



나라장터종합쇼핑몰

 SolidStep CCE

보안 취약점 진단 자동화 솔루션

솔리드스텝 CCE 제품소개서

SSR의 컨설팅 노하우와 기술력이 집약된 국내 시장점유율 1위인 보안 취약점 진단 자동화 솔루션입니다.

CONTENTS

- 01 SSR 소개
- 02 SolidStep CCE 제품소개
- 03 SolidStep CCE 주요기능
- 04 레퍼런스

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



고급 이상의 보안컨설팅 인력
대다수가 MENSA로 구성된
최상의 보안 전문가 집단



100% 순수 자체 기술과
컨설팅 노하우로 개발한
IT 보안제품 시리즈



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



2018년
코스닥 상장

500,000+진단수행



전 산업분야 500,000회 이상
취약점 진단과 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. (주)에스에스알 설립**



3. 사업분야

정보보호 전문서비스 기업!
보안의 디테일을 연구합니다.



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 취약점 진단 자동화 솔루션

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

웹 서버 보안 솔루션

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



02. SolidStep CCE 제품소개

1. 취약점 관리의 필요성
2. SolidStep CCE 제품개요
3. SolidStep CCE 특징점
4. SolidStep CCE 구성도
5. SolidStep CCE 지원 플랫폼
6. SolidStep CCE 도입효과

1. 취약점 관리의 필요성 (1/2)

취약점(Vulnerability)이란?

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



취약점 악용



비인가자
접근 허용

- 악의적 크래커의 침투
- 내부 비인가자 통제 어려움



정상적인
서비스 방해

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



주요 데이터
유출/변조/삭제

- 인사정보 및 기밀정보 유출

1. 취약점 관리의 필요성 (2/2)

다양한 보안 이슈에 대한 대응 필요

지속되는 해킹의 위협과 서비스 환경의 변화로 취약점에 대한 이슈 및 피해 사례 증가, 취약점으로부터 발생하는 피해를 예방하기 위한 **정보보호 관련 법규 및 준수사항 강화**, 다양한 인증 관리 시 내부 정보시스템에 대한 **상시적인 취약점 진단 및 조치를** 요구하고 있습니다.

해킹 피해사고 증가

- 지속되는 해킹의 위협과 서비스 환경의 변화(보호 대상 영역의 확대) 등에 따른 취약점 피해 사례 증가
- 취약점을 복합적으로 악용하여 지능화된 악성코드 유포 기승

정보보호 인증 컴플라이언스 준수 필요

- 정보보호 및 개인정보보호 관리체계 (ISMS-P), 정보보안경영시스템 (ISO/IEC27001) 등 다양한 정보보호 인증 관리 시 내부 정보시스템에 대한 상시적인 취약점 진단 및 조치 요구



취약점 관련 법령 준수사항 강화

- 정보통신기반보호법, 전자금융감독 규정 등 정보보호 관련 법규 및 준수사항 강화
- 운영 중인 내·외부 서비스의 정기적인 취약점 진단 수행 요구 (주요정보통신 기반시설, 전자금융기반시설은 매년 취약점 분석/평가 실시해야 함)

클라우드 보안 인증 컴플라이언스 준수 필요

- 클라우드 서비스 보안 인증(CSAP)을 위한 취약점 진단 수행 요구
- 클라우드 및 컨테이너 환경 자산에 대한 위험을 식별하고 침해사고에 대한 효율적인 대응을 위해 상시적인 취약점 진단 필요

2. SolidStep CCE 제품개요 (1/2)

취약점 진단 자동화 솔루션

SolidStep CCE는 서버, 네트워크 장비와 같은 IT 인프라 자산의 **보안 진단을 상시적으로 자동 수행하는 취약점 진단 자동화 솔루션**입니다.

SolidStep CCE



나라장터종합쇼핑몰

식별번호 : 24396441
 식별번호 : 24396440
 식별번호 : 24396439
 식별번호 : 24396437

✓ 국내 시장점유율 1위 솔루션으로 GS1등급 인증 획득

✓ 국내 컴플라이언스에 대해 완벽 대응

✓ 진단 항목 커스터마이징으로 내부정책 진단 최적화

✓ 간편한 자동화 전수 진단 및 다양한 진단 옵션 제공

✓ 발견된 취약점 항목의 자동 조치기능으로 신속한 운영 지원

✓ 컨설턴트가 직접 작성한 수준의 결과보고서 제공

2. SolidStep CCE 제품개요 (2/2)

컨설팅과 동일한 수준의 취약점 진단 수행

SolidStep CCE는 다양한 플랫폼 환경의 시스템 자산을 대상으로 국내·외 법령 및 규제(컴플라이언스)를 준수하기 위해 컨설팅과 동일한 수준의 취약점 진단을 자동으로 수행합니다.

