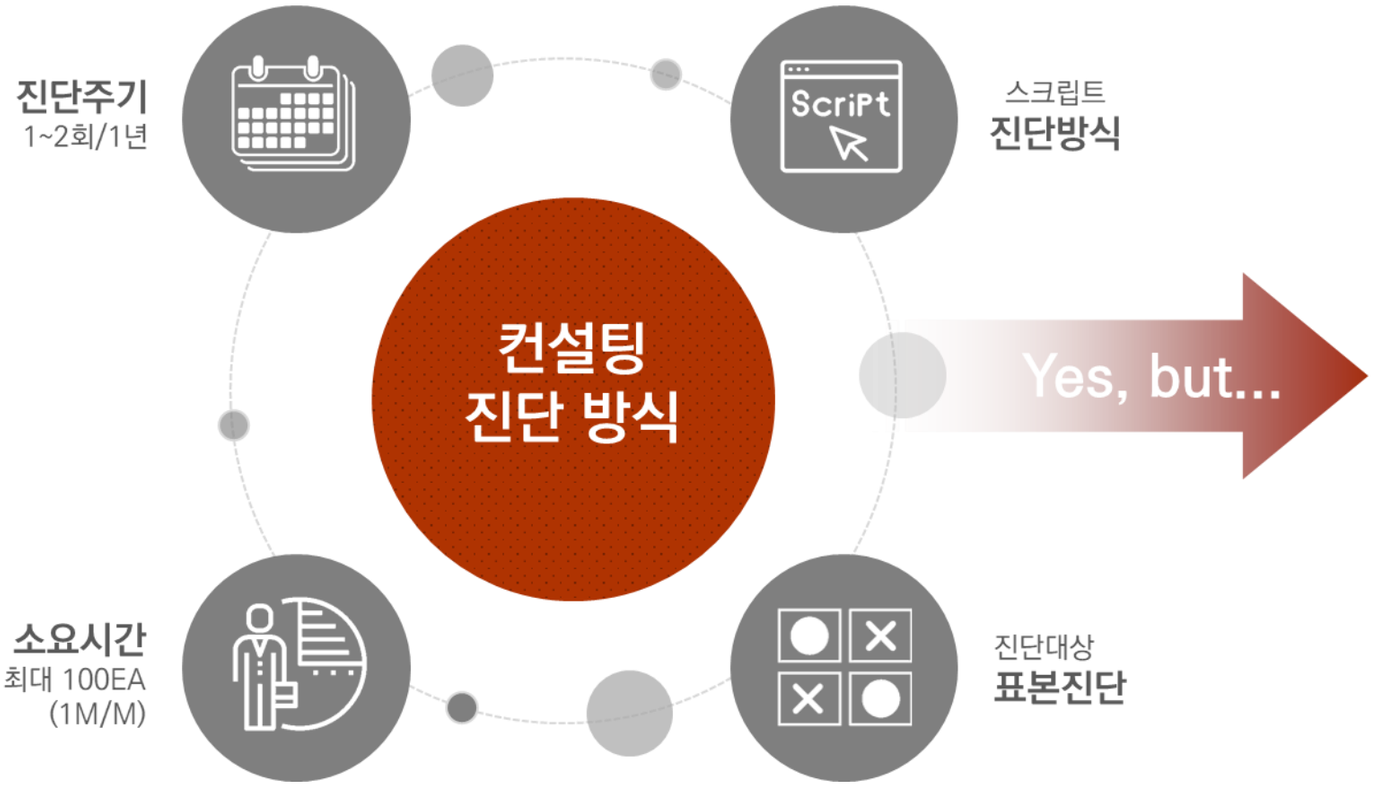

- ✓ 취약점 진단 대상 정보자산의 수가 많을 경우
- ✓ 지속적인 정보자산의 관리가 필요한 경우
- ✓ 상시적이며 즉각적인 취약점 진단 체계가 필요한 경우
- ✓ 매년 동일한 진단 수준의 유지 및 이력관리가 필요한 경우

| 구분 | 내 용 |
|---|---|
| 장점 | • 상시적인 취약점 진단이 가능하여 높은 보안성 유지<br>• 진단 대상 자산관리가 용이하며, 자산 변경 시 즉각적인 대응 가능<br>• 장기적인 관점에서 컨설팅 비용 대비 절감 효과(ROI) |
| 단점 | • 솔루션 도입의 초기 투자 비용이 컨설팅 대비 높음<br>• 취약점의 진단 결과에 대해 자체 판단 가능한 수준의 전문성 필요<br>• 컴플라이언스의 일부 개정 및 신설 시 즉각적인 대응이 어려움 |

# 3. 정보보호 컨설팅 방식의 한계

SolidStep

컨설팅를 통해 진행하는 취약점 진단은 비용과 기한의 문제로 **연간 1~2회 수행**하며, **스크립트를 통한 샘플링 진단**을 수행합니다. 진단의 주기와 방식 등에서 컨설팅 취약점 진단은 다양한 한계와 문제점이 발생합니다.




〈 THE CRITICAL POINT 〉

1. 취약점 진단 주기의 문제점
2. 취약점 진단 기한의 문제점
3. 취약점 진단 방식의 문제점
4. 취약점 진단 대상 선정의 문제점

# 3. 정보보호 컨설팅 방식의 한계 (계속)

SolidStep

정보보호 컨설팅을 통한 취약점 진단 방식은 **취약점 진단 주기에 따라** 추가, 변경되는 자산들의 취약점 진단이 어려우며, **컨설턴트의 역량에 따라** 진단 수량이 상이하고 정확한 소요 시간 예측 어려움 등의 한계점이 발생합니다.

## 진단 주기의 문제점


진단 후에 도입된 자산

⋮

내년까지 無 진단?

or

폐기 시까지 無 진단?

- ✓ 연간 1~2회 수행 주기 또는 1회성 진단으로 보안 연속성 확보 어려움
- ✓ 진단 후 발생하는 신규 도입 또는 자산 변경 시 취약점 진단 누락의 위험성
- ✓ 진단 후 발생하는 주요 설정 값의 변경에 대한 추적이 어려움
- ✓ 매회마다 컨설팅 비용이 소요되며, 취약점의 조치이행 점검 시 추가 비용 발생

## 진단 기한의 문제점


- ✓ 컨설턴트의 일정에 종속되어 정확한 기간 산정(WBS) 어려움
- ✓ 컨설턴트의 역량에 따라 1개월 최대 진단가능 자산 수 한정(최대 50~100대)
- ✓ 수 작업으로 인하여 자산 규모에 따라 결과산출 장기간 소요
- ✓ 투입 인력 변경 시 이력관리가 어려우며, 자산정보의 외부 유출 가능

# 3. 정보보호 컨설팅 방식의 한계 (계속)

SolidStep

정보보호 컨설팅을 통한 취약점 진단 방식은 **수작업으로 발생하는 다양한 문제점**과 중요 자산만 선정하여 취약점 진단을 수행하는 **표본진단으로 취약점 관리의 어려움**이 발생합니다.

## 진단 방식의 문제점

정보보호 컨설팅

**취약점의 수동 진단**

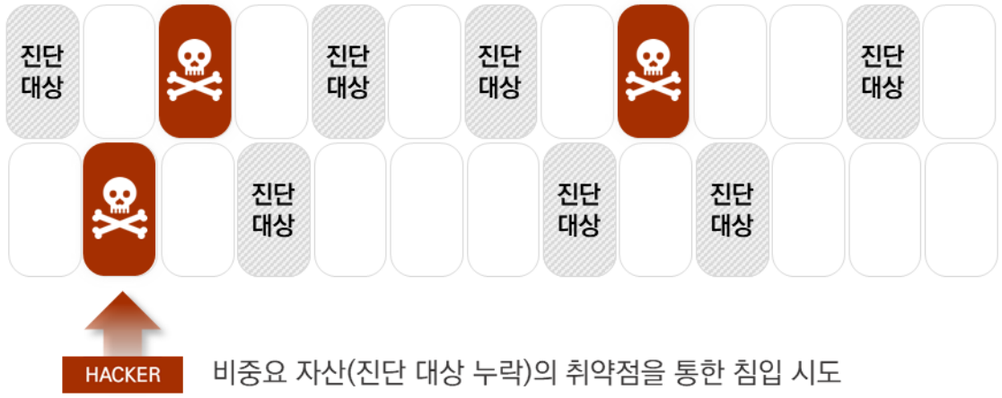
- ✓ 진단 대상의 설정 직접 확인
- ✓ 명령어를 통한 수동 진단

**보안담당자 인터뷰**

- ✓ 담당자에게 설문지 작성 요청
- ✓ 담당자와의 인터뷰를 통해 진단

- ✓ 암호화 되지않은 스크립트 방식으로 인해 데이터 관리의 문제 발생 가능
- ✓ 진단 대상의 관리자 계정 등의 자산정보 관리 문제(유출 등) 발생 가능
- ✓ 투입인력의 역량의 의존적으로 매회 진단 기준 및 분석, 조치 가이드 상이
- ✓ 사람에 의한 오탐·미탐 발생 가능

## 진단 대상 선정의 문제점




비중요 자산(진단 대상 누락)의 취약점을 통한 침입 시도

- ✓ 취약점 진단 비용과 투입 인력, 시간 등의 한계로 인한 매년 또는 매회 중요자산을 선정하여 취약점 진단 수행
- ✓ 자산의 중요도 변동 가능성이 낮아 매회 진단대상 중복 가능성 높음
- ✓ 비중요 자산(진단 대상 누락)의 취약점을 통해 침해사고 발생 가능성 높음

# 4. 취약점 진단 자동화 솔루션의 필요성

취약점 진단 자동화 솔루션 도입 시 정보보호 컨설팅의 다양한 한계점을 보완하고, **취약점에 대한 신속하고 정확한 대응** 및 **취약점 분석평가 현황의 체계적인 관리**를 제공합니다.

보안담당자

- ✓ 추가, 변경되는 컴플라이언스에 빠른 대응 방법은?
- ✓ 보안 현황을 간단하고 신속하게 파악할 수 있는 방법은?
- ✓ 잘못된 시스템 설정으로 인한 문제점 해결 방법은?
- ✓ 매년 아웃소싱하는 컨설팅 비용을 절감하는 방법은?

Solution

## 취약점 진단 자동화 솔루션

# Ⅲ

# 취약점 진단 자동화 솔루션

## - SolidStep -

# 1. SolidStep 개요

SolidStep은 다양한 플랫폼 환경의 시스템 자산을 대상으로 **국내 · 외 법령 및 규제(컴플라이언스)를 준수하기 위해 컨설팅과 동일한 수준의 취약점 진단을 수행하는 자동화 솔루션**입니다.

