Business Overview

SSR Security Strategy Research

Brain Beyond Brands SSR

1. 회사소개 - 개요

SSR은 과학기술정보통신부에서 지정한 정보보호 전문서비스기업으로 공공 및 대기업, 금융/교육/의료기관을 대상으로 취약점 진단, 정보보호 관리체계 수립, 개인정보보호 컨설팅, IT 솔루션 개발과 구축을 포함한 종합 보안 서비스를 제공합니다.

- 정보보호 전문서비스기업
- 개인정보 영향평가 기관
- LG CNS 보안컨설팅 특화업체
- MOU : 펜타시큐리티
- KISA 업무 공유

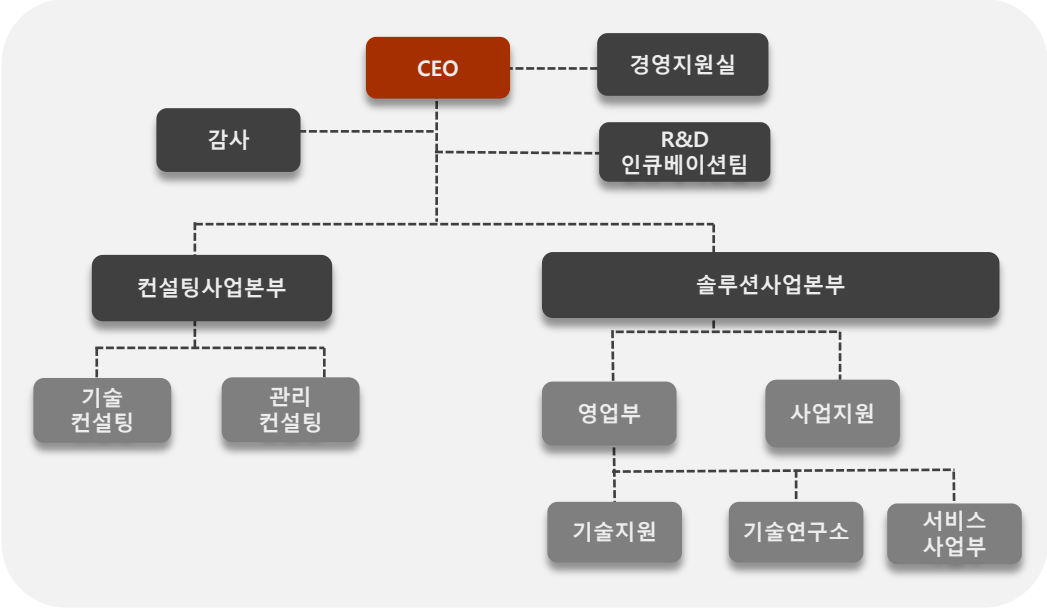
- 침투 성공률 100%
- 웹, 모바일, C/S 취약점 진단
- 인프라 시스템 보안진단
- 스마트 가전 보안진단
- 소스코드, 리버스 엔지니어링

- 정보보호 관리체계(국내, 글로벌)
- 개인정보보호 관리체계
- 주요정보통신 기반보호시설 진단
- 금융위원회 전자금융감독 규정 진단

- IT 인프라(서버, NW, DB, WEB) 진단
- 인프라 취약점 진단 클라우드 서비스
- 침입행위 탐지
- 웹 소스 변경관리
- 사회공학적 해킹 침투 방지 솔루션

