SolidStep

(인프라 보안진단 관리 솔루션)

(주)에스에스알

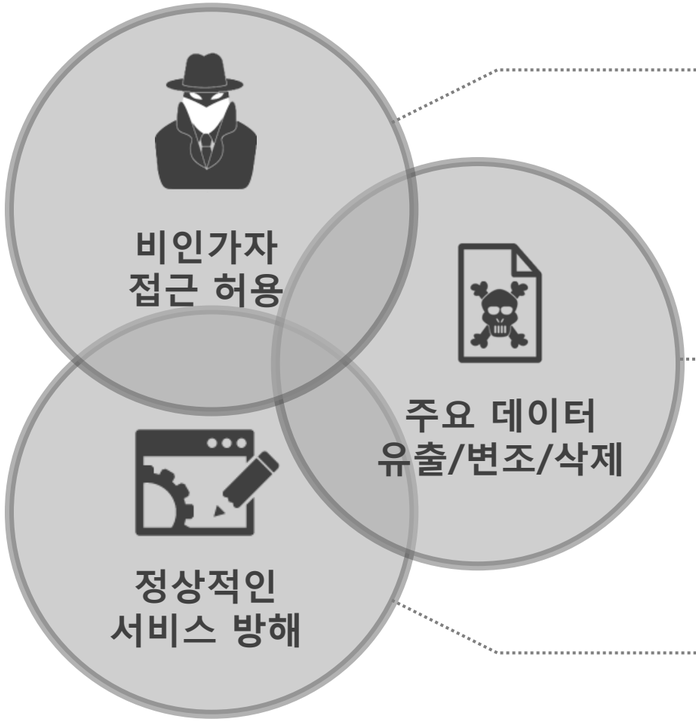
Brain Beyond Brands

1. 취약점진단 이란?

취약점 (脆弱點, Vulnerability) 컴퓨터의 H/W, S/W의 결함이나 설계(설정)상의 허점



취약점 **악용**



- ✓ 악의적 크래커의 침투
- ✓ 내부 비인가자 통제 어려움

- ✓ 인사정보 및 기밀정보 유출
- ✓ 제품 설계도면 유출

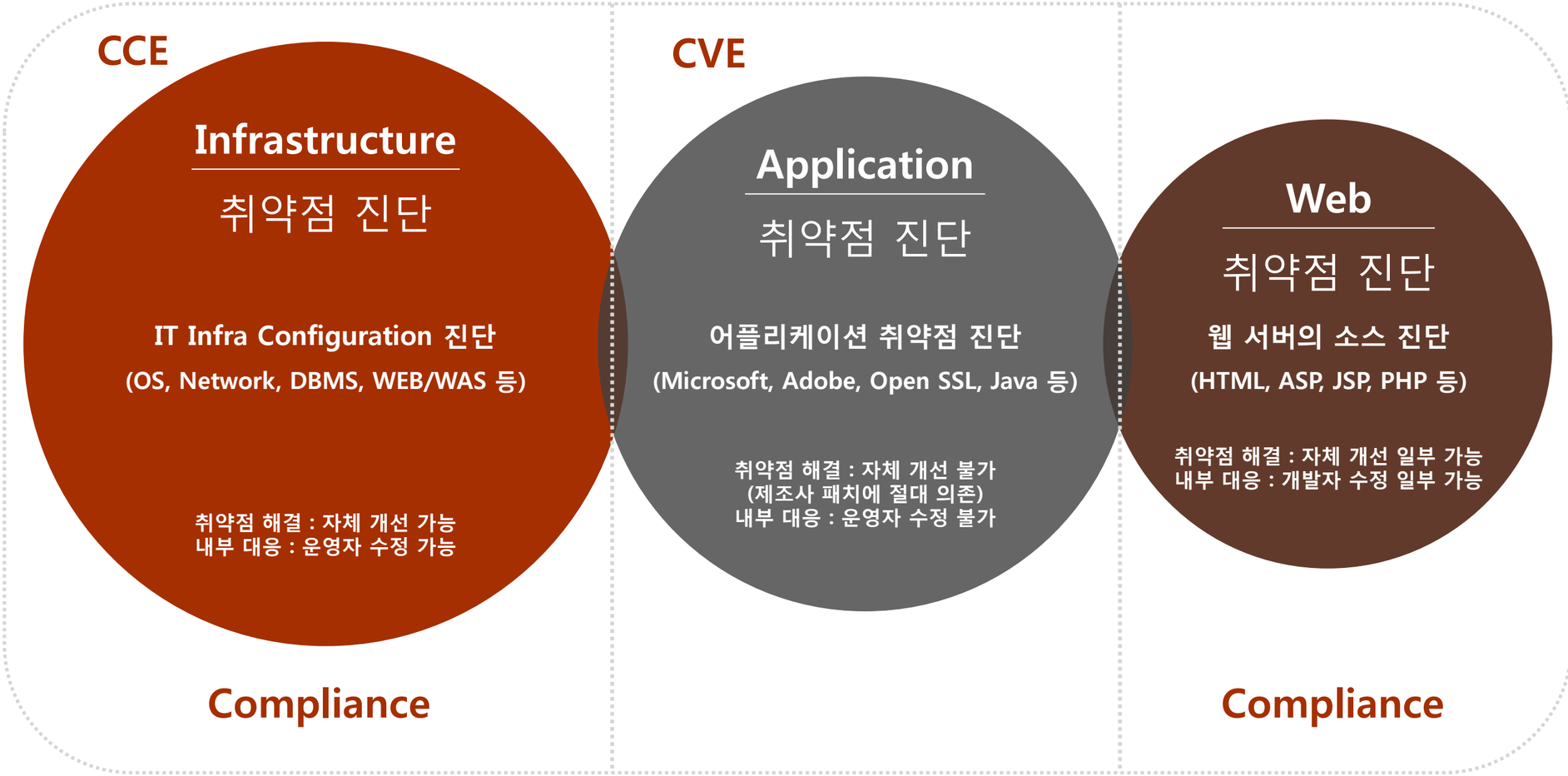
- ✓ 서비스 거부 공격 (DoS)
- ✓ 서비스 차단 (Interruption)