## 취약점 진단 대상

OS, DBMS, WEB, WAS, Network 등
다양한 플랫폼 환경의 취약점 진단 지원

Server WEB/WAS DBMS Network PC

## 취약점 진단 기준

국내 · 외 법령 및 규제(컴플라이언스)
준수를 위한 취약점 진단 기준 항목 대응


## 취약점 진단 범위

운영 중인 시스템 자산의 다양한 영역을
보안 컨설팅과 동일한 수준으로 취약점 진단

파일 및 디렉토리 관리 | 계정 관리 | 로그 관리 | 접근 관리 | 서비스 관리 | 패치 관리 | 보안 관리

## 취약점 진단 방식

시스템 운영 환경 및 플랫폼의 특성을 고려한
다양한 취약점 진단 방식 지원

Online
- ✓ Agent
- ✓ Agentless

Offline
- ✓ 수동진단
- ✓ Portable

# 2. SolidStep 지원 플랫폼

SolidStep은 운영 중인 시스템 환경의 다양한 **OS, DBMS, WEB/WAS, Network 등 50개 이상 플랫폼의 취약점 진단을 제공**합니다.

| 플랫폼 구분 | 상세 내역 | 비 고 |
|---|---|---|
| OS | • Windows<br>– 서버계열 : 2003/2003 R2/2008/2008 R2/2012/2016<br>– PC계열 : 7/8/10<br>• Linux(Cent OS, OpenSUSE, Ubuntu, Fedora, Oracle Linux)<br>• Unix(HP-UX, AIX, Solaris) | |
| DBMS | • Oracle, MSSQL, MySQL, DB2, SYBASE, Tibero, Altibase, Postgres SQL, Maria DB, Vertica, Cubrid, HANA DB, Mongo DB 등 | |
| WEB | • Apache, IIS, WebtoB, Oracle Http Server, IBM Http Server 등 | |
| WAS | • Tomcat, WebLogic, iPlanet, Jeus, WebSphere, Nginx, Jboss, Resin, Jrun, Jetty 등 | |
| Network | • Cisco, Juniper, HP(3Com), Alteon, Alcatel, Extreme, AVAYA, Brocade, ubQuoss, PIOLINK, A10, Citrix, Huawei, HanDreamnet, DELL, Arista, F5, DASAN 등 | |
| 기타 | • RHEV | |

※ 신규 플랫폼에 대한 지속적인 개발 및 지원

# 3. SolidStep 진단 기준

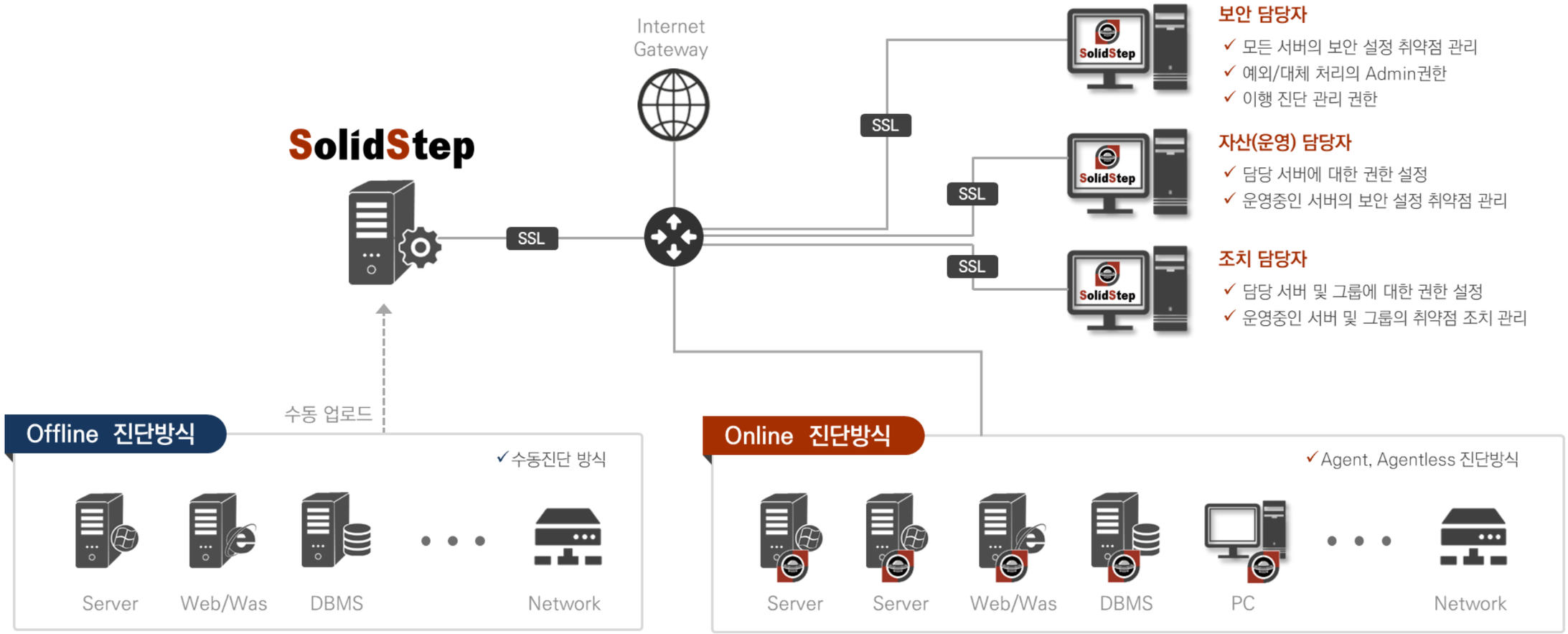
취약점 진단 시 정보통신기반보호법, 전자금융거래법, 정보보호관리체계, 개인정보관리체계 등에서 법률적 통제를 의무화하는 **인프라 환경의 취약점 진단 항목을 100% 지원**하며, 내부 보안가이드에 따른 **진단 항목 커스터마이징**을 지원합니다.

| 플랫폼 구분 | 진단 대상 | | | | | | 비 고 |
|---|---|---|---|---|---|---|---|
| | Server | DBMS | WEB/WAS | Network | PC | Total | |
| 금융위원회 기준항목 | 154 | 87 | 26 | 440 | - | 707 | 산업통산자원부, 교육부, 국방부 등 다양한 기관의 취약점 진단 항목 지원 |
| 주요정보통신기반시설 기준항목 | 128 | 120 | 27 | 152 | 20 | 447 | |
| ISMS-P | 87 | 119 | 135 | 38 | - | 379 | |
| 기타 지원 항목 | 626 | 414 | 171 | 394 | 18 | 1,623 | |
| SSR Standard Template (합계) | 995 | 740 | 359 | 1,024 | 38 | 3,156 | |

※ 신규 및 변경 컴플라이언스에 대한 지속적인 업데이트 지원

# 4. SolidStep 시스템 구성도

SolidStep 구축 시 운영 중인 네트워크 구성 환경을 분석하여 **솔루션의 안정적인 성능과 보안성**, Agent가 설치되는 **정보자산(서버)의 영향력 등을 고려**하여 최적화 된 시스템을 구성합니다.



# 5. SolidStep 특장점

SolidStep은 **정보보호 전문서비스 업체인 자사가 직접 개발한 보안 솔루션**으로 다양한 국내 기관 및 업체의 BMT, POC 결과 우수한 평가를 받은 객관적인 솔루션이며, **타사의 솔루션과 업체 역량, 기술력 등에서 비교되는 검증된 솔루션**입니다.

## 국내 1위, 검증된 취약점 진단 자동화 솔루션

### ☑ 정보보호 전문서비스 업체가 직접 개발한 보안 솔루션

- 기술/관리 컨설팅의 노하우가 집약되어, 취약점 진단에 최적화된 자동화 솔루션

### ☑ CCE 취약점 진단 솔루션 부분 국내 1위

- 취약점 진단 솔루션 부분의 조달구매율 3년 연속 1위(2016 ~ 2018년 조달 구매 기준)
- 국내 시장점유율 80% 이상 고객사 보유

### ☑ 완벽한 컴플라이언스 대응

- 국내, 외 기준을 만족하는 1,000개 이상의 보안진단 항목 진단 기능
- 취약점 항목의 커스터마이징으로 내부 보안지침을 반영한 취약점 진단

### ☑ 취약점 진단에 최적화된 아키텍처 구조

- 정보 수집(Agent) / 분석(Manager) 을 분리 수행하여 취약점 진단 시 안정적인 서비스 운영
- 컨설턴트(인력) 대비 28,800배 빠른 진단 속도(인력 수행 시 100대 1M/M)

# 5. SolidStep 특장점 : ① 제조사의 기술력

SolidStep은 **보안 솔루션 개발/구축과 정보보호 기술/관리컨설팅 서비스**를 제공하고 있으며, 컨설턴트를 통해 수집된 취약점 진단 항목의 즉각적인 반영과 개발부서의 강도 높은 테스트를 거쳐 지속적인 업데이트 및 솔루션을 개발하고 있습니다.

## 보안 솔루션 개발/구축

SolidStep
취약점 진단 자동화 솔루션

MetiEye
실시간 웹쉘 탐지 솔루션

MudFix
악성 이메일 모의훈련 솔루션

SeedCrock
보안취약점 통합관리 솔루션

BlackVoice
보이스 피싱 탐지 서비스

## 관리컨설팅

ISMS-P 인증컨설팅

ISO27001 인증컨설팅

기반시설 취약점 분석/평가

금융기관 취약점 분석/평가

- 정보보호 관리체계(국내, 외)
- 전자금융기반시설 점검
- 주요정보통신기반시설 점검
- 개인정보 영향평가
- 개인정보보호 컨설팅

## 기술컨설팅

모의해킹

서비스 보안점검

정보자산 보안점검

- 침투 성공률 100%
- 웹, 모바일, C/S 취약점 점검
- 인프라 시스템 보안점검
- 악성 이메일 모의 점검 서비스
- 소스코드, 리버스 엔지니어링
- 정보보호시스템 취약점 점검
- 침해사고 분석 서비스

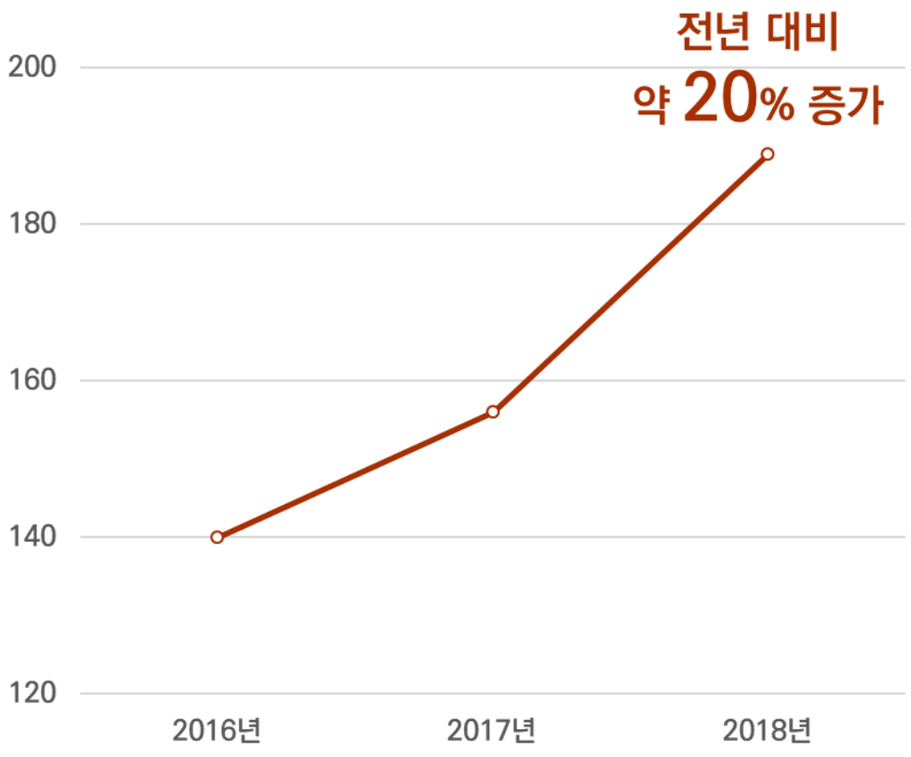
# 5. SolidStep 특장점 : ② 시장 점유율

SolidStep은 다양한 공공기관, 금융권, 기업 등에 구축되어 안정적으로 운영되고 있는 솔루션으로 매년 경쟁사가 늘어남에도 **CCE 취약점 진단 솔루션 분야 조달구매율 1순위** 유지 및 매출 금액이 증가하고 있습니다.