1. 회사소개 – 인력 / 조직

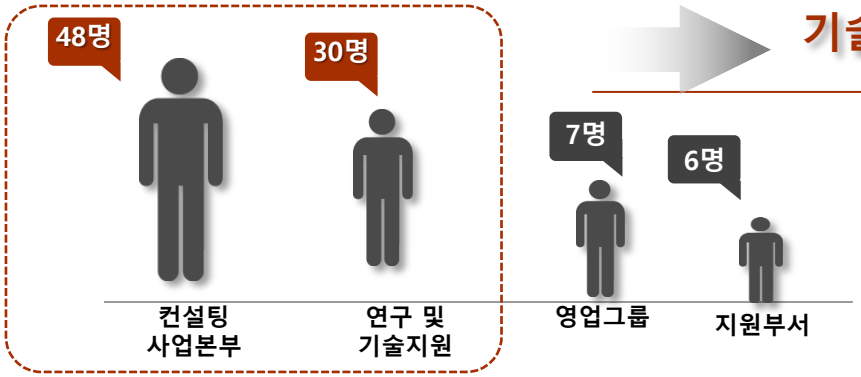
2018. 04월 현재 2개 본부, 1개 실, 7개 그룹, 1개 연구소, 23개 팀, 총 93명의 인원으로 운영되고 있으며, 전체 인원의 약 84%가 IT 보안기술 전문인력으로 구성되어 있습니다.



담당업무	인원
컨설턴트	48
연구, 개발 (R&D)	15
기술지원	15
영업	7
지원부서	6
경영진	2
인원 (명)	93

등급	인원
특급	4
고급	6
중급	18
초급	20
인원 (명)	**48**

★ MENSA 20명 !!



기술인력 78명

최대규모의 전문 인력!!

" SSR은 정보보호 전문서비스 기업으로
최고의 정보보호 전문가로
구성되어 있습니다. "