現 조직의 현황파악 기술적 분석

연간 위험관리 활동 : 정보보호 컨설팅, 내부 보안감사 등

Brain Beyond Brands SSR

2. 취약점진단 유형

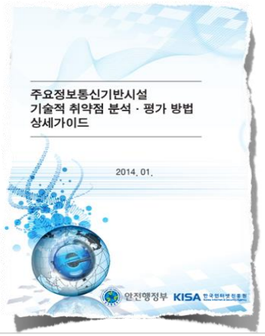


취약점 진단의 컴플라이언스는 **자체적으로 개선이 가능**한 인프라 및 웹 취약점을 위주로 선정

Brain Beyond Brands SSR

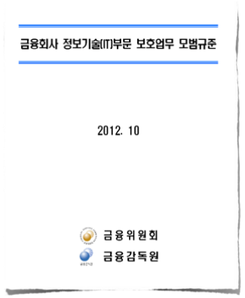
3. 강화되는 정보보호 관련 법규 준수사항

정보통신기반보호법

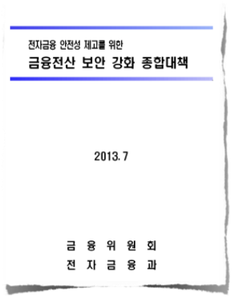


- ✓ 주요정보통신 기반보호시설 관리기관은 **매년 취약점 분석/평가를 실시**하여야 함 [정보통신기반 보호법 제 9조]
- ✓ Unix, Windows, Network 장비, DBMS, WEB/WAS, 보안 장비, 제어시스템, PC에 대한 **설정현황을 확인**
- ✓ 총 **313** 개의 **기술적 점검항목**에 대해 취약여부를 점검

전자금융거래법 + 금융위원회



- ✓ 전자금융기반시설에 대해 **매년 정기평가** 실시
- ✓ 금융회사의 **취약점 분석, 평가 결과 및 이행 실태를 점검**
- ✓ **CEO 책임**하에 취약점 점검 및 보완조치 이행 철저



- ✓ 시스템 계정 사용권한, 접근기록 등 **중점 관리 및 통제**
- ✓ 非 **금융 전산시스템**까지 취약점 점검 확대
- ✓ 정보보안 조직은 임직원의 **IT 보안법규 준수 여부**를 **정기적으로 점검**하고, 결과를 **CISO 및 CEO에 보고**

Brain Beyond Brands SSR

4. 현재 수행되고 있는 컨설팅 취약점 진단의 현황

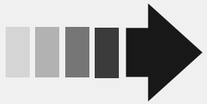
구분	내용
How Often?	1~2회 / 1년
How Much?	Man/Months (50EA:Max.)
What Method?	Script
What Target?	**Sampling**

조직의 IT 인프라에 대한 취약점 전수진단 수행비용 예시





1M/M : **10,000,000원**



예상비용 : 약 100,000,000원



Brain Beyond Brands SSR

5. 현재 컨설팅 취약점 진단의 한계점 및 개선 방향

구분	내용	문제점
How Often?	1~2회 / 1년	자산의 **신규도입** or **서비스 변경** 시 누락위험
How Much?	Man/Months (50EA:Max.)	**기존 고비용** 저효율 방식 -> 고급인력의 **스케쥴 종속**
What Method?	Script	**텍스트 형태의 결과 저장** 및 관리자 **계정 공유**
What Target?	**Sampling**	매년 **진단대상이 중복**될 가능성 높음

문제점 개선방향

변경관리와 연동
취약점 상시 관리체계
구축 및 이행

인력 → 솔루션
자동화 수행으로
예산 및 리소스 절감

암호화 저장 및 관리
내부 인력이
직접 진단 수행

중요순위를 탈피
전 인프라 대상
취약점 진단 수행

現 **수행방법의 구조적, 비용적 한계는 자동화 솔루션 도입을 통한 패러다임의 전환으로 개선이 필요!!!**

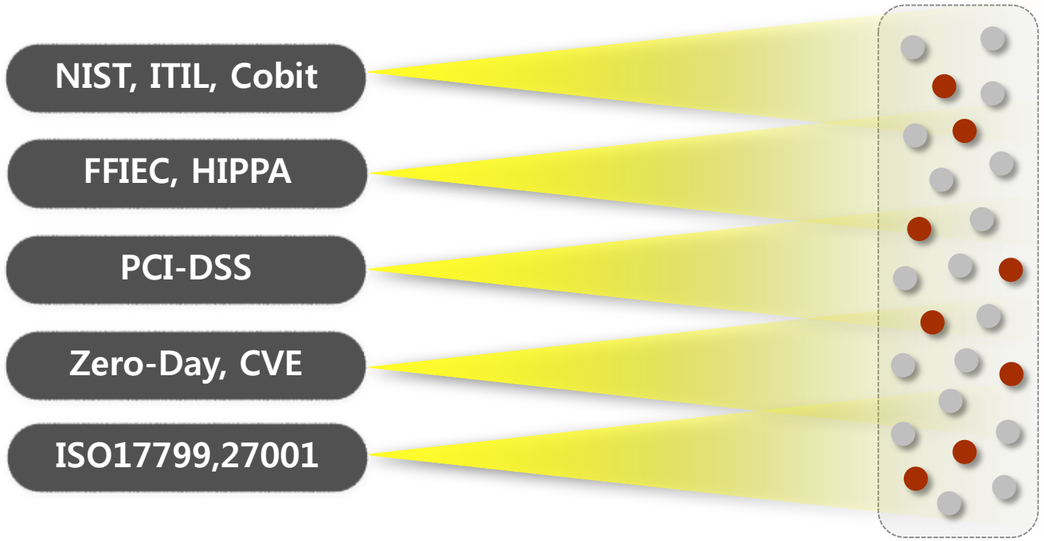
Brain Beyond Brands SSR

“진단 솔루션의 필수요건”

1. 보안기준 매칭

Q. 내・외부의 다방면으로 주요 보안기준을 만족하는가?

기존 취약점 진단 솔루션



: Non-Compliance Item : Compliance Item

- ✓ 대외적으로 오픈된 알려진 항목 (내부 환경과 큰 **GAP**이 존재)
- ✓ 대부분 외국 기준으로 진단하여 국내환경 적용이 미흡
- ✓ 컨설팅을 대체할 만큼의 수준의 진단이 불가 (항목 및 수준)