## 조달 구매율 (출처 : 조달정보개방포털)

| 솔루션 제조사 | 2018년 조달 구매 | |
|---|---|---|
| | 금액(원) | 점유율 |
| 에스에스알 | 2,379,257,600 | 77.4 % |
| N 사 | 207,000,000 | 6.7 % |
| L 사 | 10,800,000 | 0.4 % |
| 기타 | 477,719,000 | 15.5 % |
| 합 계 | 3,074,776,600 | 100 % |

## 레퍼런스 현황 (단위 : SolidStep 고객사 수)



# 5. SolidStep 특장점 : ③ 컴플라이언스 완벽 대응

SolidStep

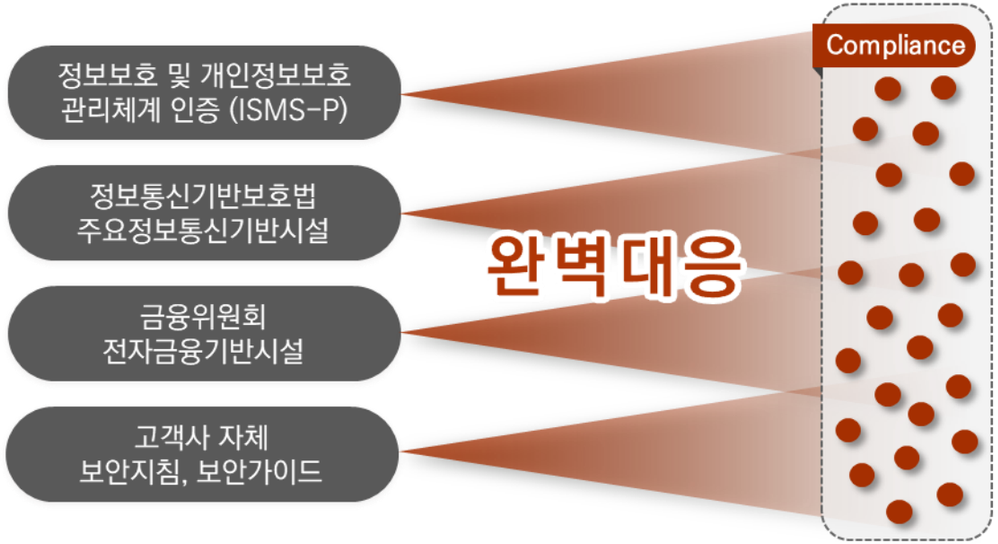
SolidStep은 정보통신기반보호법, 전자금융거래법, 정보보호관리체계, 개인정보관리체계 등에서 법률적 통제를 의무화하는 **인프라 환경의 취약점 진단 항목을 100% 지원**하며, 내부 보안가이드에 따른 **진단 항목 커스터마이징**이 가능합니다.

### 〈 기존 취약점 진단 솔루션 〉


- ✓ 대외적으로 알려진 항목(내부 환경과 큰 차이점이 존재)에 대해서만 취약점 진단
- ✓ 대부분 외국 기준으로 진단하여 국내환경 적용이 미흡하거나 즉각적인 업데이트 불가
- ✓ 정보보호 컨설팅을 대체할 만큼의 수준으로 취약점 진단이 불가

VS

### SolidStep




- ✓ 취약점 관련 법률 및 컴플라이언스 항목은 반드시 포함하여 취약점 진단
- ✓ 다양한 진단 방식으로 폐쇄망 및 망 연계 시스템 환경 등의 취약점 진단
- ✓ 정보보호 컨설팅을 대체할 만큼의 수준(다양한 보고서 제공)으로 취약점 진단

# 5. SolidStep 특장점 : ④ 취약점 진단 최적화 아키텍처

SolidStep

SolidStep은 **취약점 진단에 최적화된 솔루션 아키텍처 구조**로 진단 대상 시스템에 대한 **영향력을 최소화**하여 취약점 진단 시 시스템의 안정성 및 취약점 진단 데이터의 보안성을 보장합니다.


**Online 방식 (with Agent)**

- Install-Free
  - Portable (설치 불필요)
- OS Free
  - Windows, Linux, Unix 등 5종 지원
- Resource Free
  - CPU 소모량 1% 이하
- ACL Free
  - Agent Port Listening 없음
  - HTTPS Protocol 이용

**Online 방식 (Agentless)**

- SSH, Winexec를 이용한 진단
  - Agent 방식과 동일한 분석 결과 보장
  - 서버 접속정보 입력 및 관리 필요, 네트워크 접근 ACL필요
  - 부가기능(리소스 모니터링 등) 이용불가, 예약진단 이용불가

**Offline 방식 (수동진단)**

- 스크립트를 통해 암호화된 정보 수집 및 수동 등록 후 취약점 진단 수행

# 6. 솔루션 라인업

취약점 진단 자동화 솔루션 SolidStep은 서버 및 네트워크 장비의 취약점을 진단하는 **SolidStep**, 단독형으로 어플라이언스 구축이 필요 없는 **SolidStep Portable**, 취약점 진단 핵심기술을 PC에 적용한 **SolidStep for PC**로 구성되어 있습니다.

## SolidStep

SolidStep

최첨단 보안진단 솔루션으로 모든 IT 자산의
**보안 진단을 상시적으로 자동 수행**하는
취약점 진단 자동화 솔루션입니다.

- ✓ CC 및 GS 인증 획득 솔루션
- ✓ 국내 컴플라이언스에 대해 완벽 대응
- ✓ 진단 항목 커스터마이징으로 내부정책 진단 최적화
- ✓ 신속한 자동화 전수 진단 및 다양한 진단 옵션 제공
- ✓ 주요 설정 값에 대한 변경 감시 및 미등록 자산 관리
- ✓ 컨설턴트가 직접 작성한 수준의 결과보고서 제공

## SolidStep Portable

SolidStep portable

SolidStep을 **어플라이언스-FREE**로
개발하여 **폐쇄망 구간**에서 오프라인으로
취약점 진단이 가능한 솔루션

- ✓ 단독형으로 관리서버 없이 취약점 진단 수행
- ✓ 솔루션을 통해 진단대상 자산의 보안현황 제공
- ✓ 취약점 진단부터 진단결과 및 취약점에 대한 상세 조치가이드 제공
- ✓ 직관적인 UI로 취약점 진단 관리의 편의성 제공
- ✓ Windows OS 서버 진단 지원

## SolidStep for PC

SolidStep for PC

변경감시 기능과 보안정책을 통해
보안수준을 향상시킬 수 있는 SolidStep의
**취약점 진단 핵심기술을 PC에 적용**한 솔루션

- ✓ SolidStep의 모든 취약점 진단 기능을 PC에 적용
- ✓ 솔루션을 통해 진단대상 자산의 보안현황 제공
- ✓ 취약점 진단부터 진단결과 및 취약점에 대한 상세 조치가이드 제공
- ✓ 변경감시 기능 및 개인정보 탐지 기능 제공
- ✓ Windows OS PC 취약점 진단 지원

# 7. 솔루션 도입 기대효과

취약점 진단 자동화 솔루션 SolidStep은 인프라 시스템에 대한 취약점 관리 업무 연속성 확보, 상시 취약점 진단, 분석, 조치, 이력 관리 등 **자동화된 취약점 관리체계의 구축**을 지원합니다.

## " 취약점 분석평가 현황의 체계적인 관리 및 정량화 "


### 01 컴플라이언스(법/규정) 완벽 대응

- 대내·외 컴플라이언스 및 보안 가이드 대응을 통한 침해사고 예방
- 주요정보통신기반시설 및 금융보안원, 전자금융감독규정 등 다양한 국내 컴플라이언스 기준 보안취약점 진단요건 대응
- 취약점 진단 항목의 커스터마이징으로 고객사 보안지침(가이드) 및 내부감사 대응

### 02 취약점 관리 업무의 프로세스 개선

- 취약점 진단 및 조치이행 현황 등 실시간 모니터링 체계 구축
- 취약점 분석·평가 및 위험평가의 객관적 지표 활용
- 상시적인 취약점 진단을 통한 보안 취약점 집중 관리
- 자율 진단을 통한 취약점 진단 소요기간 최소화

### 03 보안규정 강화 및 보안체계의 고도화

- 취약점 조치에 대한 이행 여부 확인(조치, 예외처리 등)
- 운영 시스템의 가용성, 신뢰성, 안정성 확보
- 중요 정보에 대한 기밀성 및 무결성 보장
- 자산의 균일한 보안 수준 유지 및 상향 평준화 확립

### 04 업무의 효율성 증대 및 관리비용 감소

- 보안담당자의 기술 내재화로 운영관리의 효율성 및 관리업무의 전문성 증대
- 취약점 진단을 컨설팅에서 솔루션으로 대체하여 진단 비용 절감
- 중요 정보의 유출 방지를 통한 손실비용 감소

# 8. 솔루션 레퍼런스

SolidStep은 다수의 공공기관 및 금융기관, 기업 등에 구축되어 안정적으로 운영되고 있으며, 단일 사업 최대규모의 설치 운영 레퍼런스를 보유하고 있습니다.

| | |
|---|---|
| 정부 부처 | 국가보훈처, 식품의약품안전처, 한국원자력안전위원회, 교육부(KORUS), 문화체육관광부, 보건복지부 사이버안전센터 |
| 공공기관 | 대법원, 전파연구원, 주택도시보증공사, 한국환경공단, 특허청, 한국도로공사, 부산항만공사, 국민연금공단, 한국공항공사, 경상북도개발공사, 한국토지주택공사, 한국석유공사, 국가평생교육진흥원, 한국원자력환경공단, 한국문화진흥원, 기술보증기금, 농업기술실용화재단, 한국인터넷진흥원, 게임물관리위원회, 한국재정정보원, 항국신용정보원, 한국항공우주연구원, 한국건설기술연구원, 국가평생교육진흥원 금융감독원, 보험개발원, 한국예탁결제원, 한국교육개발원, 부산시교육청, 한국교육학술정보원 |
| 지자체 | 평택시청, 성남시청, 구리시청, 연천군청, 함안군청, 고성군청, 영월군청, 창녕군청, 남해군청, 전라남도청, 울주군청, 안성시청, 진주시청, 세종특별자치시, 통영시청, 제주도청, 서귀포시, 구리시 교통정보센터, 제주도 자치경찰단 교통정보센터(ITS), 제주시청, 하동군청, 양주시청 |
| 국방 | 사이버사령부, 기무사령부, 방위사업청, 해병대사령부, 국방기술품질원, SEC연구소, 국방과학연구소, 한국국방연구원, 군사안보지원사령부, 육군제2작전사령부 |
| 공기업 | 한국전력공사, 한국동서발전, 한국중부발전, 한국남부발전, 한국남동발전, 한국수력원자력, 한전KDN, 강원랜드, 청주국제공항 |
| 교육/병원 | 국립암센터, 서울과학기술대학교, 강원대학교, 신라대학교, 울산과학기술대학교, 경상대학교, 울산대학교, 전국교육대학교, 제주국제학교, 울산과학기술원, 의료기관인증평가원, 울산교육연구정보원 |

# 8. 솔루션 레퍼런스 (계속)

SolidStep은 다수의 공공기관 및 금융기관, 기업 등에 구축되어 안정적으로 운영되고 있으며, 단일 사업 최대규모의 설치 운영 레퍼런스를 보유하고 있습니다.