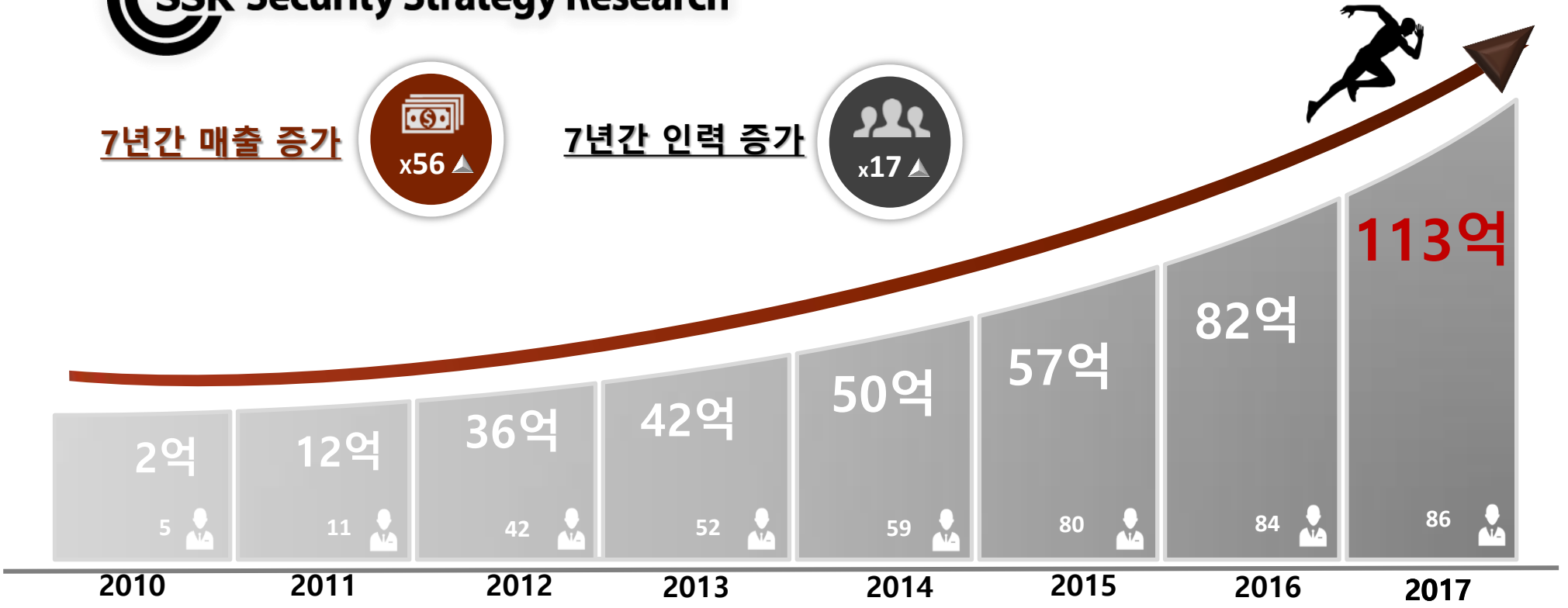
1. 회사소개 – 재무 구조

SSR의 주력사업인 정보보호 컨설팅 분야에서 괄목할만한 성장세를 꾸준히 유지하고 있으며, 2013년을 시작으로 정보보호 솔루션 사업에 전략적인 투자를 집중하여 설립 8년 만에 매출액 113억을 달성하는 쾌거를 이루었습니다.