국내 인프라 환경의 요구사항



: Non-Compliance Item : Compliance Item

- ✓ 관련 법률 및 컴플라이언스 진단항목은 반드시 포함
- ✓ 폐쇄망 점검 및 고도화 수준의 진단 필요 (**컨설팅 대체**)
- ✓컨설팅을 대체하는 솔루션 도입으로 인한 ROI 확보 보장

Brain Beyond Brands SSR

2. 보안기준 매칭 - 계속

Q. 정책 및 지침 항목과 솔루션 평가 항목이 **일치**하는가?

내부 정책 (가이드)

패스워드

영문, 숫자, **특수문자**를 혼용하여 **9자리** 이상으로 사용한다.

ex) **abc1234!@#** ->조건만족

계정잠금

계정입력의 오류가 5번 이상일 경우, 잠금처리하고 잠금기간은 60분으로 한다.

✓정책 및 지침은 조직환경에 따라 **상이하게 구성**

진단항목

패스워드

영문, 숫자를 혼용하여 **8자리** 이상으로 사용하는가?

ex) **abc12345** ->내부정책조건 미달

계정잠금

진단항목이 존재하지 않음.

✓진단기준과 내부항목 **매칭이 필수**

결과 리포트

결과 : 양호

영문, 숫자를 혼용하여 **8자리**로 사용.

진단기준은 만족하나, 실제 정책의 준수 확인은 미흡.
따라서, **진단결과를 신뢰할 수 없음.**

진단불가

해당 취약점 **진단수행 불가**.

✓진단결과의 신뢰도는 **항목일치 여부에 종속**

일치하지 않은 평가기준으로 진단하는 솔루션의 경우 결과의 신뢰도 및 활용 가능성 저조

Brain Beyond Brands SSR



SolidStep

보안진단매니저

Brain Beyond Brands

1. 내부 정책기반의 최적화 진단

내부 정책 (가이드)

계정잠금

계정 로그인의 **오류가 5회 이상**일경우, 계정은 잠금 처리한다.

패스워드 최대 사용기간

패스워드의 최대 사용기간은 **최대 90일**이다.

진단항목

항목명	로그인 실패 횟수 제한
분류	계정관리
보안기준	* 로그인 실패 횟수 제한이 5회를 초과하여 설정되어 있으면 취약하다. * 로그인 실패 제한 횟수 확인 - Linux cat /etc/pam.d/system-auth | grep tally

항목명	패스워드 최대 사용 기간 제한
분류	계정관리
보안기준	* Linux, Solaris, HPUX(shadow 사용) : shadow 파일을 확인하여 다섯 번째 필드의 값인 패스워드 최대 사용기간이 90을 초과하여 설정되어 있다면 취약하다. * HPUX(trusted mode) : /tcb/files/auth/<계정명의 첫 번째 알파벳>/<계정명> 파일을 확인하여 u_exp(단위:초) 값이 7776000 보다 큰 값으로 설정되어 있다면 취약하다. * AIX : "/etc/security/user "파일을 확인하여, "maxage(단위:주)"의 값이 '13'보다 큰 값으로 설정되어 있다면 취약하다.

결과 리포트

코드	U-03	위험도	상	분류	계정관리
항목	로그인 실패 횟수 제한				
진단결과	미흡				
기준	로그인 실패 횟수 제한이 '5회 이상'(패스워드 정책에 따라)으로 설정되어 있으면 취약하다. 로그인 실패 제한 횟수를 확인한다.				
현황	문제점1. 로그인 실패 횟수 제한 설정 없음 참고. 진단 예외 계정 없음				
조치방법	로그인 실패 횟수 제한을 '5회 이하'로 설정한다. Linux "/etc/pam.d/system-auth" ⇒ "auth required pam_tally.so onerr=fail deny=3" 이하 양수 (Pam 인증 사용시 설정 가능) HPUX Solaris "/etc/default/login" ⇒ "RETRIES=3" 이하의 양수 AIX				

코드	U-08	위험도	중	분류	계정관리
항목	패스워드 최대 사용 기간 제한				
진단결과	미흡				
기준	Linux, Solaris, HPUX(shadow 사용) : shadow 파일을 확인하여 다섯 번째 필드의 값인 패스워드 최대 사용기간이 90을 초과하여 설정되어 있다면 취약하다.				
현황	문제점1. 계정 생성 시 기본 패스워드 최대 사용기간 무기한 문제점2. dbadmin 계정의 패스워드 만료 기간 없음 문제점3. root 계정의 패스워드 만료 기간 없음				
조치방법	새로 생성될 계정의 패스워드 최대 사용기간 설정을 위하여 아래 설정 파일을 수정한다. Linux Solaris "/etc/login.defs" => "PASS_MAX_DAYS 60" 이하 "/etc/default/passwd" => "MAXWEEKS=8" 이하 HPUX AIX				