| | |
|---|---|
| 금융(은행) | 페퍼저축은행, 신한은행, 국민은행, IBK기업은행, 우리은행, BNK경남은행, MG새마을금고, 신용협동조합(신협중앙회) |
| 금융(보험) | 미래에셋생명보험, DGB 생명보험, KB생명보험, 한화생명보험, 오렌지라이프생명보험, 흥국생명보험, 신한생명보험, NH농협생명보험, 교보생명보험, 롯데손해보험, 메리츠화재보험, NH농협손해보험, 한화손해보험, KB손해보험, 캐롯손해보험 |
| 금융(증권) | 유안타증권, 신한금융투자, 한화투자증권, DB금융투자, 한국증권금융, 키움증권 |
| 금융(카드) | 비씨카드, 우리카드, 롯데카드 |
| 금융 (저축은행 / 기타) | SBI저축은행, 웰컴저축은행, 신한캐피탈, 세틀뱅크, 스마트로, KG이니시스, KG모빌리언스, 브이피, 하나금융티아이, 에이앤디신용정보, 서울외국환중개, 세틀뱅크, |
| 기업 | 현대기아차, 현대오토에버, 현대기아차(북미법인), 현대기아차(유럽법인), 현대모비스, 현대위아, SK Telecom, SK 브로드밴드, SK네트웍스 SK C&C, SK하이닉스, SK건설, SK E&S, LGU+, LG화학, LG생활건강, KT, KT 뮤직, KT DS, 대한항공, 아시아나항공, 한화S&C, 대림B&CO, 삼성전자로지텍, 안랩, 한성자동차, 인터파크, CJ오쇼핑, 롯데백화점, 녹십자헬스케어, 코웨이, 골프존, 에스오일, 이수그룹 , 코오롱베니트, 나이스정보통신, 한국정보통신, 한국케이블텔레콤, 서울반도체, 한국통신사업자연합회, 청주공항, 시스템아이씨, 삼성전자 구미사업장, 서브원 |

# Ⅳ

# 주요 기능

# 1. SolidStep 주요기능

SolidStep

SolidStep은 다양한 보안 **컴플라이언스(정책)를 적용**하여 취약점 진단을 수행하고, 정보보호 담당자에게 취약점 정보를 전달하여 해당 **취약점 관리에 대한 종합적인 업무환경을 제공**하며, **관리업무의 일원화 및 체계적인 운영을 지원**합니다.

## 자산 관리

- ✓ 인프라 자산 관리
- ✓ 다양한 그룹 관리
- ✓ 자산의 상세정보 관리
- ✓ 미등록 자산 관리
- ✓ 자산 담당자 지정 관리

**자산 관리 기능**

Excel 데이터 자산 등록, 미등록 자산 관리 등

## 취약점 진단

- ✓ Online, Offline 방식 진단
- ✓ 진단 수행 및 결과 수집
- ✓ 취약점 조치
- ✓ 취약 항목 맞춤화 관리
- ✓ 이행점검

**취약점 진단 수행**

Agent, Agentless, 수동진단

## 현황 관리

- ✓ 자산별, 그룹별 현황
- ✓ 결과 비교 관리
- ✓ 진단이력 현황 관리
- ✓ 조치계획 및 완료 현황
- ✓ 설정 값 변경감시

**취약점 분석 현황 및 통계**

자산/그룹별 보안 점수 및 통계 제공

## 시스템 관리

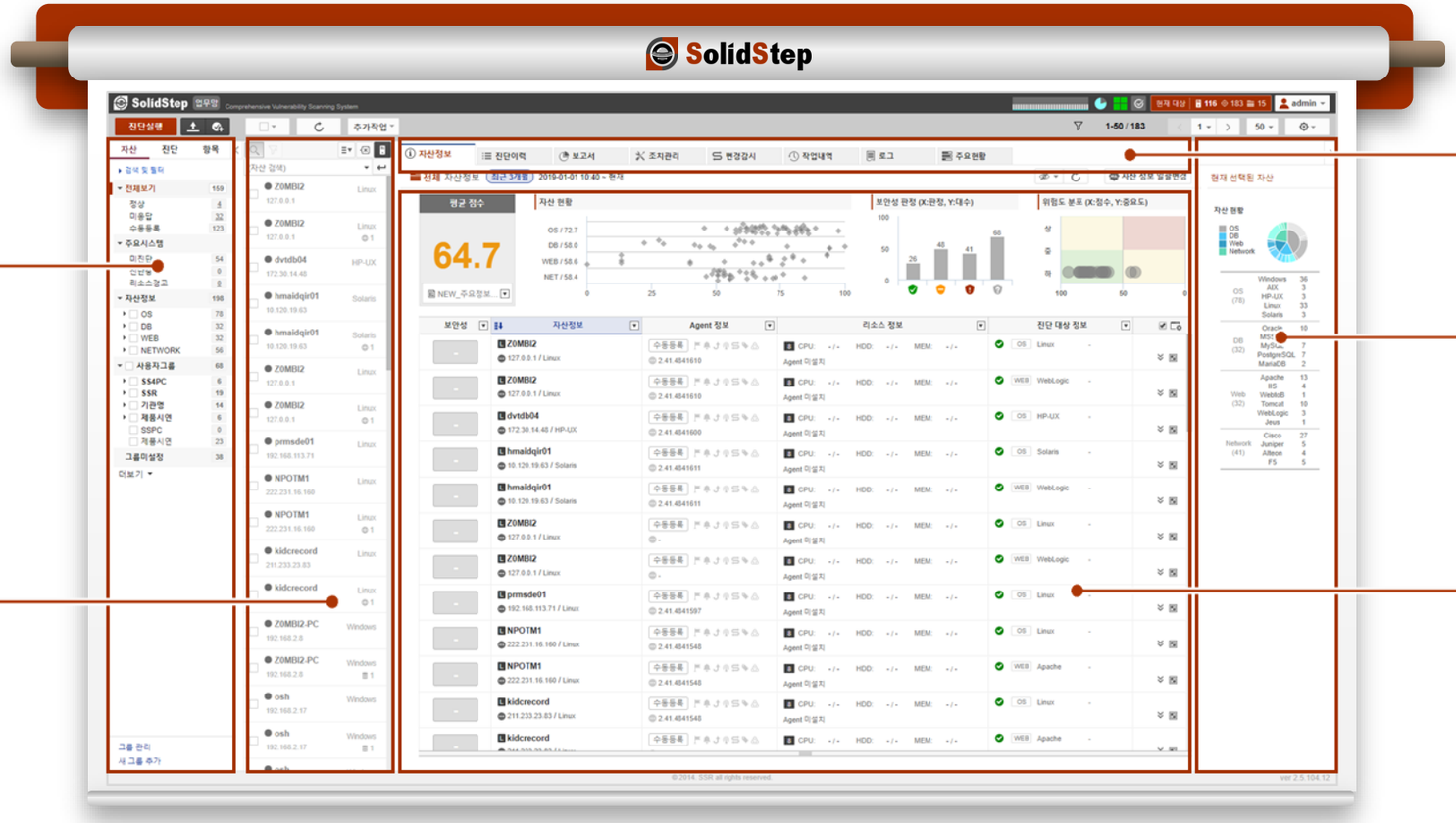
- ✓ 사용자 관리
- ✓ 접근 제어
- ✓ 권한 관리
- ✓ 컴플라이언스(정책) 관리
- ✓ 로그 관리

**시스템 관리 기능**

사용자 계정관리 및 API 제공

# 2. SolidStep – UI 구성

사용자 접근성 및 편의성을 고려한 Web UI 방식의 관리화면으로 전체 자산에 대한 보안 현황 및 자산정보, 진단이력, 보고서, 조치관리, 변경감시, 작업내역, 로그 등 다양한 관리 기능을 제공합니다.

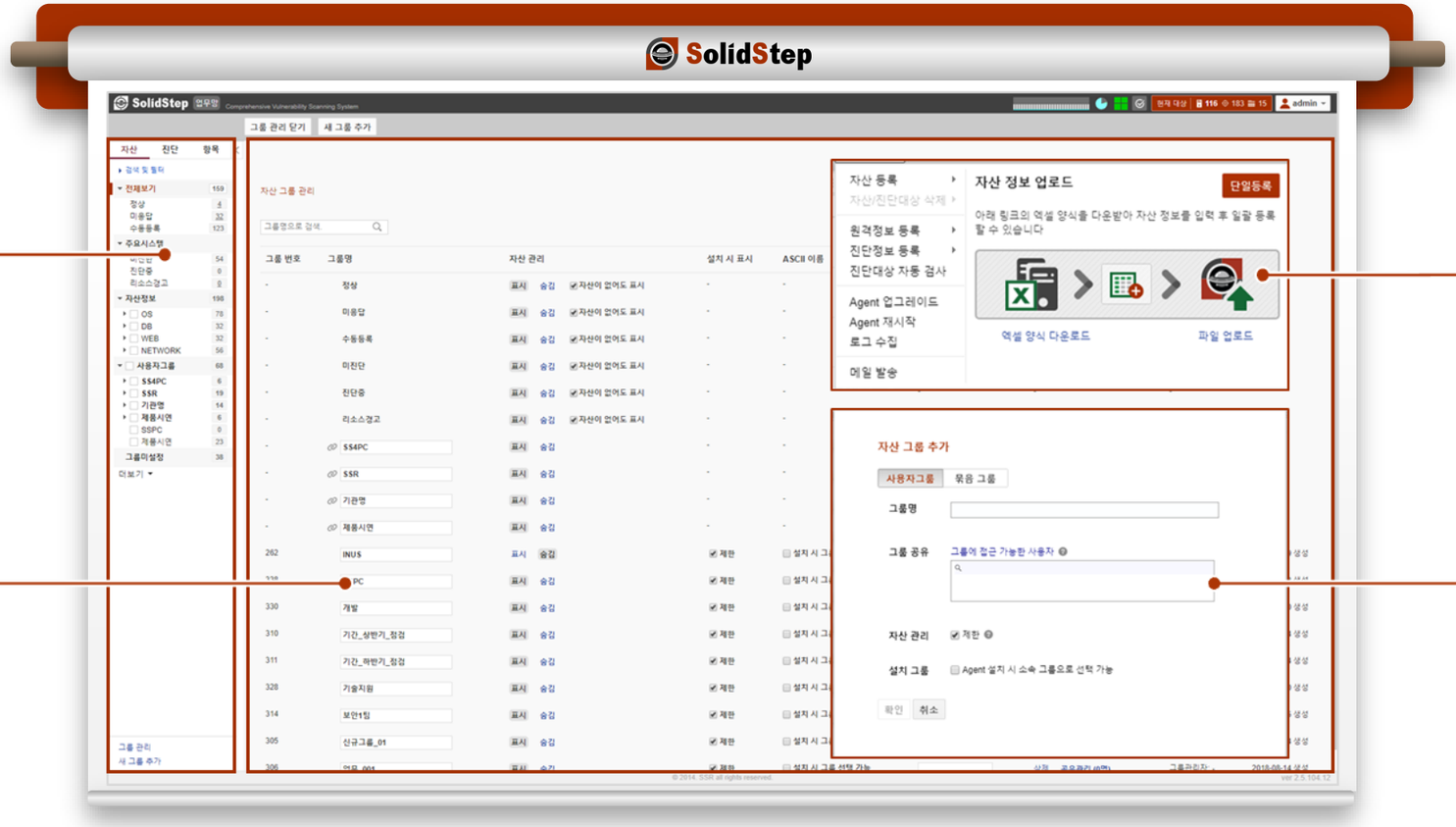



- ✓ 그룹, 진단, 항목 탭으로 구성
- ✓ 각 탭 선택 시 해당 탭의 내용 확인가능
- ✓ 선택된 탭의 해당하는 자산 목록
- ✓ 다양한 관리기능 제공
- ✓ 선택된 그룹, 진단, 항목 탭의 플랫폼별 수량 확인
- ✓ 선택된 대상에 대한 평균점수, 자산별 점수 분포, 위험도 분포, 플랫폼별 수량 등 다양한 통계 및 현황에 대한 대시보드 제공

# 2. SolidStep – 자산관리

SolidStep

물리적, 논리적 그룹화 관리를 지원하며, 자산별, 운영 부서별 다양한 그룹핑을 설정하여 관리자/사용자별 접근 권한 관리 기능을 제공합니다.