SSR Security Strategy Research

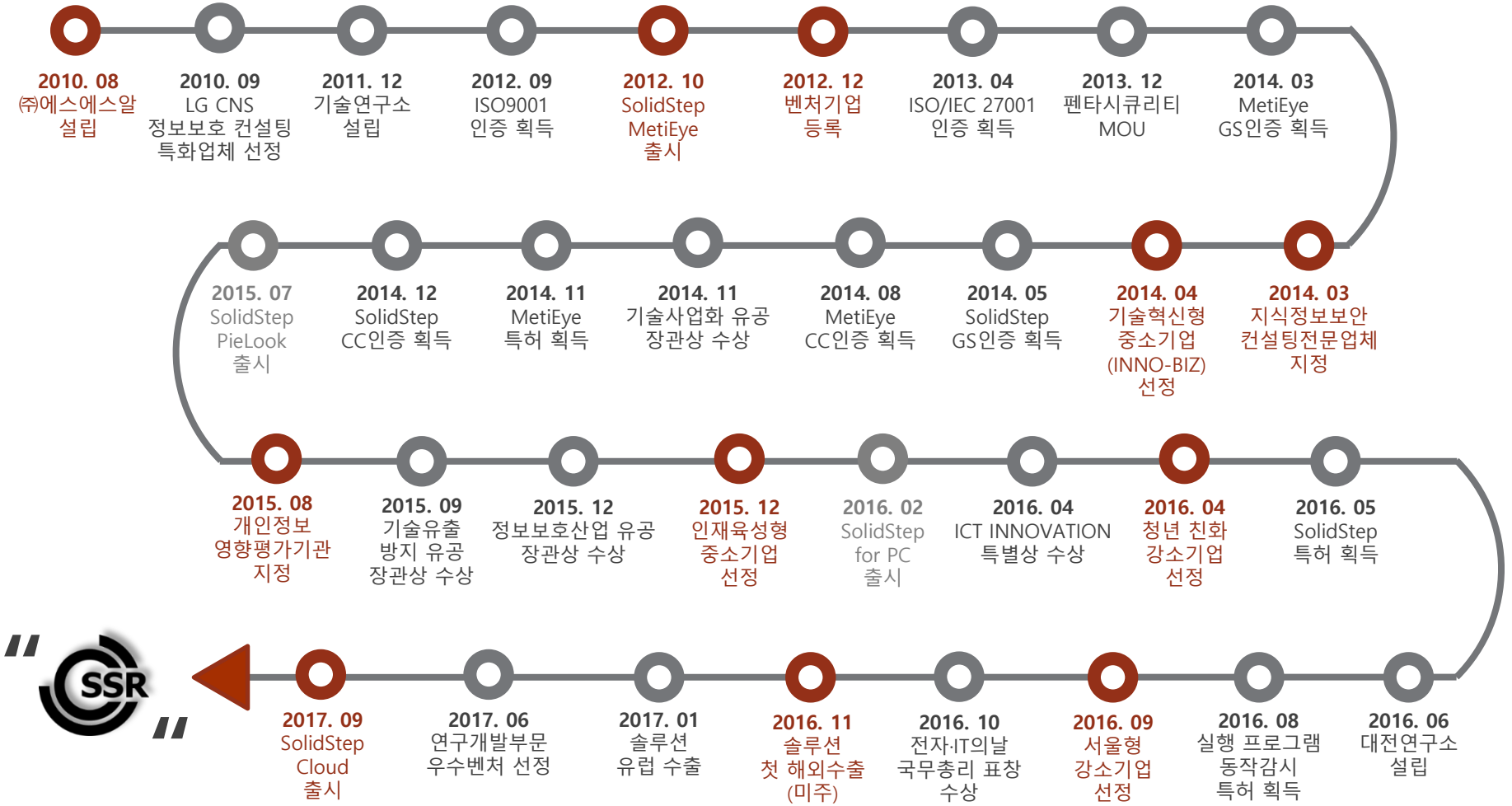
7년간 매출 증가 x56

7년간 인력 증가 x17



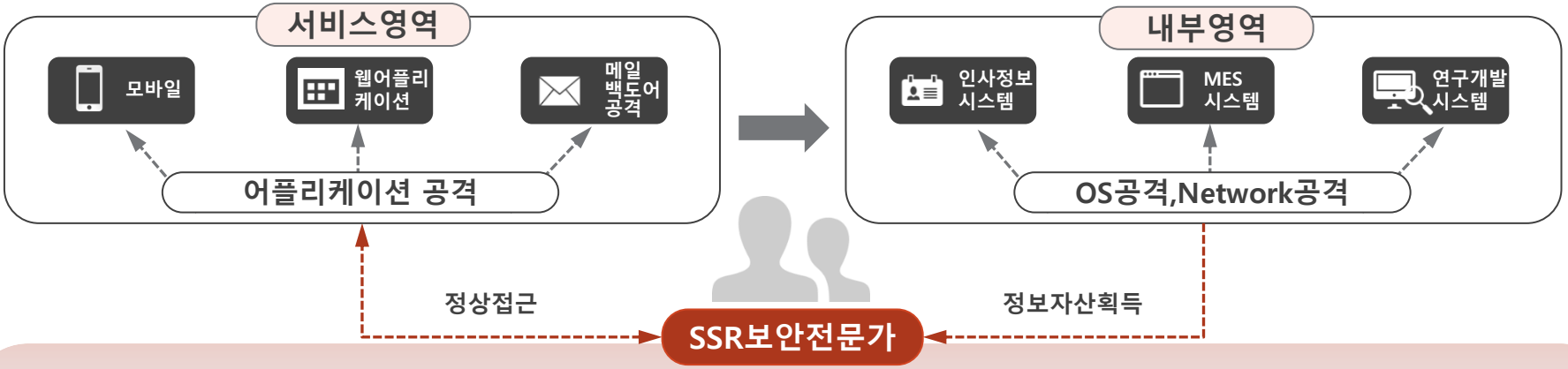
1. 회사소개 – 연혁

SSR은 2010년 8월 설립을 시작으로 해마다 훌륭한 발자취를 남기며 앞으로 전진하고 있습니다.



2.1. 모의해킹 컨설팅

SSR의 모의해킹 서비스는 고객사 비즈니스의 높은 이해도를 바탕으로 다양한 시나리오 기법을 적용하여 예상 위협에 대해 심도있는 분석을 수행하며, 100% 침투 성공률을 자랑합니다.



모의해킹전문가
보안전략팀

- SSR 모의해킹 감각이 뛰어난 보안 컨설턴트
- 100% MENSA로 구성
- SSR 최고 모의해킹 실력의 팀장

인프라전문가
기술컨설팅 1팀

- 서버, 네트워크, 보안장비 무선장비 등의 시스템 진단 전문가들로 구성
- CCIE, SCSA, SCNA, CISSP, OCP등의 자격 보유자들로 구성
- 시스템 및 보안등 다양한 경력의 팀장

모바일전문가
기술컨설팅 2팀

- 모바일 전문가들로 구성
- 스마트 가전 및 IoT 취약점 진단 수행
- 최신 기술에 강하고, 각종 해킹대회 입상자들로 구성
- 모바일 보안회사 출신의 팀장