취약점 진단 대상

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



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



취약점 진단 방식

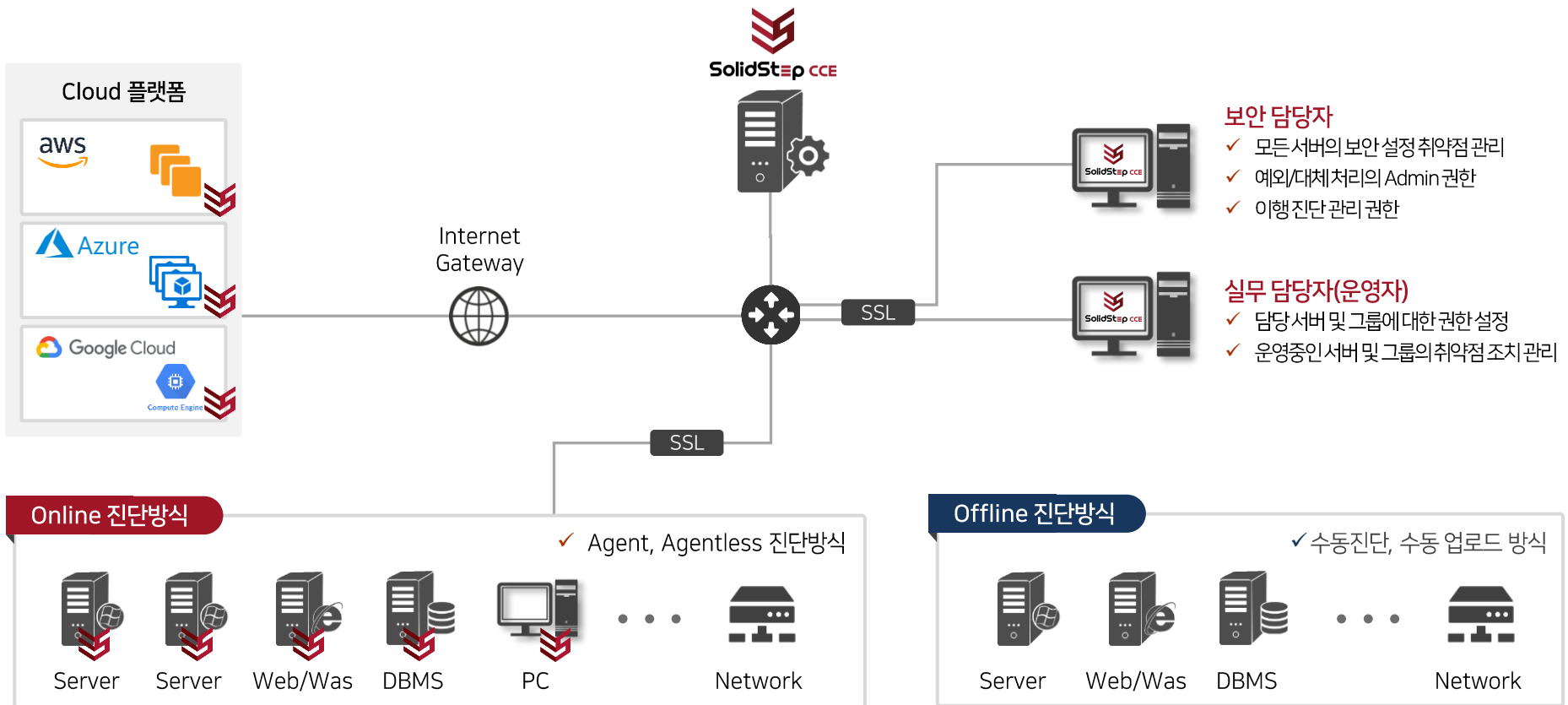
시스템 운영 환경 및 플랫폼의 특성을 고려한
다양한 취약점 진단 방식 지원



3. SolidStep CCE 구성도

안정성과 보안성을 고려한 최적화된 시스템 구성

SolidStep CCE 구축 시 운영 중인 네트워크 구성 환경을 분석하여 솔루션의 안정적인 성능과 보안성, Agent가 설치되는 정보자산(서버)의 영향력 등을 고려하여 최적화된 시스템을 구성합니다.



4. SolidStep CCE 특징점

국내 1위의 검증된 기술력으로 자체 개발한 솔루션

SolidStep CCE는 정보보호 전문서비스 기업인 에스에스알이 다년간의 컨설팅 노하우로 직접 개발한 보안 솔루션으로, 다양한 국내 기관 및 업체의 POC, BMT에서 타사 대비 월등히 높은 기술력과 업체 역량, 제품 우수성을 검증 받은 솔루션입니다.

☑ 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 6년 연속 1위(2016~2021년 조달 구매 기준)
- 국내 시장점유율 70% 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

☑ 다양한 종류의 클라우드 진단 가능

- AWS, Azure, GCP 진단 가능
- Auto-Scaling을 통해 변동되는 취약점 진단 자산에 대한 최적화된 이력관리 가능



취약점 관리

고객사 내부 보안기준 맞춤

전체 자산에 대한 보안현황 관리

취약점 분석평가의 계량화

체계적인 취약점 조치 이행관리

취약점 자동 조치 및 자체 결재시스템 등의 추가 기능

4. SolidStep CCE 특징점 - ① 개발사의 기술력

SolidStep CCE 개발사인 에스에스알은 **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 업데이트와 솔루션 연구·개발에 힘쓰고 있습니다.



보안 솔루션 개발/구축



CCE 취약점 진단 자동화 솔루션



CVE 취약점 진단 자동화 솔루션



PC 취약점 진단 자동화 솔루션



단독형 PC, 폐쇄망 제어 PC 취약점 진단



실시간 웹шел 탐지 솔루션



관리컨설팅

ISMS-P 인증컨설팅

ISO 27001 인증컨설팅

기반시설 취약점 분석/평가

금융기관 취약점 분석/평가

- 정보보호관리체계(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

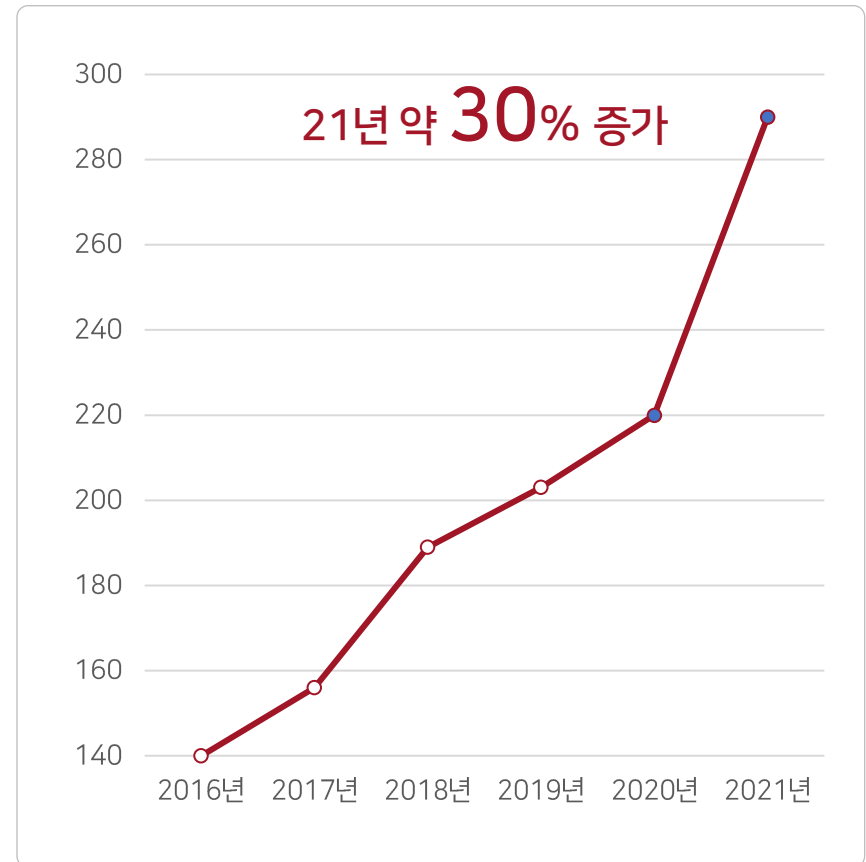
4. SolidStep CCE 특징점 - ② 시장점유율

SolidStep CCE는 공공기관, 금융권, 일반기업, 교육기관 등 다양한 산업분야에 구축되어 안정적으로 운영되고 있는 솔루션으로, 매년 경쟁사가 늘어남에도 **CCE 취약점 진단 솔루션 분야 조달 구매율 1위**를 유지하며 꾸준한 매출 성장세를 이어가고 있습니다.