✓ 자산 탭에서 그룹관리 및 새 그룹 추가 가능

✓ 자산 그룹 관리 메뉴에서 그룹명 변경, 자산 표시/숨김 등의 관리 기능 제공

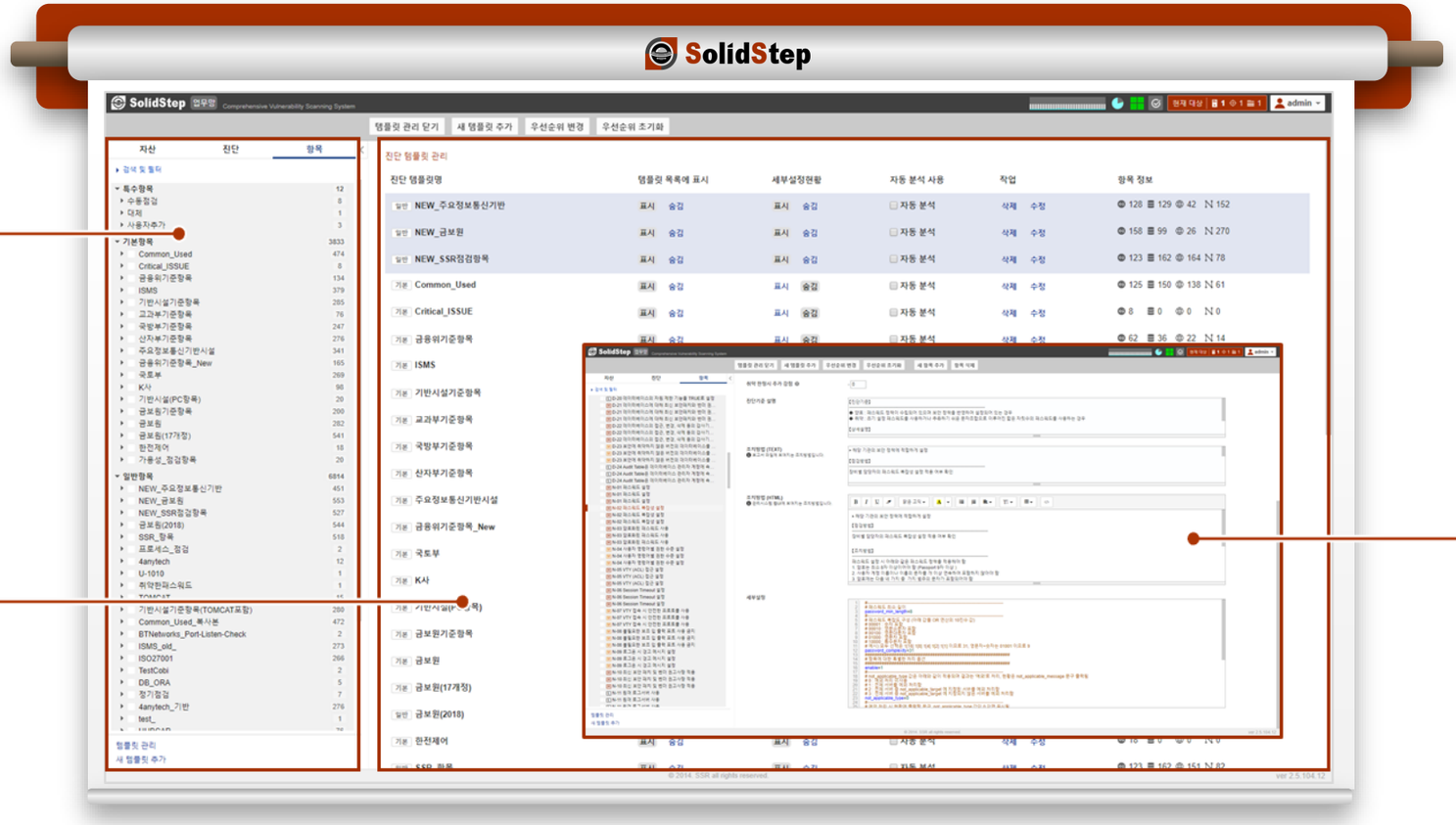
✓ 엑셀 양식을 통해 신규 자산 등록 가능

✓ 신규 그룹 생성 기능

# 2. SolidStep – 진단 템플릿 관리

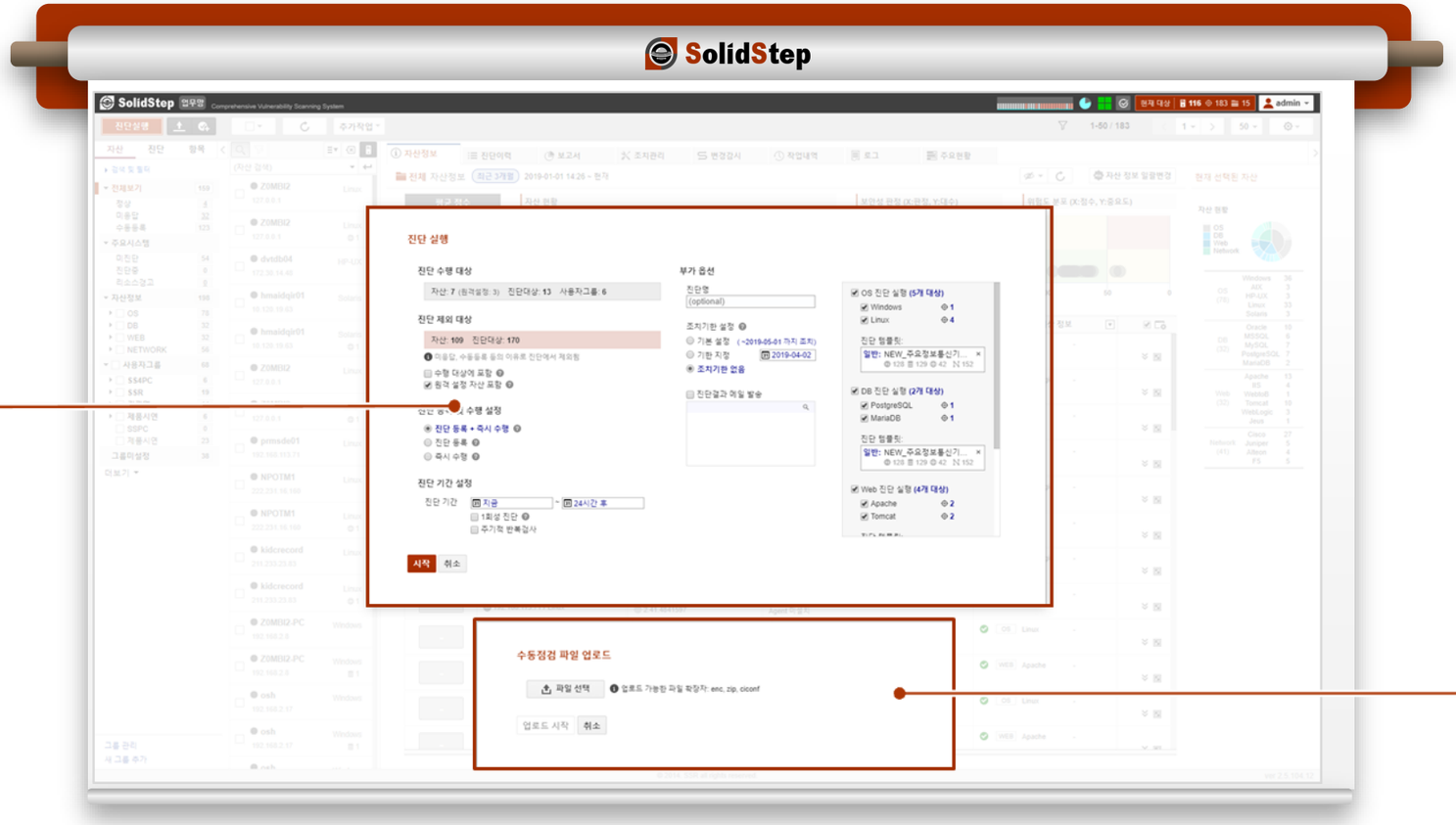
템플릿 관리를 통해 취약점 진단 기준 항목의 수정 및 삭제, 내부 지침(보안 가이드)에 따른 진단 항목 설정 값 수정(커스터마이징) 등의 관리 기능을 제공합니다.

- ✓ 항목 탭에서 템플릿 관리 및 새 템플릿 추가 가능
- ✓ 템플릿 관리 메뉴에서 템플릿 표시/숨김, 삭제, 수정 등의 관리 기능 제공
- ✓ 진단 항목 설정 값 수정(커스터마이징)



# 2. SolidStep – 진단 실행

취약점 진단 시 자산별, 그룹별, 네트워크 대역별(IP Address) 등 진단 대상을 다양하게 선정하여 취약점 진단이 가능하며, 수행 중인 작업의 취소가 가능합니다.