정책의 세부 내용을 완벽하게 충족하는 항목으로 진단을 수행하여 결과를 100% 수용

Brain Beyond Brands SSR

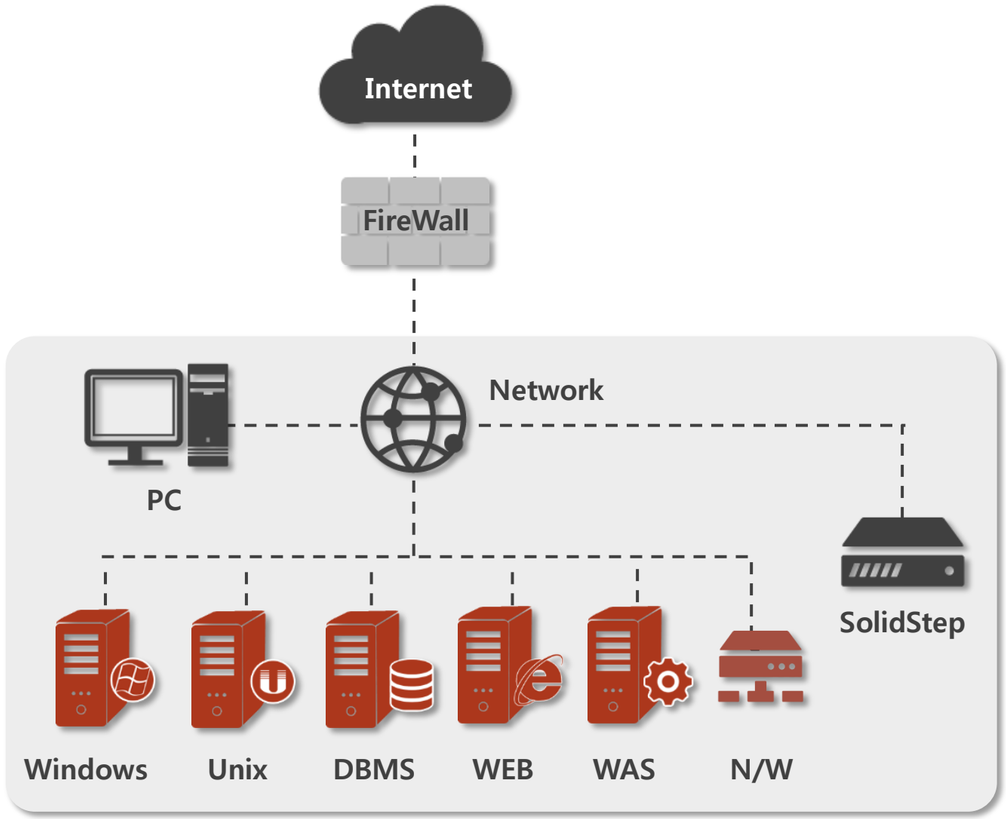
2. 취약점 진단 범위(2015. 05)

솔리드스텝 구성

		기본 진단		금융위원회	정보통신기반시설
OS	Windows	86	PASSED	28	80
	Linux	112	PASSED	34	65
	HP-UX, Solaris, AIX	112	PASSED	34	65
NETWORK	CISCO, Juniper, Alcatel Alteon, HP(3Com)	99	PASSED	28	80
WEB	Apache	18	PASSED	7	8
	I.I.S.	31	PASSED	15	16
	O.H.S.	12			
	WebToB	18			
	NGINX	14			
WAS	JEUS	20			
	Tomcat	17			
	WebSphere	15			
	Jboss	9			
	Weblogic	16			
DBMS	MS SQL	43	PASSED	13	25
	My SQL	33	PASSED	10	24
	Oracle	59	PASSED	13	24
	DB2	25			
	Sybase, Tibero, Altibase PostgreSQL, MariaDB	16			

Brain Beyond Brands SSR

3. 아키텍처



4-free

with Agent

Online

- **Install-Free**
  Portable 프로그램
  (재부팅 불필요)
- **Resource Free**
  CPU 소모량 1% 이하
- **OS Free**
  Windows, Linux, AIX, HP-UX
  Solaris 등 5종 지원
- **ACL Free**
  Agent Port Listening 없음
  HTTPS Protocol 이용

Agentless

- **SSH, Winexec를 이용한 점검**
  Agent 설치관련 운영 이슈 Zero, Agent 방식과 동일한 결과 보장
  서버 접속정보 입력 및 관리 필요, 네트워크 접근 ACL필요
  부가기능(리소스 모니터링 등) 이용불가, 예약진단 이용불가

Offline 암호화된 정보 수집 파일 수동 반영

Password Crack (3-Ways)

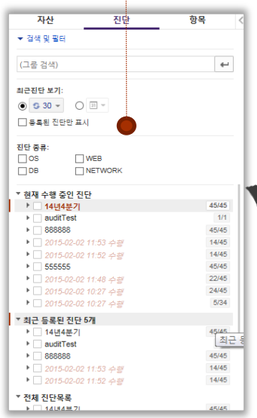


Brain Beyond Brands SSR

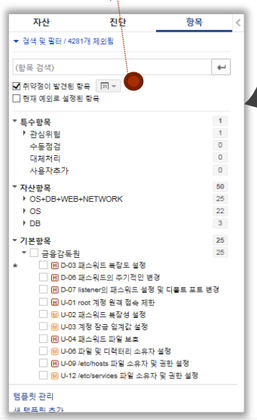
4. 기능 – Gmail like UI

SolidStep은 편의성을 극대화 하기 위한 플랫 메뉴 방식의 화면과 무엇이든 검색 가능한 토큰 인터페이스를 제공합니다.