조달 구매율 (출처: 조달정보개방포털)

솔루션 제조사	2021년 조달 구매	
	금액(원)	점유율
 에스에스알	1,378,660,800	53 %
N 사	891,764,800	34 %
J 사	269,233,800	10 %
L 사	75,700,000	3 %
합계	2,916,474,000	100 %

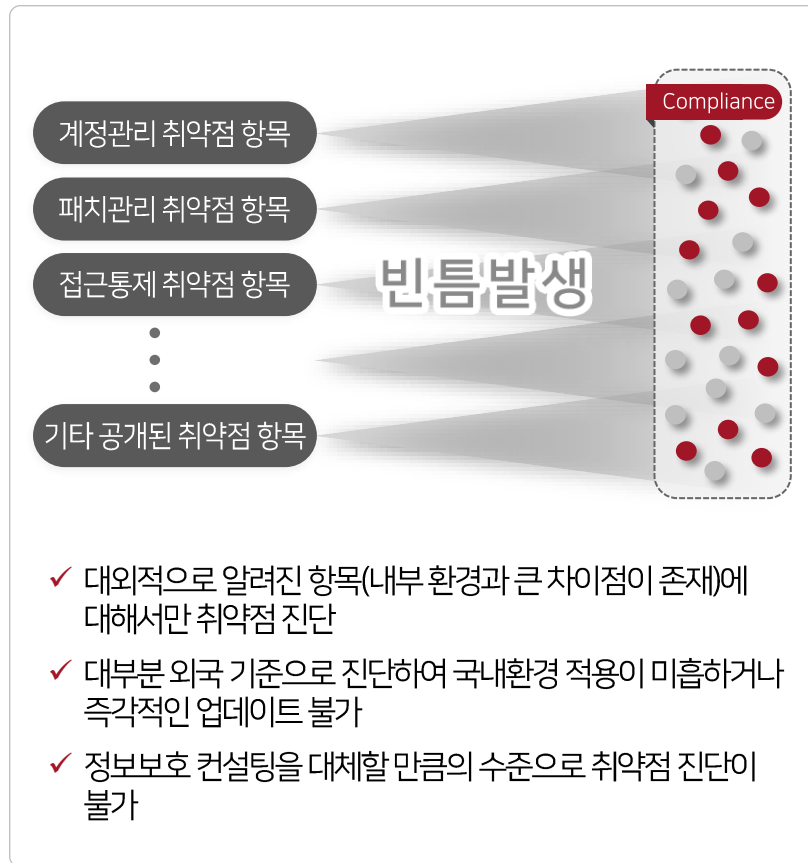
레퍼런스 현황 (단위: 고객사수)



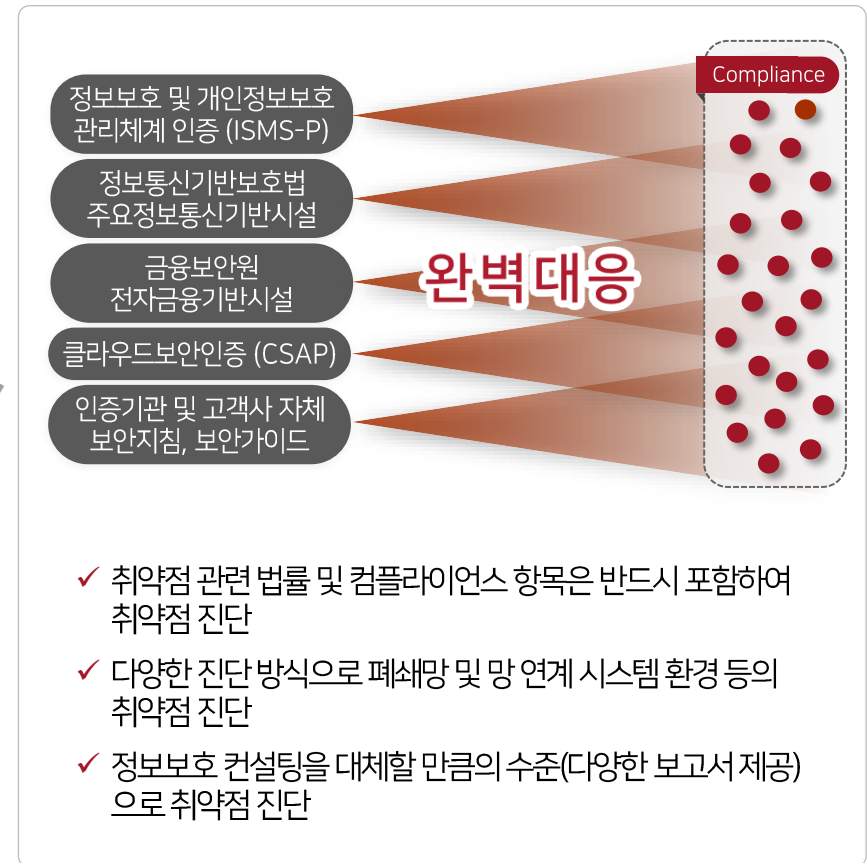
4. SolidStep CCE 특징점 - ③ 컴플라이언스 완벽 대응

SolidStep CCE는 정보통신기반보호법, 전자금융거래법, 정보보호관리체계, 개인정보관리체계, 클라우드 보안 인증 등에서 법률적 통제를 의무화하는 **인프라 환경의 취약점 진단 항목을 100% 지원**하며, 내부 보안가이드에 따른 **진단 항목 커스터마이징이** 가능합니다.