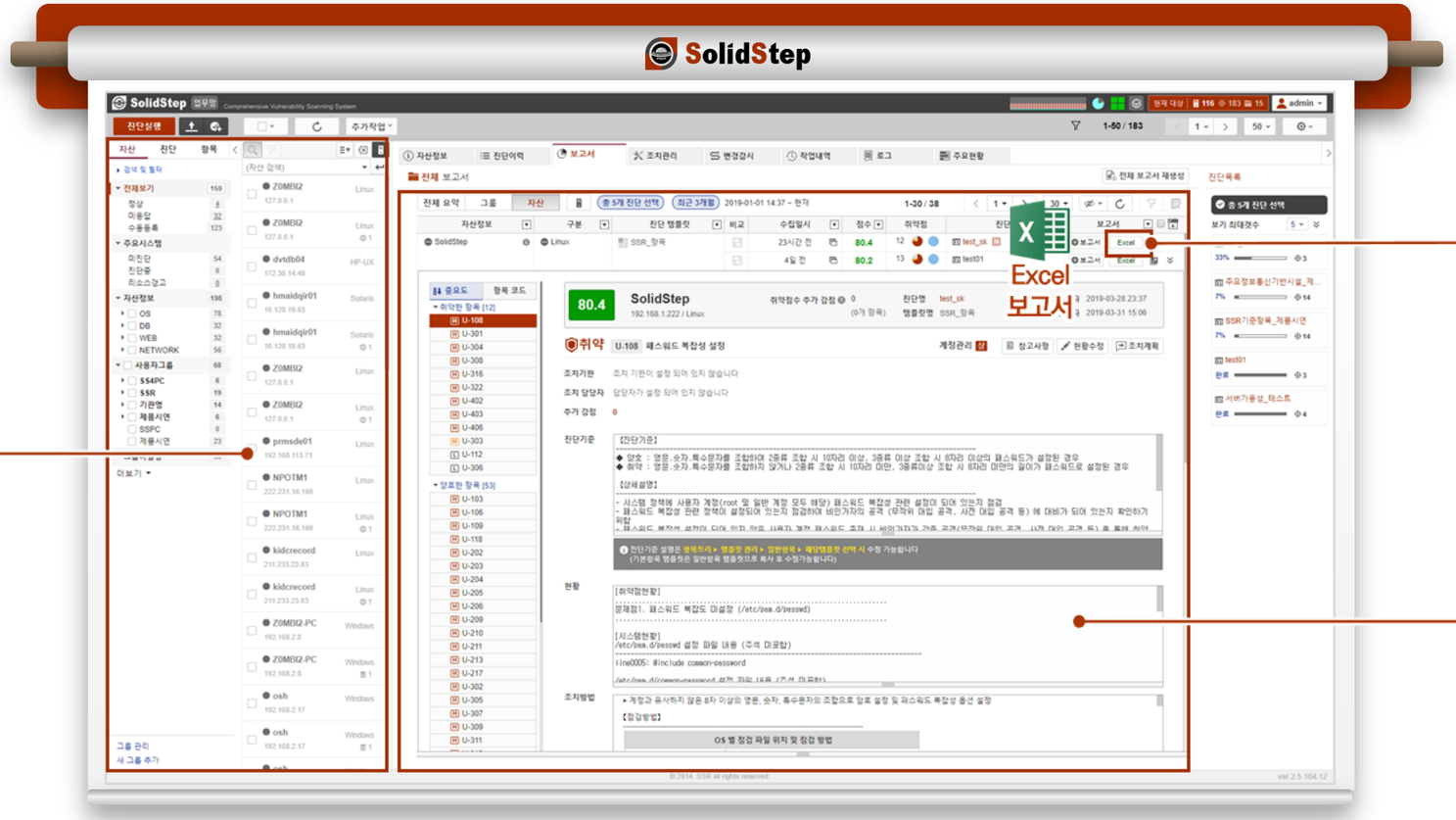



- ✓ 진단 실행
- ✓ 진단 기간 설정 가능 (매일/매주/매월/3개월/6개월)
- ✓ 진단 템플릿 설정 가능

- ✓ 수동진단 후 생성된 결과 파일을 업로드하여 진단 수행

# 2. SolidStep – 진단 결과

취약점 진단 후 결과 보고서가 자동으로 생성되며 Web UI 상의 보고서와 Excel 형태의 개별 보고서를 통하여 캡처 화면 등을 첨부한 상세한 가이드 제공 및 결과에 대한 비교기능을 제공합니다.



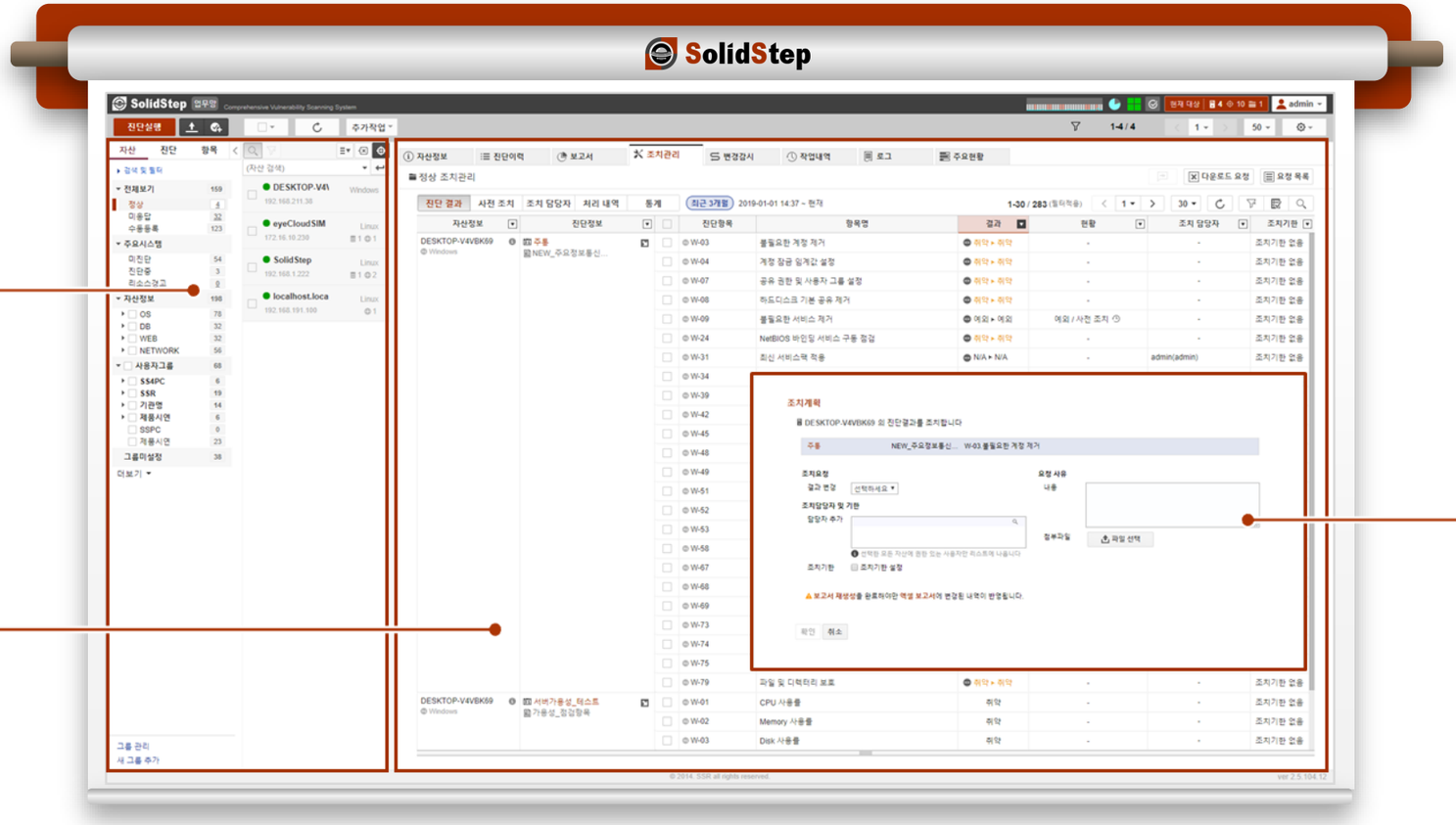

✓ 진단이 완료된 그룹의 자산 선택

✓ 다양한 관리기능 제공

✓ 진단 항목별 진단기준, 현황, 조치방법 확인 가능

# 2. SolidStep – 이행 조치

취약점 진단 결과 항목에 대해 임의적(예외/대체/NA/양호/취약/수동)으로 수정할 수 있도록 조치 관리 기능을 제공하며, 항목별 조치 담당자, 조치 일정 등을 지정 가능합니다.




✓ 진단이 완료된 그룹의 자산 선택

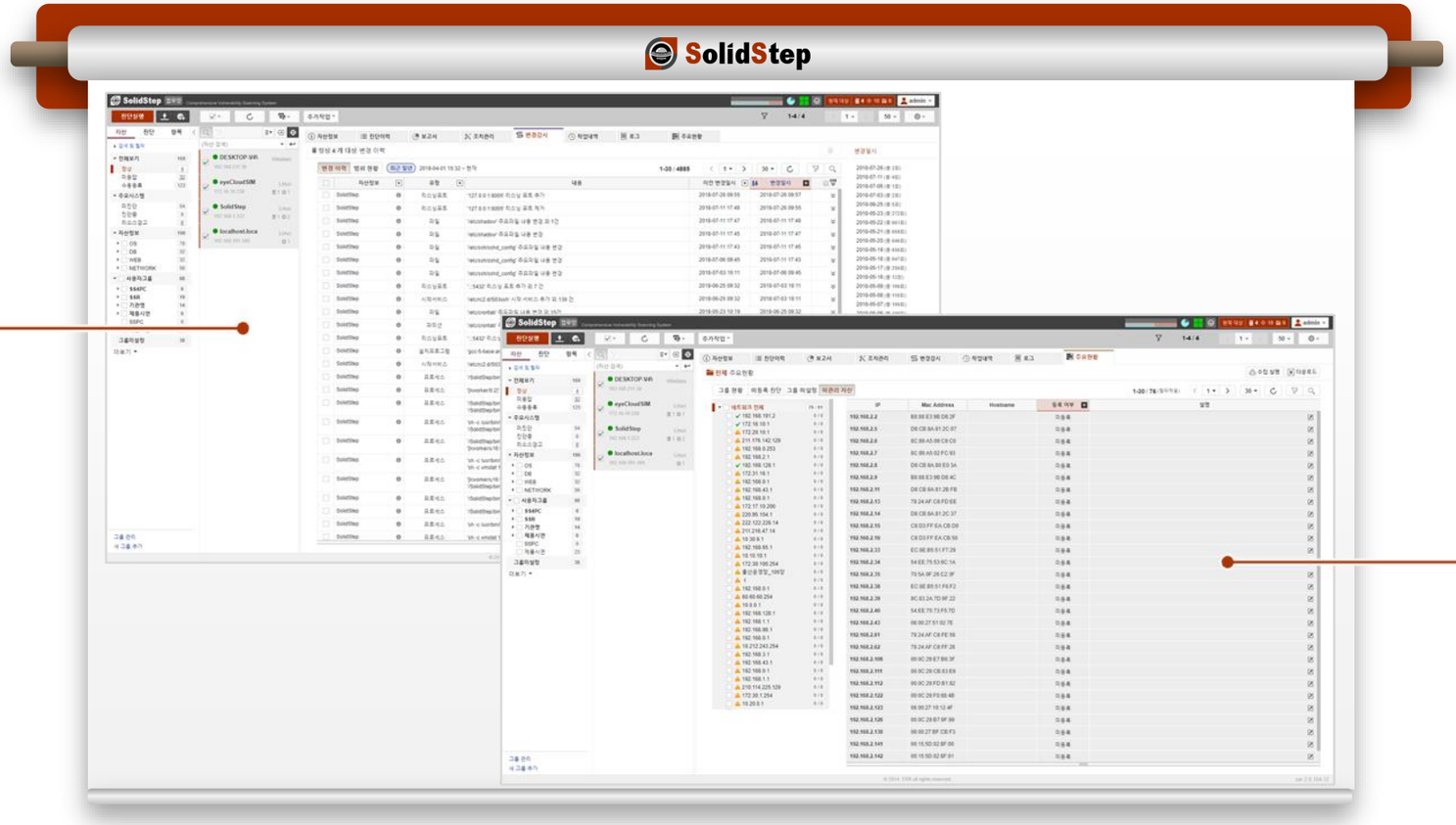
✓ 진단 결과에 개해 이전 진단 결과와 현재 진단 결과의 비교 및 이력관리 기능 제공

✓ 진단 결과 항목에 대해 임의적인 수정기능 및 항목별 조치 담당자, 조치 일정 지정 가능

# 2. SolidStep – 추가 기능

변경감시 정책 설정을 통해서 취약점 진단 수행 이후 OS 계정, 프로세스 등 주요 설정 값의 변경을 모니터링(실행 주기 설정) 하는 기능을 제공하며, 관리서버에 등록되지 않은 인프라 자산을 탐지하는 기능을 제공합니다.