✓ 진단 현황/검색/필터



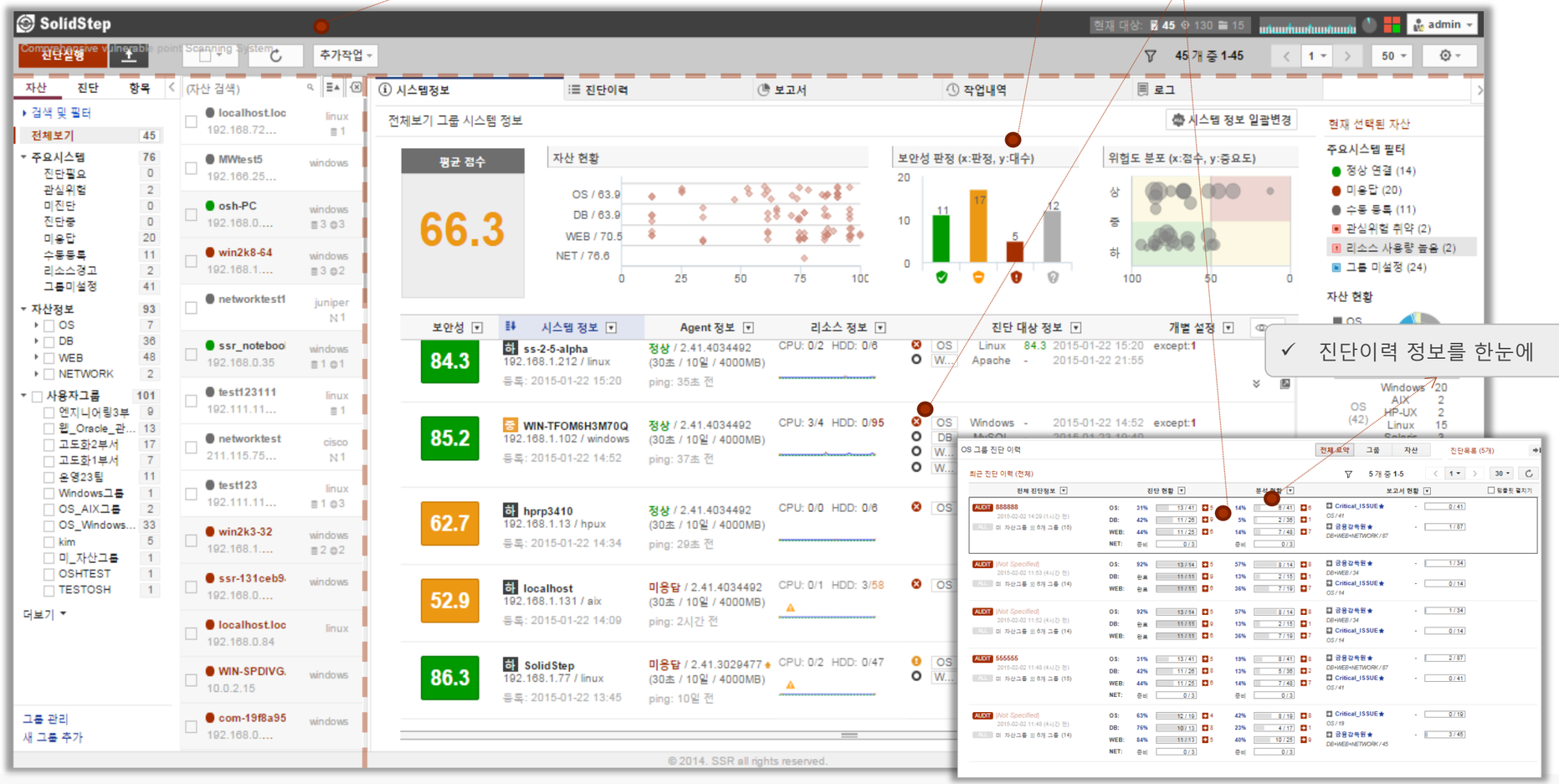
✓ 진단 항목 사용 현황
✓ 검색/필터/예외 등



✓ **3 분할 화면** *사용편의를 위해 상/좌 패널은 항상 고정*
-상) 진단실행, 각종 필터, 시스템 리소스 대시보드
-좌) 자산/항목/템플릿
-우) 진단관련 모든 정보

✓ 꼭 봐야 하는 지표들만 대시보드 화

✓ 각종 아이콘과 색상으로 클릭 없이 모든 정보 표시

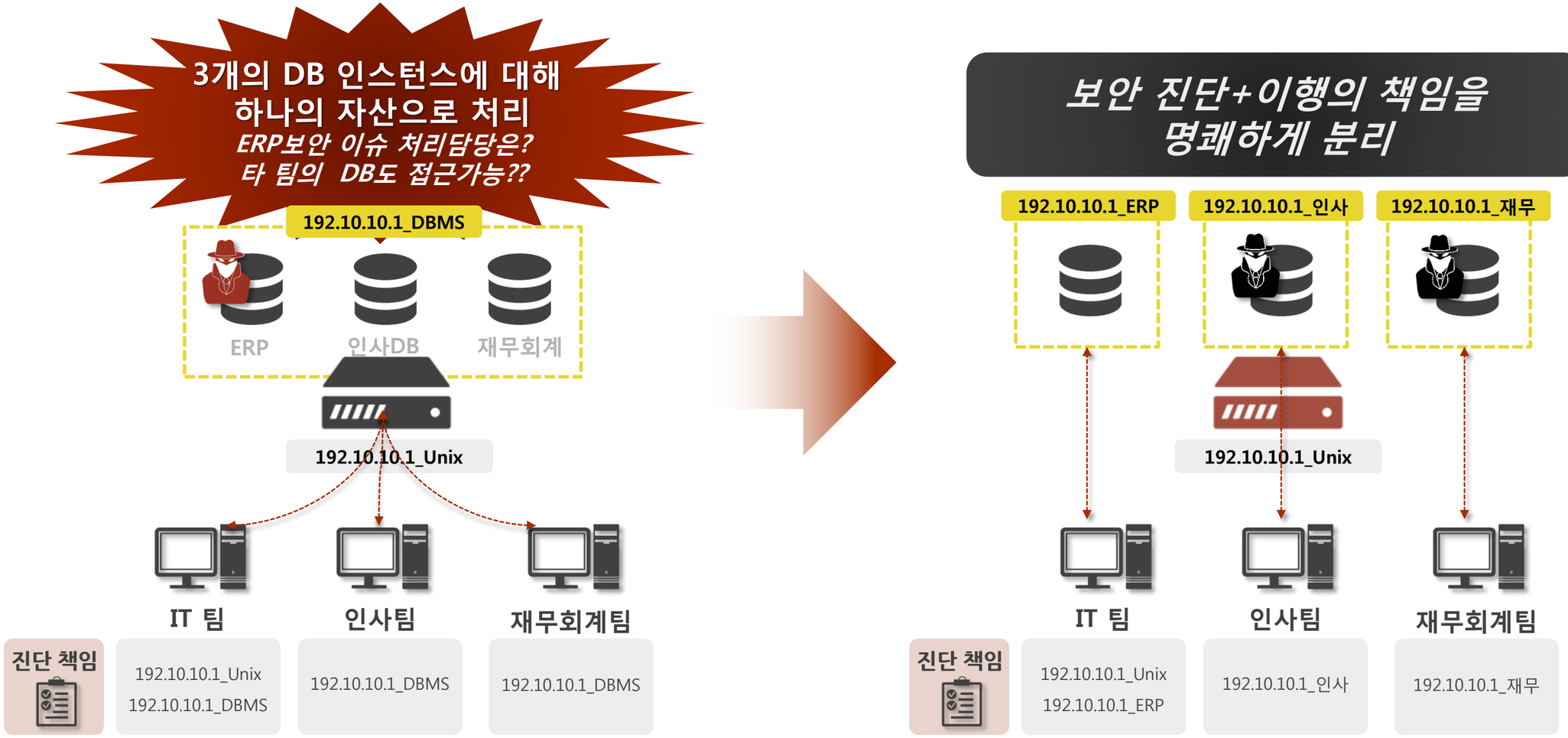


✓ 진단이력 정보를 한눈에

Brain Beyond Brands SSR

4. 기능 - 자산관리

물리 또는 IP 기반으로 자산을 등록하는 일반적인 취약점 진단 솔루션은 하나의 자산을 여러 부서에 할당하거나 자산을 중복 등록하는 등의 이슈가 발생하므로 원활한 보안관리 활동이 어렵습니다. SolidStep은 이러한 현실을 고려하여 **논리적인 자산(인스턴스) 등록을 통해 진단/이행 부서 간 원활한 업무 진행이 가능**하게 합니다.