기존 취약점 진단 솔루션



SolidStep CCE



4. SolidStep CCE 특징점 - ④ 취약점 진단 최적화 아키텍처

SolidStep CCE는 **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, RPC 서비스를 이용한 진단
 - Agent 방식과 동일한 분석 결과 보장
 - 서버 접속정보 입력 및 관리 필요, 네트워크 접근 ACL필요
 - 부가기능(리소스 모니터링 등) 이용불가, 예약진단 이용불가
- API를 이용한 Cloud 진단 (AWS, Azure, GCP, ESXi)
 - API 인증을 위한 인증 정보 입력 및 관리 필요

! Offline 방식 (수동진단)

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

5. SolidStep CCE 지원 플랫폼

50개 이상 플랫폼의 취약점 진단

SolidStep CCE는 운영 중인 시스템 환경의 다양한 OS, DBMS, WEB/WAS, Network 등 50개 이상 플랫폼의 취약점 진단을 제공합니다.

플랫폼 구분	상세 내역	비고
OS	<ul style="list-style-type: none"> Windows <ul style="list-style-type: none"> - 서버계열 : 2008/2008 R2/2012/2016/2019/2022 - PC계열 : 7/8/10/11 Linux(Debian, RHEL, CentOS, Ubuntu, OpenSuse, Amazon Linux, ProLinux) Unix(HP-UX 11 이상, AIX 5.2 이상, Solaris 5.8 이상) 	
DBMS	<ul style="list-style-type: none"> Oracle, MSSQL, MySQL, DB2, SYBASE, Tiberio, Altibase, Postgres SQL, Maria DB, Vertica, Cubrid, Mongo DB, Redis, Teradata 등 	
WEB	<ul style="list-style-type: none"> Apache, IIS, WebtoB, Oracle Http Server, IBM Http Server, Lena Web Server 등 	
WAS	<ul style="list-style-type: none"> Tomcat, WebLogic, iPlanet, Jeus, WebSphere, Nginx, Jboss, Resin, Jrun, Jetty, Lena Web Application Server 등 	
Network	<ul style="list-style-type: none"> Cisco, Juniper, HP(3Com), Alteon, Alcatel, Extreme, AVAYA, Brocade, ubQuoss, PIOLINK, A10, Citrix, Huawei, HanDreamnet, DELL, Arista, F5, DASAN, Aruba 등 	
Cloud	<ul style="list-style-type: none"> AWS, GCP, Azure 등 	
Application OS	<ul style="list-style-type: none"> OpenStack, Docker, Hadoop, Kubernetes, ElasticSearch 등 	
HyperVisor	<ul style="list-style-type: none"> VMware ESXi, Citrix XenServer, Hyper-V, KVM 등 	

※ 신규 플랫폼에 대한 지속적인 개발 및 지원

6. SolidStep CCE 도입효과

취약점 분석평가 현황의 체계적인 관리 및 정량화

SolidStep CCE는 인프라 시스템에 대한 취약점 관리 업무 연속성 확보, 상시 취약점 진단, 분석, 조치, 이력 관리 등 **자동화된 취약점 관리체계 구축을 지원합니다.**

01

컴플라이언스(법/규정) 완벽 대응

- 대내·외 컴플라이언스 및 보안 가이드 대응으로 침해사고 예방
- 주요정보통신기반시설 및 금융보안원 전자금융감독규정, 클라우드 보안 인증 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

03. SolidStep CCE 주요기능

1. 편리한 Web UI 방식의 통합 대시보드
2. 자산 설정 및 자산그룹 관리
3. 진단 기준 항목 템플릿 관리
4. 다양한 대상 및 유형별 진단 실행
5. 상세 진단 결과 가이드 제공
6. 신속한 조치 관리
7. 결재 관리
8. 자동 조치
9. 클라우드 플랫폼 진단
10. 안전한 시스템 관리

1. 편리한 Web UI 방식의 통합 대시보드

SolidStep CCE는 사용자 접근성 및 편의성을 고려한 **Web UI 방식**으로, 취약점 진단 데이터를 바탕으로 다양한 현황 및 통계를 직관적으로 확인할 수 있는 **통합 대시보드**를 제공합니다.

The screenshot displays the SolidStep CCE Web UI dashboard. The interface is divided into several sections:

- Navigation Menu (Left):** A sidebar menu with icons for home, search, and various management functions. It includes a search bar and a filter button.
- Asset Management (Top Left):** A tree view showing asset groups and individual assets. Assets are listed with their OS, IP, and status (e.g., 정상, 미응답).
- Asset Information (Top Right):** A header area with tabs for '자산정보', '진단 결과', '조치관리', '결재관리', '자동 조치', '적용내역', and '로그'. A callout box points to these tabs, stating: "자산정보/진단결과/조치관리/결재관리/자동조치/작업내역/로그 등 다양한 관리 기능".
- Dashboard (Main Area):** A central area displaying a list of assets with their average scores and status. A callout box points to this area, stating: "자산별/진단대상별 평균점수, 진단현황, 자산 설정 등 에이전트 현황 및 설정".
- Summary Dashboard (Right):** A detailed view of an asset (SSR_기준항목) showing a score of 42.1. It includes a donut chart for '발견된 취약점' (67), a bar chart for '위험도' (10% to 15%), and a table for '조치 현황' (420, 670, 420). A callout box points to this dashboard, stating: "진단 템플릿의 현황을 수시로 확인할 수 있도록 대시보드 화면의 자동 갱신시간 설정".
- Configuration Modal (Bottom Right):** A '대시보드 설정' (Dashboard Settings) modal window. It allows users to select a '진단 템플릿 선택' (SSR_기준항목) and set the '페이지 갱신' (Page Refresh) interval to 10 minutes. Buttons for '취소' (Cancel) and '확인' (Confirm) are visible.

Additional callout boxes provide further details:

- Bottom Left: "자산 그룹, 자산 분류, 진단 그룹에 따른 보기 방식을 모달창 최소화 기능을 적용한 사이드바 메뉴 형식으로 작업 영역 확보 및 사용자 편의성 제공"

2. 자산 설정 및 자산그룹 관리

자산별, 운영 부서별 다양한 그룹핑 설정으로 물리적/논리적 그룹화 관리가 가능하며, 관리자/사용자별 접근 권한 관리 기능을 제공합니다.