- ✓ 자산정보 설정의 메뉴에서 변경감시 기능과 알림 기능을 이용하여 서버의 보안 설정 값 변경 시 알림
- ✓ 변경내용 비교 화면을 통하여 변경된 내용 확인 가능

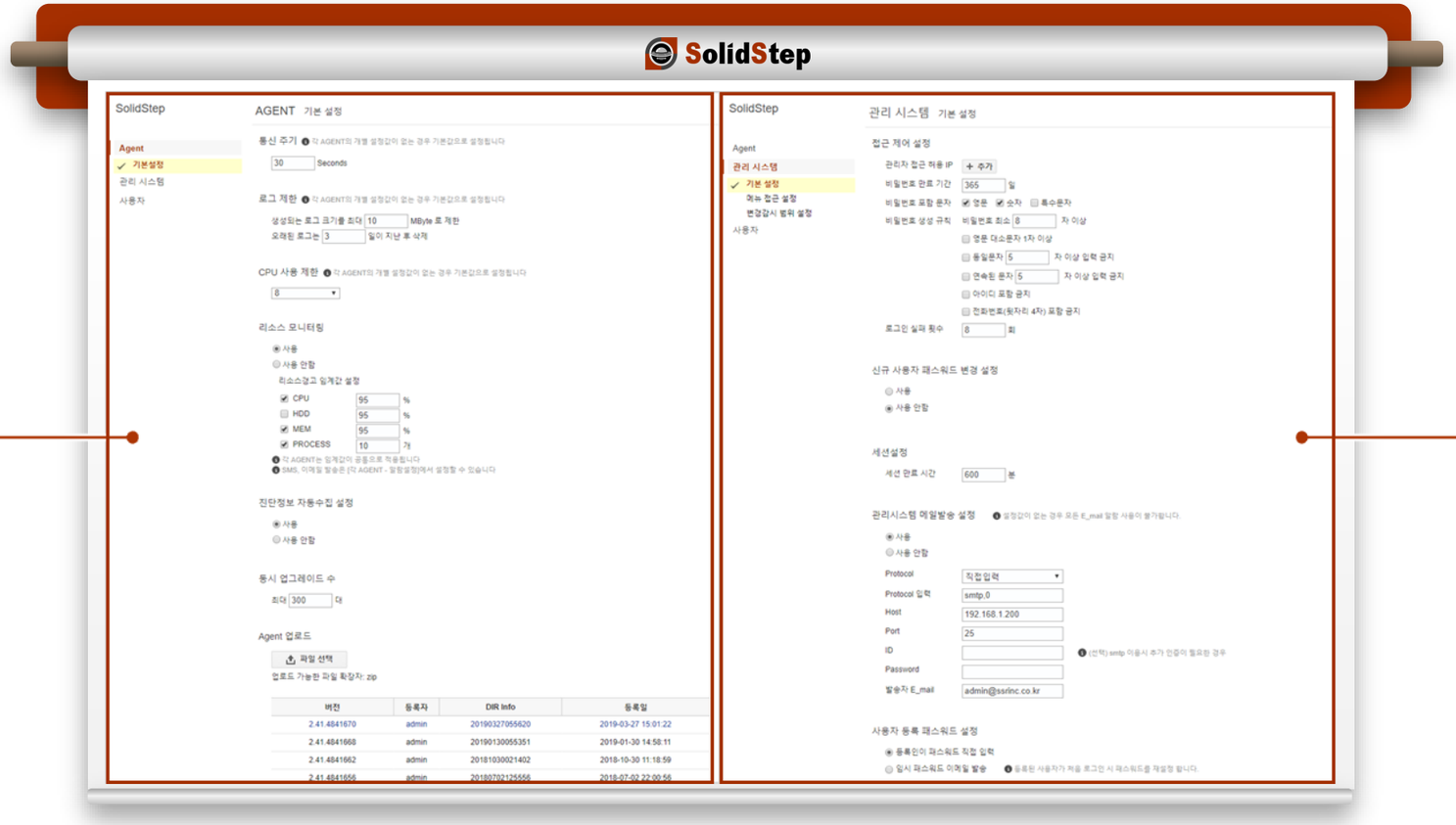



- ✓ 서버 시스템 내 자산의 IP, Hostname, MAC-Address 정보를 수집하여 SolidStep Manager의 기존 정보와 비교 후에 미등록 자산을 탐지

# 2. SolidStep – 시스템 관리

시스템의 영향을 최소화하기 위해 자산의 Agent CPU 사용률 조절 기능 및 알림 기능을 제공합니다. 또한 사용자 계정관리 및 권한별 접근 가능한 메뉴의 접근 관리기능을 제공합니다.

- ✓ 선택된 자산의 Agent CPU 사용률 조절 기능을 제공
- ✓ 개별 시스템 설정 값이 없는 경우 Agent의 기본 설정을 통해 일괄 적용 가능
- ✓ 다양한 Agent 기본 설정 기능 제공




- ✓ 사용자 관리, 관리 시스템 설정(기본 설정, 메뉴 접근 설정, 변경감시 범위 설정) 등을 통해 권한 관리/접근 제어 관리 등 다양한 설정 기능 제공

# 3. SolidStep Portable – UI 구성

SolidStep Portable은 직관적인 UI 디자인을 통해 사용자들의 취약점 진단 이해도와 사용성을 증가시키며, 오프라인 환경에서 단독적으로 취약점 진단을 수행합니다.


✓ 시스템 현황, 결과보기, 시스템 정보 메뉴

✓ 보안점수, 진단시작 버튼

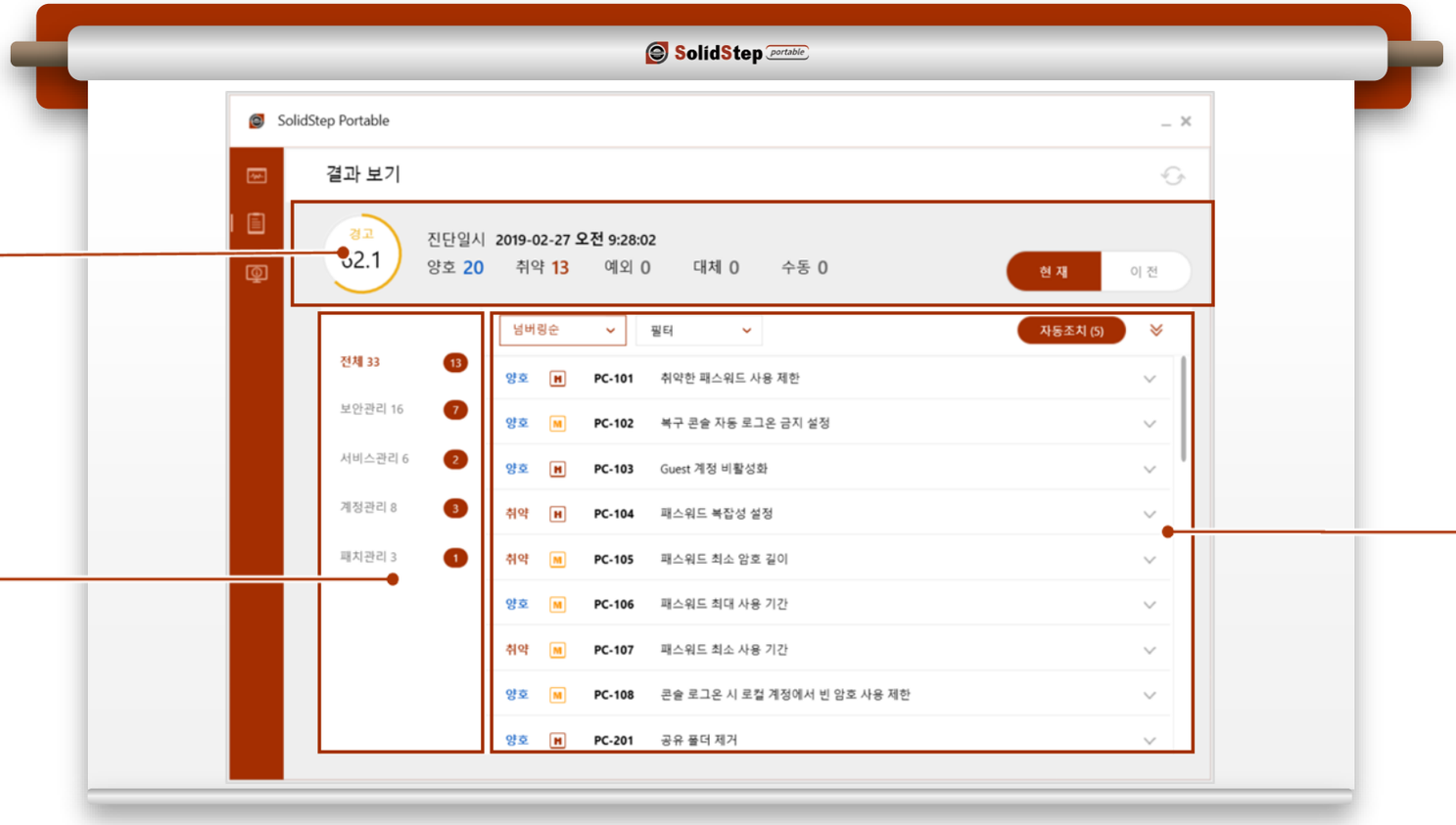
✓ 진단결과 항목 수 및 진단 템플릿 확인

✓ 이전 진단결과와 현재 진단결과 변경 항목 확인

# 3. SolidStep Portable – 진단 결과

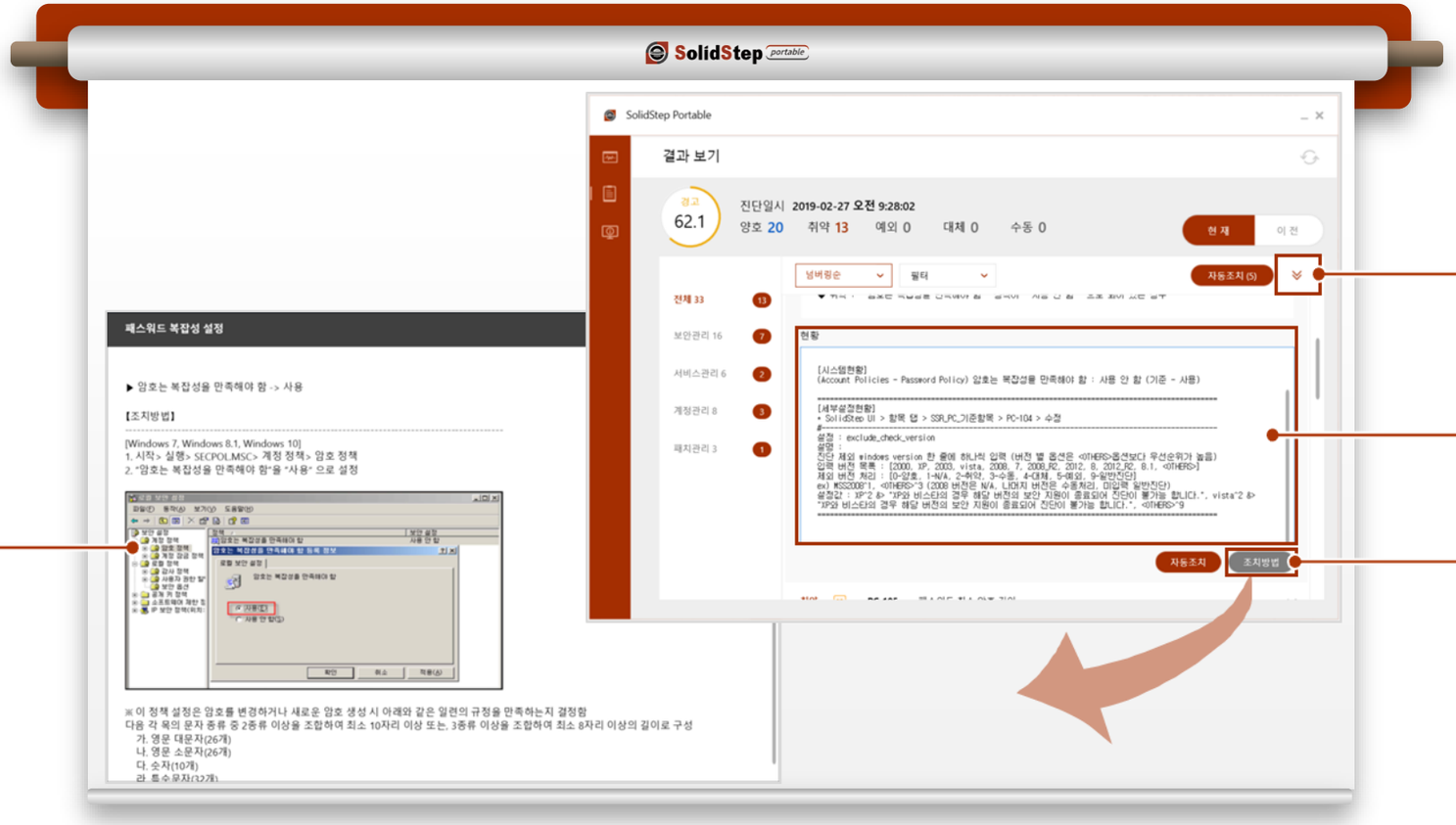
SolidStep Portable은 취약점 진단 수행 후 진단결과 및 진단 항목에 대한 현황을 제공합니다.