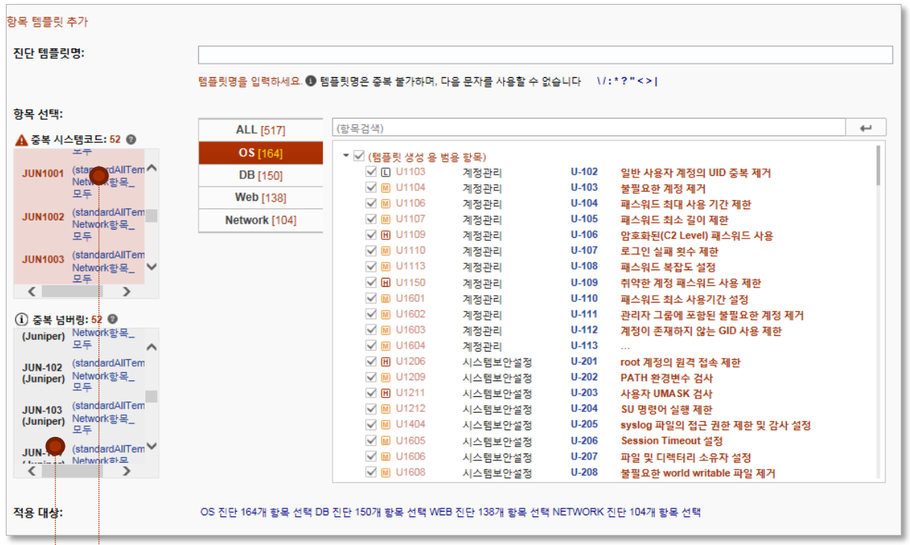


Brain Beyond Brands SSR

4. 기능 – 진단 실행

순수하게 진단업무 중심으로 UI가 구성되어 어디에서나 '진단실행'버튼에 접근하여 진단할 수 있으며, 오류를 즉각적으로 알려줌으로써 빠르게 진단 템플릿을 생성/적용할 수 있게 합니다.

즉각적인 오류검증 → 빠르고 쉬운 진단 템플릿 생성



2개 이상의 동일 id를 포함하여 템플릿을 만들 수 없습니다. 중복 id 는 상위 1개만 포함되었으니 확인하여 중복을 제거하세요.

진단 대상이 같은 항목에 대해 2개 이상의 동일 넘버링이 선택되었습니다. 템플릿을 만들 수 있지만 진단 결과에 동일한 넘버링이 중복으로 나타납니다.