The screenshot displays the SolidStep CCE interface for managing asset groups. The left sidebar shows navigation options, with '자산그룹 관리' (Asset Group Management) selected. The main area shows a tree view of groups under 'Root', including 'GROUP_1', 'GROUP_1.1', 'GROUP_1.2', and 'GROUP_1.2.1'. A callout points to the 'GROUP_1.2.1' group, stating: "자산그룹의 Multi Depth(연결그룹) 기능" (Multi-Depth (connected group) feature of asset groups).

The right panel shows the details for 'GROUP_1.2.1', including its name, creation date (2019-01-02), and group number (110). A callout points to the '일반' (General) tab, stating: "그룹명 변경, 사용자 추가, 승인이 필요한 작업 요청의 결재선 관리 기능" (Group name change, user addition, approval management for tasks requiring approval).

Below the main interface, a '새 그룹 추가' (Add New Group) dialog box is shown. It allows creating a group under 'ROOT' and offers two options: '연결그룹' (Connected Group) and '자산그룹' (Asset Group). The '연결그룹' option has checkboxes for '하위 그룹 보유' (O), '자산 배치' (X), '권한 설정' (X), and '그룹 결재선 설정' (X). The '자산그룹' option has checkboxes for '하위 그룹 보유' (X), '자산 배치' (O), '권한 설정' (O), and '그룹 결재선 설정' (O). A callout points to this dialog, stating: "연결그룹 또는 자산그룹을 추가 생성" (Add or create connected group or asset group).

3. 진단 기준 항목 템플릿 관리

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

진단 항목 설정 값 수정 (커스터마이징)

템플릿 관리

템플릿 사용여부 설정, 우선순위 변경, 삭제 등의 진단 템플릿 관리

템플릿 상세보기

항목 상세보기

템플릿명: 기본 SSR_기준항목

시스템코드: US110

진단 대상: OS-ALL, OS-WP-ALL, OS-Linux, OS-Solars

항목 코드: U-103

항목명: 불필요한 계정 제거

분류명: 계정관리

세부 설정

```

1 #
2 # [현재 적용 중인] 패스워드 최소 길이 입력
3 check_password_min_len=8
4 #
5 # [현재 적용 중인] 진단 제외 Unix OS 한 줄에 하나씩 입력 ( OS 별 옵션은 <OTHERS> 옵션보다 우선순위가 높음 )
6 # 입력 OS 목록 : [aix, linux, hpux, solaris <OTHERS>]
7 # 제외 OS 처리 : [0-영문, 1-N/A, 2-취약, 3-수용, 4-대체, 5-예외 수신편진단 ]
8 # # aix=1, <OTHERS>=3 (aix에서는 N/A, 나머지 OS는 수용처리, 미입력默认진단)
9 exclude_check_os=<<EOT
10 EOT
11 #
12 # Linux PAM에 속성명=패스워드 설정 처리 /bin/passwd, /bin/sudo, /bin/su
  
```

진단 템플릿 관리

진단 템플릿명	항목 번호	템플릿 사용	설정 표시	언어	우선순위
기본 SSR_기준항목	123	102	104	109	사용 표시 한국어
기본 GROUP_NAME	7				수정
일반 SSR_AIX_Template	149	234	248	439	75 42 100%
기본 기법시보(기법등록)	20				한국어
기본 SSR_AIX_기법항목	33				한국어
일반 SSR_AIX_Template_복제본	149	234	248	439	75 42 100%
기본 공통취약기법항목	60	39	24	42	사용 표시 한국어
기본 취약점보통인기법시보_기본항목	128	100	27	102	사용 표시 한국어
일반 SSR_기준항목_복제본	123	102	104	109	사용 표시 한국어
일반 SSR_기준항목_복제본	123	102	104	109	사용 표시 한국어
일반 SSR_기준항목_복제본	123	102	104	109	사용 표시 한국어
일반 SSR_기준항목_복제본2222	123	102	104	109	사용 진단 영어

4. 다양한 대상 및 유형별 진단 실행

취약점 진단 시 자산별, 그룹별, 네트워크 대역별(IP Address) 등 **다양한 진단 대상을 선정**할 수 있으며, 수행 중 작업 취소도 가능합니다.

진단 실행

진단 유형

- 기본 진단: 진단 등록 후 즉시 수집 및 분석을 진행 합니다.
- 진단만 등록: 진단만 등록 후 진단 기간 중 원하는 시간에 수집 및 분석을 진행 합니다.
- 재진단: 기존 진단의 결과만 신규 데이터로 갱신 합니다.

진단명

진단명 입력

진단 기간

2021-03-03 13:15 ~ 2021-03-06 14:15

초치 기한

2020-05-22 14:01

결과 발송

진단결과 메일 발송 대상자를 선택하세요.

진단 대상

제외 대상 중 원격 접속이 가능한 대상을 진단에 포함

수행대상: 자산: 99999 진단대상: 99999 그룹: 99999 (원격접속: 99999)

제외대상: 미응답 또는 수동등록 등의 이유로 진단에서 제외되는 대상 (원격접속: 0)

진단 대상/템플릿 설정

- OS 진단 실행 (12311개 진단 대상)
 - Windows: 10000
 - AIX: 1
 - Linux: 2311
 기본: 주요정보통신 기본시설_기준항목
- DB 진단 실행 (14392개 진단 대상)
 - Mysql: 512
 - MariaDB: 1032
 - Oracle: 1598
 - PostgreSQL: 7138
 - MongoDB: 12282
 기본: 주요정보통신 기본시설_기준항목
- WEB 진단 실행 (865개 진단 대상)
 - Apache: 175
 - Apache: 456
 기본: 주요정보통신 기본시설_기준항목
- Application 진단 실행 (14392개 진단 대상)

취소 실행

수동점검 파일 등록

파일을 드래그 하거나, 여기를 눌러주세요.

업로드 가능한 파일 확장자: enc, zip, iconf

취소 업로드

진단 실행을 위한 진단 유형 및 대상 선택

수동점검 후 생성된 결과 파일을 업로드하여 진단 수행 가능

사용자가 원하는 진단 템플릿 선택 가능

5. 상세 진단 결과 가이드 제공

취약점 진단 후 Web UI에서 보고서를 확인할 수 있으며, 상세 가이드 및 결과에 대한 비교가 가능하도록 Excel, Word 형태의 결과 보고서를 제공합니다.