리버싱전문가
기술컨설팅 3팀

- Reverse Engineering 전문가들로 구성
- 시스템 영역별 전문화된 해킹 툴 개발
- 오랜 리버싱 경력의 팀장

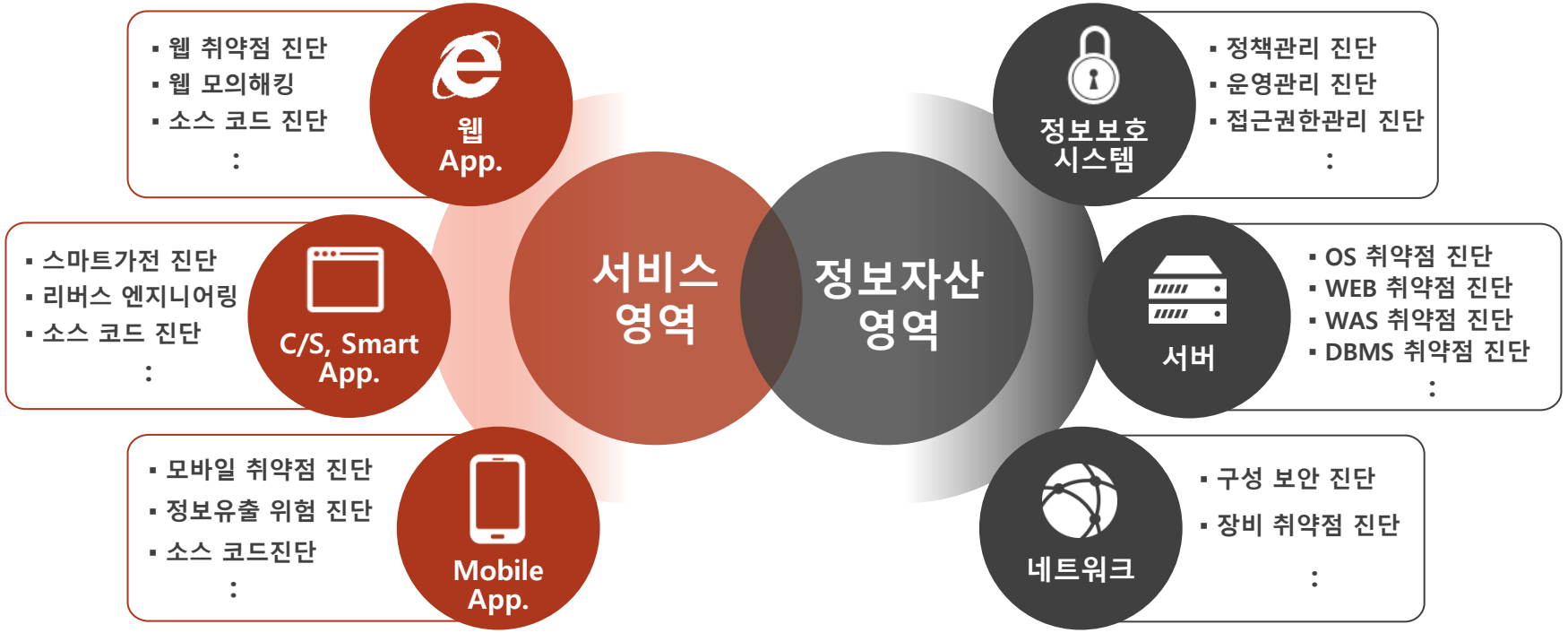
소스진단전문가
기술컨설팅 4팀

- 웹, 모바일, CS등의 프로그래머 경력을 보유한 보안 전문가들로 구성
- 리버싱팀과 더불어 각종 해킹 툴 및 보안모듈 개발
- 대기업 보안팀 출신의 팀장

SSR의 모의해킹은 각 분야의 전문가들이 다양한 방식으로 고객사의 보안 수준을 향상시켜 드립니다.

2.2. 정보보호 기술진단 컨설팅

SSR의 기술컨설팅은 서버, 네트워크, 웹, 모바일, 스마트가전 등 각 분야에 최적화된 인력으로 고도화된 컨설팅을 수행하며, 상시 진단이 가능하여 고객 맞춤형 컨설팅 서비스를 제공합니다.