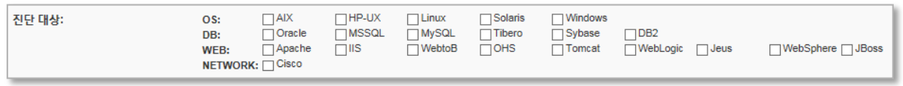
1

✓ 중복 ID 자동 체크

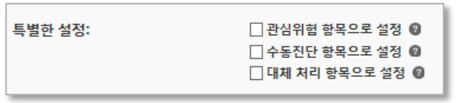
✓ 중복 넘버링 체크

자세한 진단 항목 정의

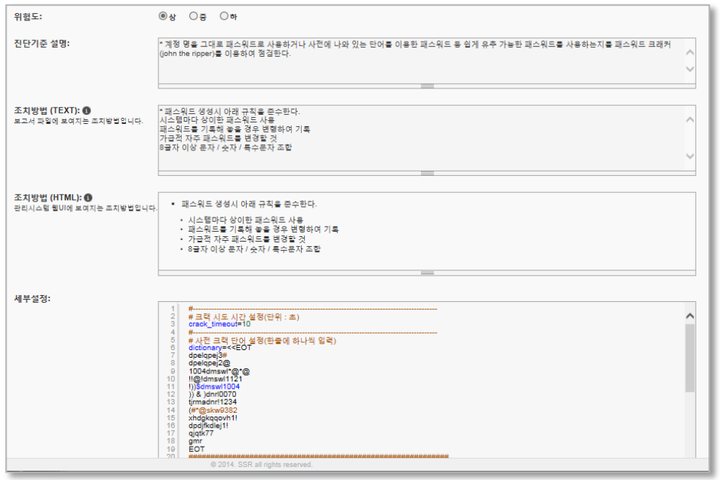
2 ✓ 다양한 진단 대상의 지원



3 ✓ 고객환경에 따라 처리할 수 있는 예외를 설정으로 정리

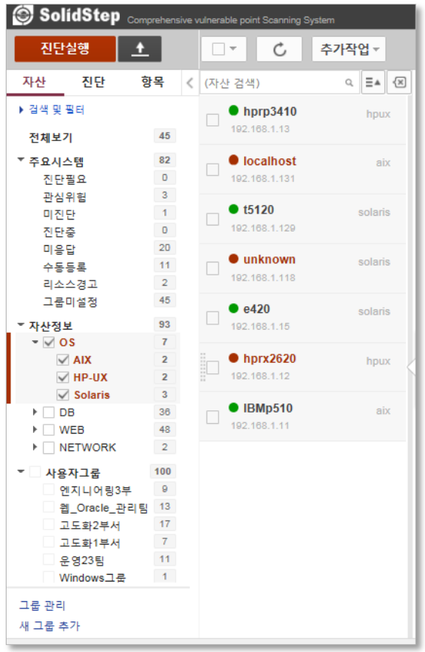


4 ✓ 조치방법의 보고서, 웹UI 구분하여 설정, 세부설정의 문법 컬러링 표시



3 Steps, OK !

1. 진단대상 선택
2. 진단실행
3. 시작

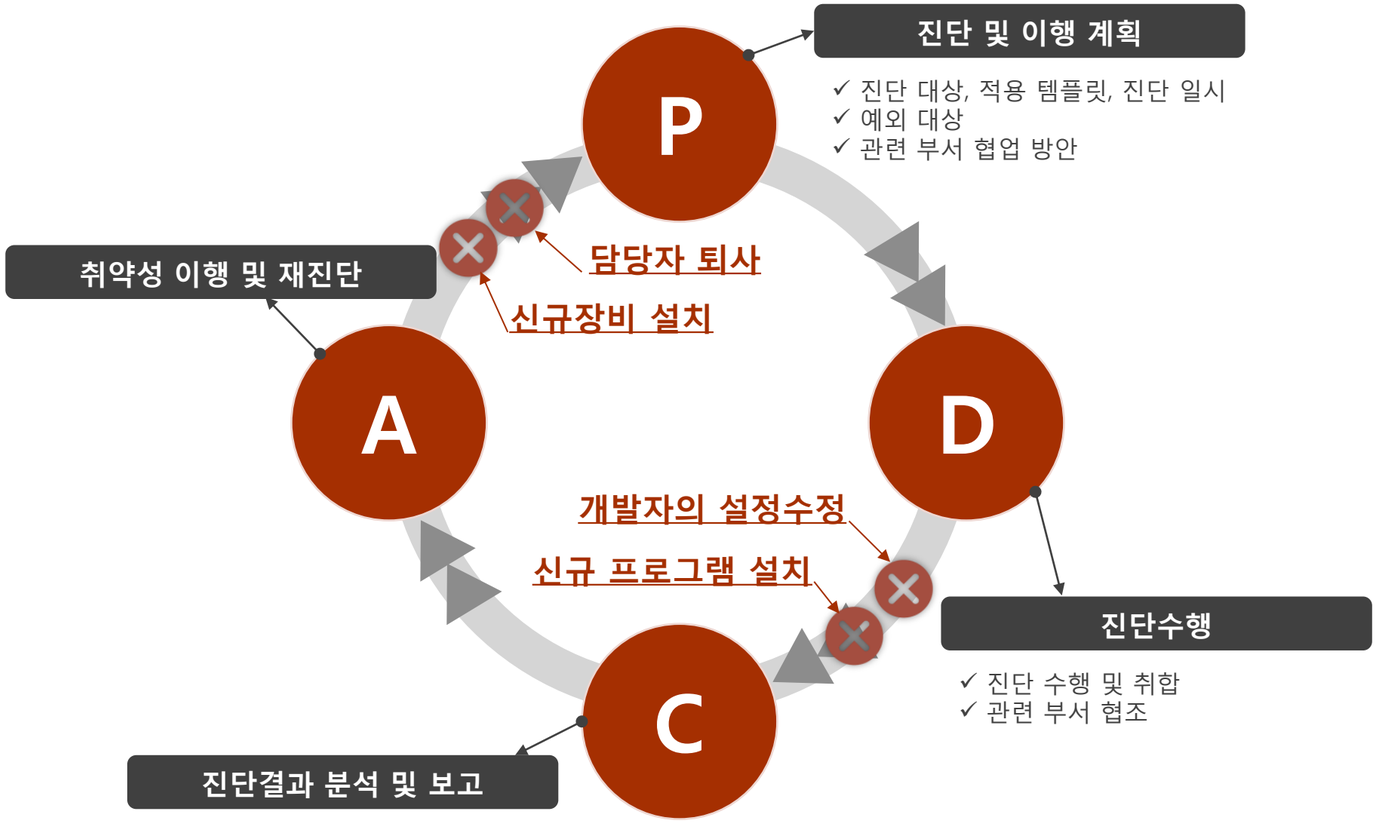


Brain Beyond Brands SSR

4. 기능 – 변경 감시 및 자동 진단

SolidStep 2.5는 진단 수행 이후 발생할 수 있는 설정의 변경을 모니터링하여 진단함으로써 **보안의 항상성을 스스로 유지합니다**. 변경사항을 자동 진단하고 보안 준수 여부를 알려줍니다.

진단Cycle과 보안설정의 변경 이슈



SolidStep 자동진단

CASE 1.

신규 또는 삭제 발생

- 자산 스캔
- 신규자산은 담당자에게 알림
- 최초 진단 수행
- 분석 및 이행

CASE 2.

설정 변경 발생

- 담당자에게 알림 + 자동 진단 수행
- 진단 결과 전송
- 변경사항 육안확인

Brain Beyond Brands SSR

4. 기능 – 진단 옵션

다양한 고객대상 컨설팅 경험을 바탕으로 보안진단의 어려움을 예외처리 옵션항목으로 구현, 진단결과를 편리하게 종합할 수 있도록 하였습니다.