The screenshot displays the SolidStep CCE Web UI interface. On the left, a sidebar lists asset groups. The main area shows diagnostic results for various assets, including a score of 75.5 for '2020년도 상시진단_기술연구소'. A callout box highlights the '진단결과' (Diagnostic Results) tab and the '진단별 보기' (View by Diagnostic) button, with the text: '진단별/그룹별/자산별로 진단결과를 선택하여 확인 가능' (You can select and check diagnostic results by diagnostic type/group/asset).

Another callout box points to the '보고서' (Report) button and its dropdown menu, which includes options like '전체 요약 보고서' (Overall Summary Report) and '전체 상세 보고서' (Overall Detailed Report). The text says: 'Excel, Word 형식의 전체 요약, 그룹 보고서 제공' (Provide overall summary and group reports in Excel and Word formats).

A third callout box points to a specific asset group in the sidebar, stating: '진단이 완료된 그룹의 자산 선택' (Select assets of the group where diagnosis is complete).

On the right, there are icons for Word (W) and Excel (X), indicating the available report formats. Below these, a preview of a report is shown, including a table of diagnostic results and a radar chart. The report title is '4 상세 진단 결과' (4 Detailed Diagnostic Results).

구분	점수	위험도	최고
시스템별	50.15	중	3.142
그룹별	50	중	3.142
자산별	100	위	3.142
시스템별	50.15	중	3.142
시스템별	100	위	3.142
시스템별	100	위	3.142
시스템별	100	위	3.142
시스템별	100	위	3.142
시스템별	100	위	3.142
시스템별	100	위	3.142

6. 신속한 조치 관리

진단 결과에 대한 신속한 이행 조치를 위해 **사전조치**, **결과조치** 기능을 제공하며, 즉시 조치가 불가능하거나 장기적인 계획이 필요한 취약점 진단 결과 항목에 대해서는 사용자가 요청한(예외/대체/NA/양호/취약/수동) 결과로 점검 가능합니다. **항목별 조치 담당자**, **조치 기한** 등의 지정이 가능합니다.

진단 결과 항목에 대한
결과조치/사전조치 기능

The screenshot displays the SolidStep CCE interface. The main table lists assets with columns for asset name, target, diagnosis status, severity, action result, assigned user, and deadline. A callout box points to the '조치관리' (Action Management) tab in the top navigation bar. Another callout box points to a modal window titled '결과조치 일괄등록' (Batch Action Registration), which includes fields for '결과조치 대상' (Action Target), '적용 대상' (Apply Target), '진단결과' (Diagnosis Result), '조치기한' (Action Deadline), and '조치담당자' (Action Assignee). The modal also features a search bar for '결과조치 대상' and a '요청사유' (Request Reason) field.

진단 결과조치 대한
결과 변경, 현황 수정,
항목별 조치 담당자,
조치기한 등을
지정하여 등록 가능

7. 결재 관리

자산의 승인이 필요한 작업 요청(사전조치, 결과조치, 조치담당자 지정 등)에 대한 **결재선 지정**이 가능하여 **신속한 조치 실행 및 결재 요청에 대한 이력관리가 용이**합니다.

결재요청 및 승인이력 등 요청 리스트를 한 눈에 확인할 수 있어 편리한 이력관리 가능

결재자 추가 및 삭제 등 유연한 관리를 위한 결재선 지정

NO	승인상태	요청업무	요청자	일부	요청일시	완료일시
19999	승인	그룹이름칭 자산 이동	전성희 (seonghee@ssrinc.co.kr)		2020-05-27 12:12	2020-05-27 12:12
19998	반려	진단결과 현황 수정	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	-
19997	진행중	결과조치 등록 or 변경	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	-
19996	진행중	결과조치 삭제	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	2020-05-26 11:12
19995	승인	사전조치 등록	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	2020-05-26 11:12
19994	반려	사전조치 변경	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	2020-05-26 11:12
19993	진행중	사전조치 삭제	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	-
19992	진행중	조치담당자 등록 or 변경	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	-
19991	승인	조치담당자 삭제	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	2020-05-26 11:12
19990	반려	조치담당자 교체결과조치 삭제	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	2020-05-26 11:12
19989	진행중	사전조치 등록	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	2020-05-26 11:12
19988	진행중	사전조치 변경	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	2020-05-26 11:12
19987	승인	사전조치 삭제	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	2020-05-26 11:12
19986	반려	조치담당자 등록 or 변경	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	2020-05-26 11:12
19985	진행중	조치담당자 삭제	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	2020-05-26 11:12
19984	진행중	조치담당자 교체	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	2020-05-26 11:12
19983	승인	결과조치 삭제	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	2020-05-26 11:12
19982	반려	사전조치 등록	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	2020-05-26 11:12
19984	진행중	사전조치 변경	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	2020-05-26 11:12
19983	진행중	사전조치 삭제	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	2020-05-26 11:12
19982	반려	조치담당자 등록 or 변경	전성희 (seonghee@ssrinc.co.kr)		2020-05-26 11:12	2020-05-26 11:12

경로 > 그룹 > 그룹 > GROUP_1_2_1_1

자산그룹에 소속된 자산의 승인이 필요한 작업 요청에 사용되는 기본 결재선입니다. 승인이 필요한 작업으로는 조치관리의 사전조치, 결과조치, 조치담당자 지정 등이 있습니다.

1	ID	이름	부서	직급	이메일	사용자 타입
	adminadminimin	민진송	기술연구소	대리	admin@ssrinc.co.kr	관리자

2	ID	이름	부서	직급	이메일	사용자 타입
	adminadminimin	민진송	기술연구소	대리	admin@ssrinc.co.kr	관리자

3	ID	이름	부서	직급	이메일	사용자 타입
	adminadminimin	민진송	기술연구소	대리	admin@ssrinc.co.kr	관리자

결재자 추가

8. 자동 조치

자동조치 기능을 통해 **발견된 취약점을 자동으로 신속하게 조치**하게 함으로써, 불필요하고 반복적인 업무를 줄이고 효율적으로 취약점을 관리할 수 있습니다.