- ✓ 진단 일시, 보안현황 및 점수, 진단결과 항목 수, 이전 진단결과 또는 현재 진단결과 구분 버튼
- ✓ 전체 또는 진단 항목 그룹 구분
- ✓ 진단결과 내용 검색 필터 및 진단항목 상세내용 확인



# 3. SolidStep Portable – 조치 가이드

SolidStep Portable은 취약점 진단 수행 후 발견된 취약점 항목에 대한 상세내용과 조치방법을 제공합니다.




✓ 취약점 항목에 대한 캡처 화면 등을 첨부한 상세한 조치방안 확인 가능

✓ 진단결과 내용 검색 상세내용 확인 버튼

✓ 진단 자산의 현황 내용 확인

✓ 진단결과에 대한 조치방법 확인 버튼

# 4. SolidStep for PC – UI 구성

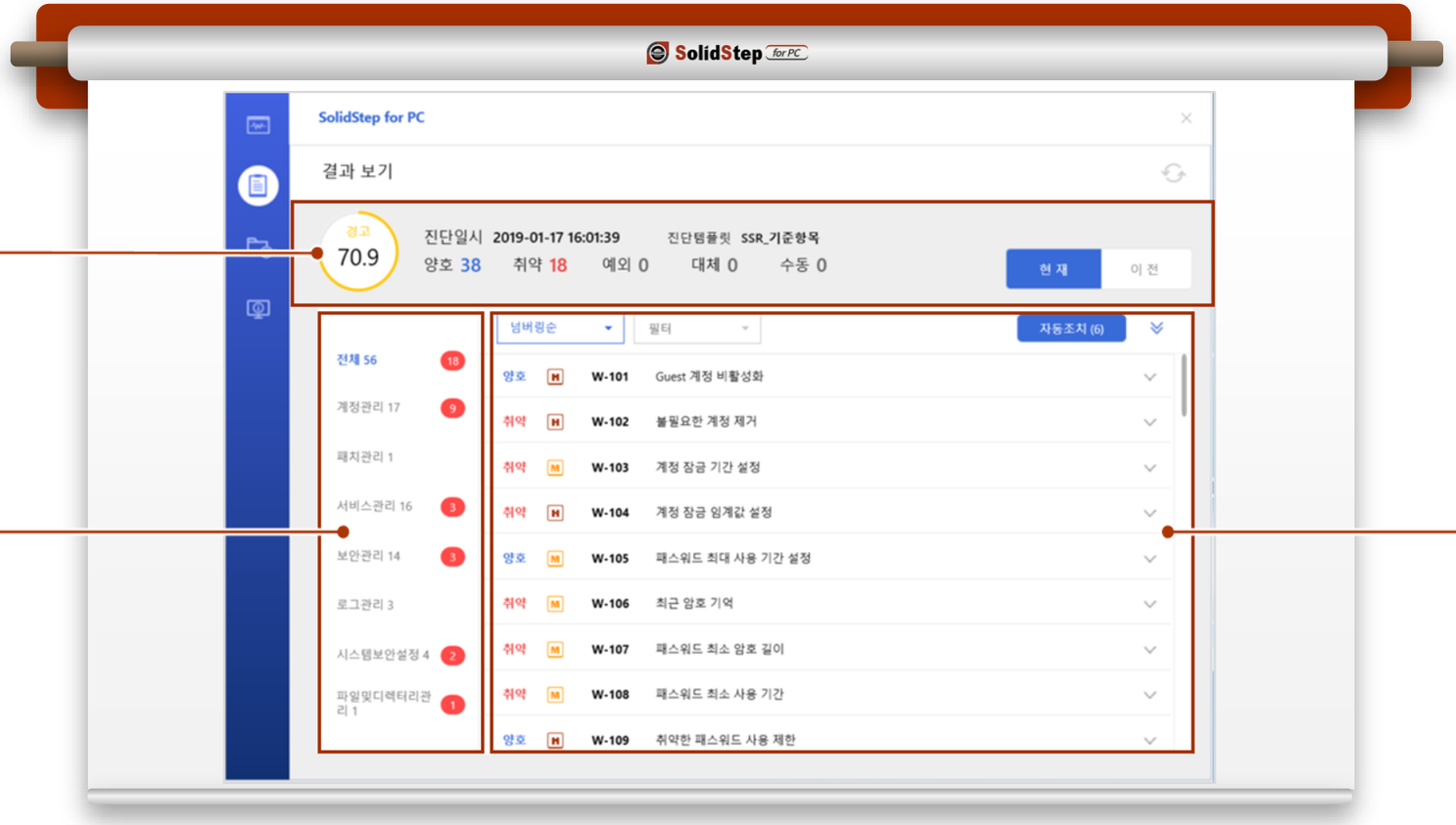
SolidStep for PC는 직관적인 UI 디자인을 통해 사용자들의 취약점 진단 이해도와 사용성을 증가시키며, 관리서버와 통신하여 Agent 방식으로 PC에 대한 취약점 진단을 수행합니다.


- ✓ 시스템 현황, 결과보기, 시스템 정보 메뉴
- ✓ 보안점수, 진단시작 버튼
- ✓ 진단결과 항목 수 및 진단 템플릿 확인
- ✓ 이전 진단결과와 현재 진단결과 변경 항목 확인

# 4. SolidStep for PC – 진단 결과

SolidStep for PC는 취약점 진단 수행 후 진단결과 및 진단 항목에 대한 현황을 제공합니다.

- ✓ 진단 일시, 보안현황 및 점수, 진단결과 항목 수, 이전 진단결과 또는 현재 진단결과 구분 버튼
- ✓ 전체 또는 진단 항목 그룹 구분
- ✓ 진단결과 내용 검색 필터 및 진단항목 상세내용 확인



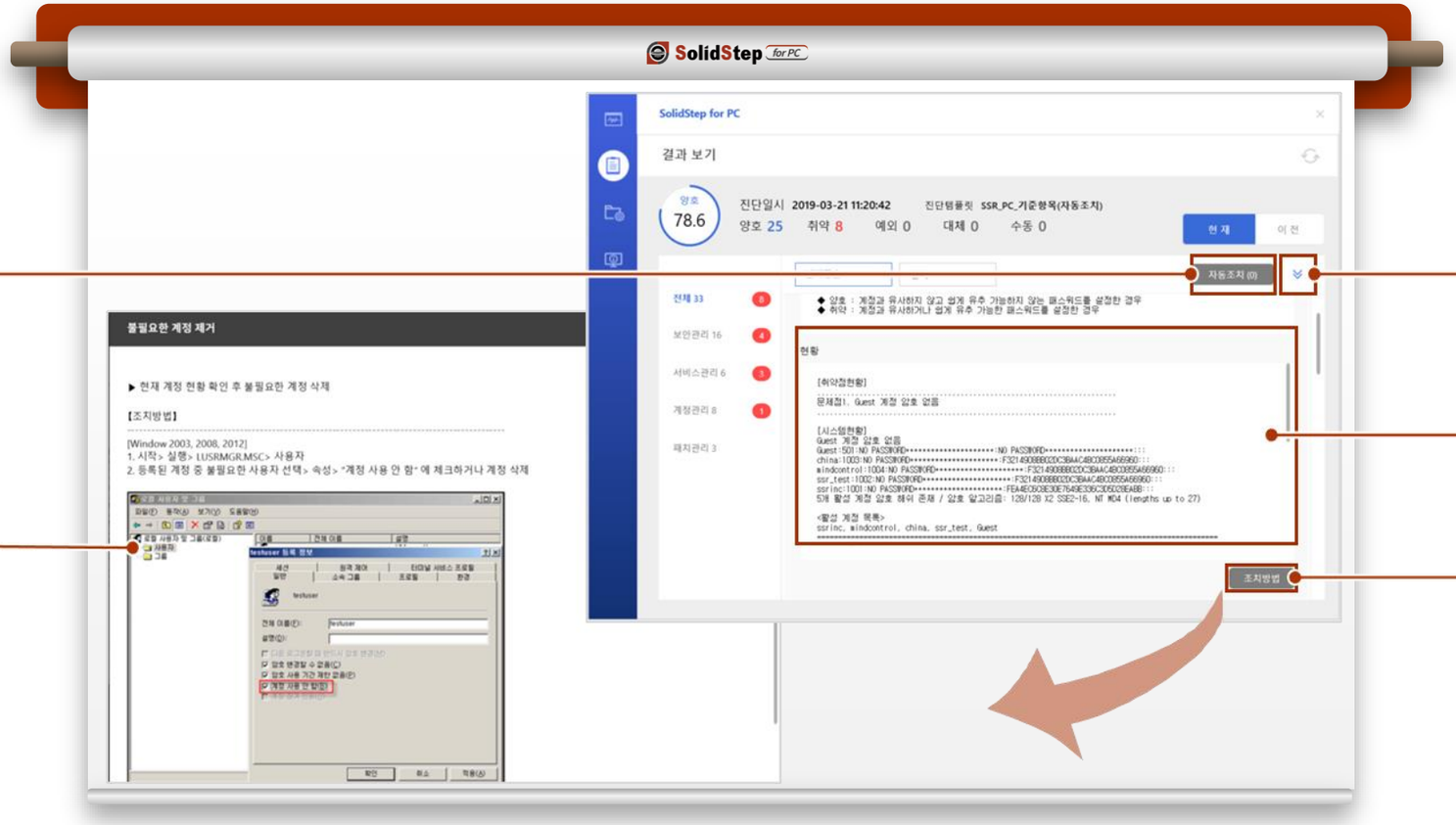
# 4. SolidStep for PC – 조치 가이드

SolidStep

SolidStep for PC는 취약점 진단 수행 후 발견된 취약점 항목에 대한 상세내용과 조치방법을 제공합니다.

✓ 자동조치 기능(로컬보안정책의 계정정책 지원)

✓ 취약점 항목에 대한 캡처 화면 등을 첨부한 상세한 조치방안 확인 가능




✓ 진단결과 내용 검색 상세내용 확인 버튼

✓ 진단 자산의 현황 내용 확인

✓ 진단결과에 대한 조치방법 확인 버튼


㈜삼에스소프트
Tel : 031-212-3390 | FAX : 031-212-3345 | sales@3es.co.kr
Addr 경기도 수원시 영통구 창룡대로256번길 91, 에이스광교타워2차 909호