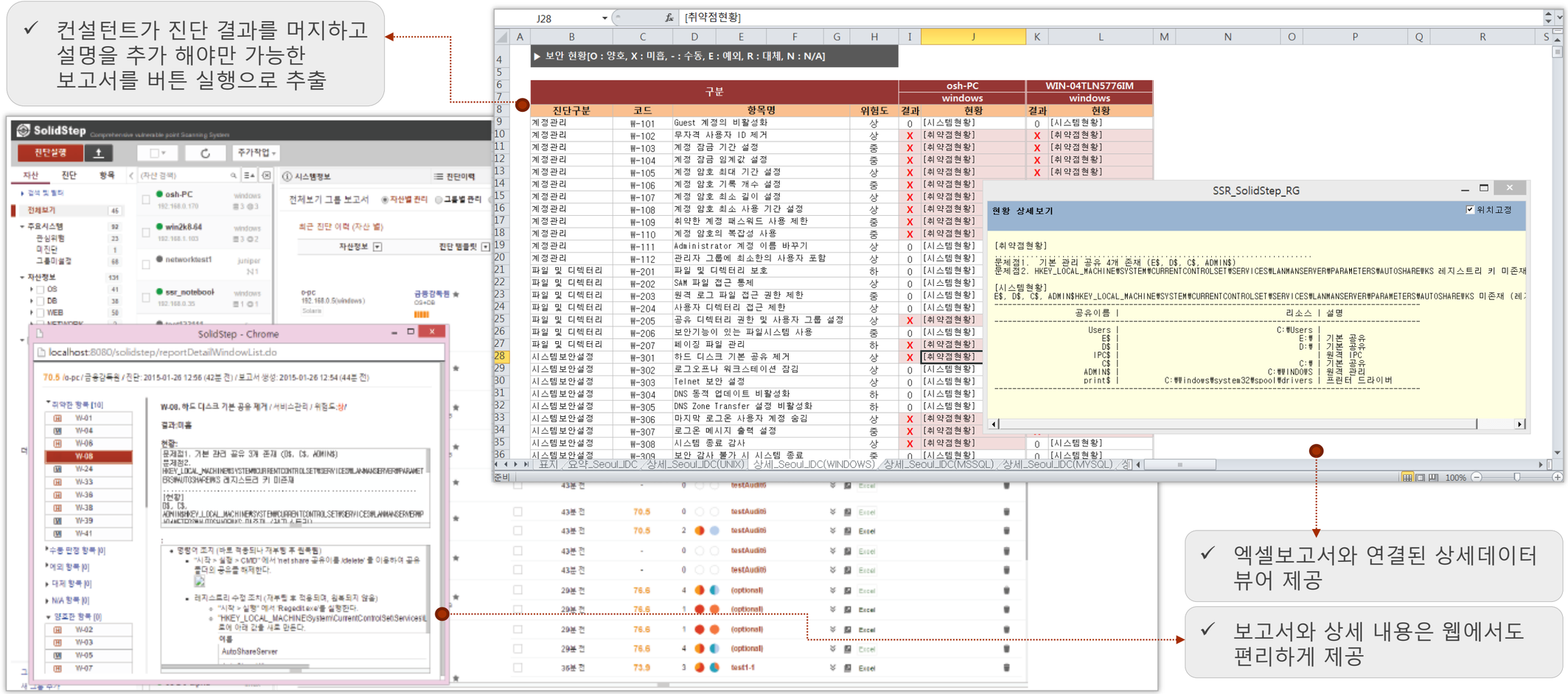
- ✓ 제외 대상 포함하여 보안점수 측정
- ✓ 원격 연결 방법을 통한 진단 포함
- ✓ 모든 대상에 대해 다시 진단(기 진단 대상을 포함)
- ✓ 기간 내 진단결과를 포함하여, 진단 내역이 없는 대상만 진단 후 종합적인 진단 결과 추출
- ✓ 진단명이 없어도 생성 가능
- ✓ 적용 템플릿도 WISWIG 수정

Brain Beyond Brands SSR

4. 기능 – 보고서

수 많은 고객사가 검증하고 칭찬하는 보안진단 '보고서'를 (1)컨설턴트 수작업과 100% 동일한 엑셀 보고서 추출 (2)결과상세를 한눈에 알 수 있는 뷰어 기능으로 한층 강화하였습니다.

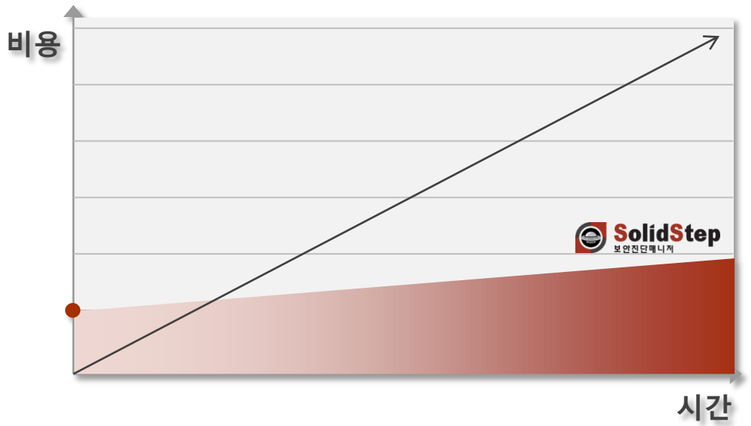
✓ 컨설턴트가 진단 결과를 머지하고 설명을 추가 해야만 가능한 보고서를 버튼 실행으로 추출



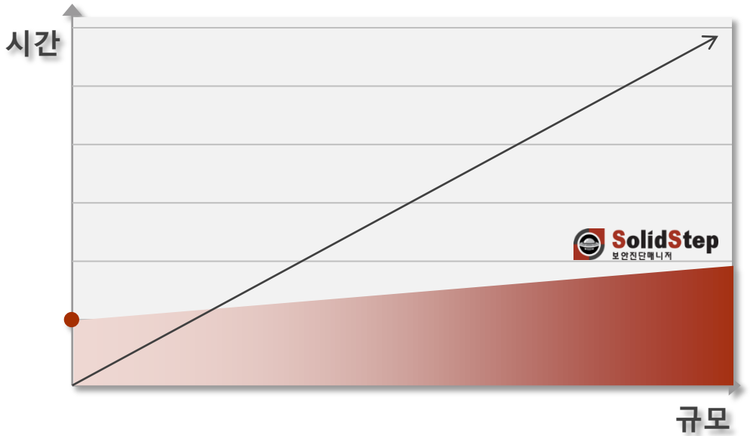
Brain Beyond Brands SSR

5. 솔루션 도입 기대효과

취약점 관리의 시간, 비용 리소스 절감



✓ 매년 진단에 필요한 예산을 집행하지 않고,
도입 시 구매 비용으로 반복 진단 수행가능



✓ 자산의 증가 및 진단대상을 확대(전수진단)해도,
추가적으로 발생하는 비용은 ZERO

인프라 보안관리의 상향 평준화

✓ 모든 인프라를 대상으로 수행되는 취약점 관리로 보안 수준이 상향 평준화하여 관리 가능

객관적으로 신뢰성 높은 수준향상 측정 가능

✓ 일관된 기준과 동일한 방법으로 수행되는 진단으로 인프라 수준의 향상도 측정이 가능

- 컨설팅 수행의 경우 수행 주체 별 방법론 및 숙련도의 차이로 기준이 동일하지 않으며, 인력의 정성적 평가 반영

Brain Beyond Brands SSR