취약점 자동조치, 조치 원복, 조치 및 원복 이력 등 관리 가능

자동조치 항목별로 문제점을 세분화하여 취약점 조치 가능

취약점 조치

자산정보	권한대상	취약코드	취약명	vNo	문제장태	취약점 조치 조치 원복
ERP_WEB	Linux	SRV-028	권력 디버깅 접속 타임아웃 설정 미흡	1	ssrinc 계정의 TMOU: 999초 (/home/ssrinc/profi	보기 및 선택
ERP_WEB	Linux	SRV-028	권력 디버깅 접속 타임아웃 설정 미흡	2	test1 계정의 TMOU: 설정 미준제 (/home/test1/pro	
ERP_WEB	Linux	SRV-028	권력 디버깅 접속 타임아웃 설정 미흡	3	root 계정의 TMOU: 설정 미준제 (/etc/profile)	
ERP_WEB	Linux	SRV-028	권력 디버깅 접속 타임아웃 설정 미흡	4	remote 계정의 TMOU: 설정 미준제 (/etc/profile)	
ERP_WEB	Linux	SRV-048	불필요한 웹 서비스 구동중 (apache2)	1	불필요한 웹 서비스 구동중 (apache2)	
ERP_WEB	Linux	SRV-069	비밀번호 관리정책 설정 미비	1	root 계정의 패스워드: 최소 사용 기간 미설정	
ERP_WEB	Linux	SRV-069	비밀번호 관리정책 설정 미비	2	ssrinc 계정의 패스워드: 최소 사용 기간 미설정	
ERP_WEB	Linux	SRV-069	비밀번호 관리정책 설정 미비	3	test 계정의 패스워드: 최소 사용 기간 미설정	
ERP_WEB	Linux	SRV-069	비밀번호 관리정책 설정 미비	4	operation 계정의 패스워드: 최소 사용 기간 미설정	
ERP_WEB	Linux	SRV-084	시스템 주요 파일 권한 설정 미흡			
ERP_WEB	Linux	SRV-084	시스템 주요 파일 권한 설정 미흡			
ERP_WEB	Linux	SRV-093	불필요한 world writable 파일 존재			
ERP_WEB	Linux	SRV-093	불필요한 world writable 파일 존재			
slm_db1	Oracle	DBM-001	유주가능한 비밀번호 설정여부(DB계정)			
slm_db1	Oracle	DBM-001	유주가능한 비밀번호 설정여부(DB계정)			
slm_db1	Oracle	DBM-007	비밀번호 복잡도 설정			
slm_db1	Oracle	DBM-007	비밀번호 복잡도 설정			
slm_db1	Oracle	DBM-007	비밀번호 복잡도 설정			
slm_db1	Oracle	DBM-007	비밀번호 복잡도 설정			
slm_db1	Oracle	DBM-007	비밀번호 복잡도 설정			
slm_db1	Oracle	DBM-007	비밀번호 복잡도 설정			

취약점 조치

조치 대상으로 선택한 취약점

자산정보	권한대상	취약코드	취약명	vNo	문제장태	취약점
ERP_WEB	Linux	SRV-069	비밀번호 관리정책 설정 미비	1	root 계정의 패스워드: 최소 사용 기간 미설정	5
ERP_WEB	Linux	SRV-069	비밀번호 관리정책 설정 미비	2	ssrinc 계정의 패스워드: 최소 사용 기간 미설정	
ERP_WEB	Linux	SRV-069	비밀번호 관리정책 설정 미비	3	test 계정의 패스워드: 최소 사용 기간 미설정	
ERP_WEB	Linux	SRV-069	비밀번호 관리정책 설정 미비	4	operation 계정의 패스워드: 최소 사용 기간 미설정	
ERP_WEB	Linux	SRV-084	시스템 주요 파일 권한 설정 미흡	1	/etc/shadow 파일에 'other' READ' 권한 설정됨	

선택하지 않았으나 동시에 조치되는 취약점

자산정보	권한대상	취약코드	취약명	vNo	문제장태	취약점
ERP_WEB	Linux	SRV-001	SNMP Community 스트루명 설정 미흡	1	Public SNMP 커뮤니티의 복잡도 미흡	1

이 진단에 대한 백업이 존재하지만 현 시점으로 새로운 백업을 만들지 않습니다.

취약점 자동조치, 조치 원복, 조치 및 원복 이력 등 관리 가능

자동조치 항목별로 문제점을 세분화하여 취약점 조치 가능

사용자가 선택한 자동조치를 통해 영향이 가는 항목에 대해 알림 기능 제공

9. 클라우드 플랫폼 진단

클라우드 및 컨테이너 환경의 자산에 대한 취약점 진단이 가능하며, 클라우드 보안인증제(CSAP) 등의 컴플라이언스 대응을 지원합니다.

The screenshot displays the SolidStep CCE Vulnerability Scanner interface. On the left, a sidebar lists various asset categories including Cloud (AWS, Azure, GCP), Application (Docker, RHEV, Kubernetes, OpenStack, Hadoop), and Hypervisor (ESXi, Xen, KVM, HyperV). The main panel shows a list of assets with their respective scores and status. A modal window titled '자산 등록' (Asset Registration) is open, allowing users to manually register cloud assets. The modal includes fields for '진단 대상' (Diagnosis Target) set to 'Cloud', '진단대상 선택' (Diagnosis Target Selection) with a dropdown menu showing 'AWS', 'Azure', and 'GCP', '호스트명' (Host Name), 'IP', and '그룹' (Group). Buttons for '취소' (Cancel) and '확인' (Confirm) are at the bottom.

클라우드 플랫폼을 수동으로 자산 등록하여 진단 수행 가능

다양한 종류의 클라우드 플랫폼 진단 가능

자산명	점수	상태	OS	IP	플랫폼
평균 점수	70.5				
debian	62.7	정상	OS	192.168.201.11	Linux
APHKO2NWL3_1A	82.7	수동등록	OS	10.249.92.2	Cisco
manho	-	정상	OS	192.168.202.11	Linux
qwfwfwwf	-	수동등록	OS		
manho_cisco_test	-	수동등록	OS		
DESKTOP-OE05573	73.3	정상	OS		
대체호스트	-	미응답	OS		
cisco	-	수동등록	OS		
DESKTOP-PAS5H7R	-		OS		

10. 안전한 시스템 관리

시스템 영향을 최소화하기 위한 자산의 **Agent CPU 사용률 조절 기능**과 안전한 시스템 관리를 위해 **알림 기능** 및 **사용자 계정관리, 권한별 접근관리** 기능을 제공합니다.

The screenshot displays the SolidStep CCE management console. On the left, a dark red sidebar contains a navigation menu with options like '관리시스템', 'Agent', '진단 모듈', '접근 제어', '사용자 관리', '자산 관리', '자산그룹 관리', '보고서', '문제 관리', '로그', '라이선스 정보', and '제품 정보'. The 'Agent' menu item is highlighted with a red box. The main content area is divided into two panels. The top panel, titled 'Agent 기본 설정', includes settings for '통신 주기 설정' (31), '로그 설정' (로그 용량 제한: 100 MB, 로그 보관 기간: 365), 'CPU 사용 제한 설정' (6), '리소스 모니터링 경고 설정' (CPU, HDD, MEM, PROCESS thresholds), '진단정보 자동수집 설정' (ON), and '업그레이드 제한 설정' (최대: 100). A callout box points to the 'CPU 사용 제한 설정' field with the text '선택한 자산의 Agent CPU 사용률 조절'. The bottom panel, titled '관리시스템 기본 설정', includes '메일 발송' (smtp settings), 'AGENT 로그 보관' (ON, 300 days), '타이틀 문구' (Vulnerability Scanner), and '보안성 점수 등급' (slider from 0 to 100). A callout box points to the '관리시스템' menu item with the text '다양한 설정들을 통해 안전하고 편리한 시스템 관리'. A third callout box at the bottom left points to the sidebar with the text '다양한 Agent 기본 설정 기능 개별 시스템 설정 값이 없는 경우 Agent의 기본 설정을 통해 일괄 적용 가능'.

04. 레퍼런스

1. 주요 고객사 리스트
2. 적용사례

1. 주요 고객사 리스트 (1/3)

SolidStep은 전 산업분야의 다양한 환경에서 **단일 사업 최대 규모의 라이선스 계약, 설치 및 운영 레퍼런스**를 보유하고 있습니다.

60,000대 이상 납품 계약 및 설치, **500,000회 이상** 진단 수행

공공

 문화체육관광부	 방위사업청	 관세청	 식품의약품안전처	 국가보훈처	 한국전력공사	 한국석유공사	 한국도로공사
 한국철도공사	 한국토지주택공사	 HUG 주택도시보증공사	 PORT OF INCHON	 부산항만공사	 울산항만공사	 KAC 한국공항공사	 국립전파연구원
 서울시농수산물공사	 대한민국 법원	 국군기무사령부	 국군사이버사령부	 군사안보지원사령부	 KIDA 한국국방연구원	 한국원자력환경공단	 한국수력원자력
 한국에너지	 KOMIPO 한국중부발전	 한국남부발전	 한국동서발전	 한국환경공단	 KOEM 해양환경공단	 KIST 한국과학기술연구원	 한국재정정보원
 KISA 한국인터넷진흥원	 국가평생교육진흥원	 한국교육개발원	 KERIS 한국교육학술정보원	 KSD 한국에탁결제원	 KOIHA 의료기관평가인증원	 울산광역시교육연구원	 KBSI 한국기초과학지원연구원
 한국신용정보원	 국방기술품질원	 ICMTC 민군협력진흥원	 한국콘텐츠진흥원	 FACT 농업기술실용화재단	 M 군인공제회	 KINS 한국원자력안전기술원	 원자력안전위원회
 KRI 한국철도기술연구원	 KARI 한미항공우주연구원	 게임물관리위원회	 KIBO 기술보증기금	 국방과학연구소	 부산광역시교육청	 세종특별자치시	 Jeju 제주특별자치도
 충청남도	 전라남도	 성남시	 구리 시민행복	 평택시	 거제시	 목포시	 고성군

.....

1. 주요 고객사 리스트 (2/3)

금융

교육기관/병원

1. 주요 고객사 리스트 (3/3)

일반기업



2. 적용사례

K보험사



- 인프라 전체에 대한 단기간의 진단 필요
 - 1,600대 이상 시스템 진단 수행
- 관련 법규 및 전자금융감독규정 준수
 - SolidStep을 통해 기존 컨설팅 대체
 - 향후 지속적인 항목 업데이트 지원
- 연간 스케줄 및 이벤트 발생 시 수시 점검
 - 신규, 변경되는 시스템에 대한 즉각적인 보안 점검
 - 지속적으로 상향되는 보안 수준의 객관적 평가 수행

인프라 전체에 대한 단기간의 전수검사로 비용 절감

기존 인력투입 컨설팅을 솔루션으로 대체함으로써 리소스 절감

전자금융감독규정 준수로 컴플라이언스 완벽 대응

L통신사



- 3사 통합에 따른 다양한 종류의 시스템 진단 필요
 - Windows, AIX, Solaris, HP-UX, Linux 5종 진단
 - 아키텍처에 따른 12종류의 진단 모듈 실행
- 최고의 안정성이 확보된 진단 필요
 - 서버 운영자 직접 실행 방식 선택
 - 10년 이상 운영된 레거시 시스템의 안정적 진단
- 격리 네트워크에 위치한 시스템 진단 필요
 - 오프라인 수집 결과의 관리서버 자동화 처리

컨설팅 수준의 인프라 전수검사로 비용 및 리소스 절감

보안지침 준수 여부 감사 및 보안수준 수치화로 보안체계 확립

실시간 보안 취약점 자동 점검으로 보안 수준 강화 및 안정화

H기업



- 해외법인 여건 상 단기간의 구축 및 진단 필요
 - 1,300대 이상 시스템 진단 수행
- 해당 해외지역 법규 분석에 기반한 진단항목 개발 필요
 - 국내 컴플라이언스 준수사항 대응 및 해외 법규 대응이 가능한 항목 개발
- 연간 스케줄 및 이벤트 발생 시 수시 점검
 - 신규, 변경되는 시스템에 대한 즉각적인 보안 점검
 - 향후 지속적인 취약점 항목 개발 협의 가능

인프라 전체에 대한 단기간의 전수검사로 비용 절감

분석을 통한 맞춤형 신규 진단 항목 개발로 해외 법규 대응 가능

상시 자동 취약점 점검 체계 구축으로 보안성 강화

SCAN ME



보안 취약점 진단 자동화 솔루션

Automatic Security Vulnerability Scanner



www.ssrinc.co.kr



(주)에스에스알

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

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

Copyright © SSR INC. ALL RIGHTS RESERVED.