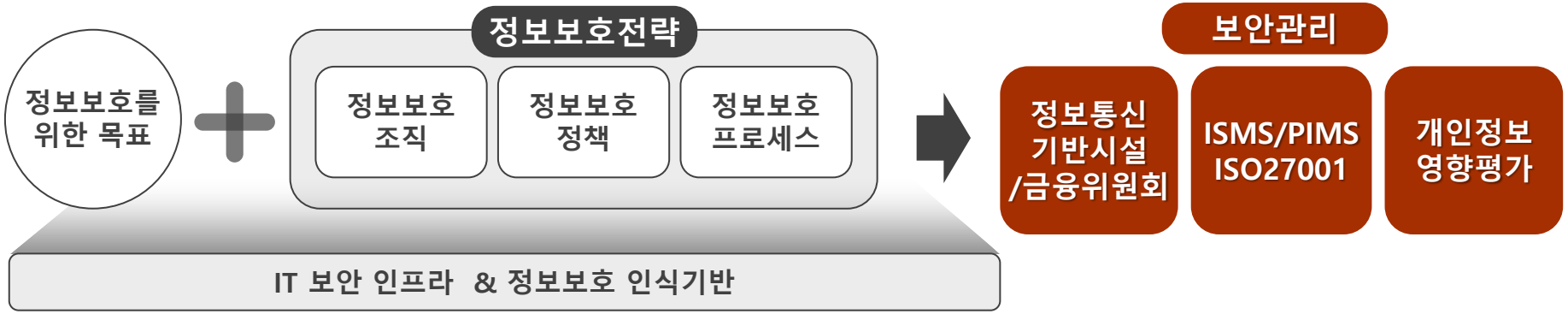
주요수행실적

상시 : 두산, 넥슨, LG U+, SK플래닛, eBay코리아
일반 : 옥션, LG전자, G마켓, BC카드, 현대 오토에버, 포스코, 다음, 국립재활원, 한국교육학술정보원, 현대 HMC 투자증권, 대림산업, 영남대학교, 질병관리본부 외 다수

2.3. 정보보호 관리 컨설팅

SSR의 관리 컨설팅은 다수의 프로젝트 경험을 기반으로 고객사의 다양한 환경에서 성공적인 지속가능 비즈니스를 위해 가시적인 정보보호 관리해법을 제공합니다.

▶ SSR의 관리컨설팅 서비스



관리체계

관리컨설팅 1팀

- ✓ 수립, 구현, 전파 등 각 역량에 최적화된 전문가
- ✓ 최고의 효율과 퍼포먼스로 무결점 프로젝트 수행
- ✓ 비즈니스 환경에 맞춘 산출물 제공

개인정보

관리컨설팅 2팀

- ✓ 영향 평가부터 관리 체계까지 1-Stop Service
- ✓ 관리 가능한 개인정보 체계 구현
- ✓ 고객 및 사내 개인정보 수준별 관리체계 적용

기반시설

관리컨설팅 3팀

- ✓ 금융위 취약점분석, 기반시설 취약점분석 전문팀
- ✓ 지속가능 비즈니스 환경 구축
- ✓ Self-care 모델을 통한 고객의 자체역량 강화

ISMS, PIMS	주요정보통신 기반보호시설	금융기관	개인정보 영향평가
ISMS, PIMS 규격에 따라 중요정보 및 개인정보 관리가 체계적, 효율적으로 운영되어 보안수준이 지속적으로 향상되도록 지원	국가 주요 기반시설의 주기적인 취약점 관리 및 보안수준 향상을 지원하고, 기간망 보안관리와 대국민 서비스의 가용성을 확보 지원	금융위원회 전자금융감독규정 및 관련 컴플라이언스를 충족하고, 특히 상대적으로 민감한 금융환경 보안수준을 향상시켜 기관 신뢰도의 완성을 지원	개인정보파일 구축·운영·변경 시 항목(수), 제3자 제공 여부, 정보주체의 권리 침해 가능성 및 그 위험 정도 등에 대한 침해요인 분석 및 개선사항을 도출

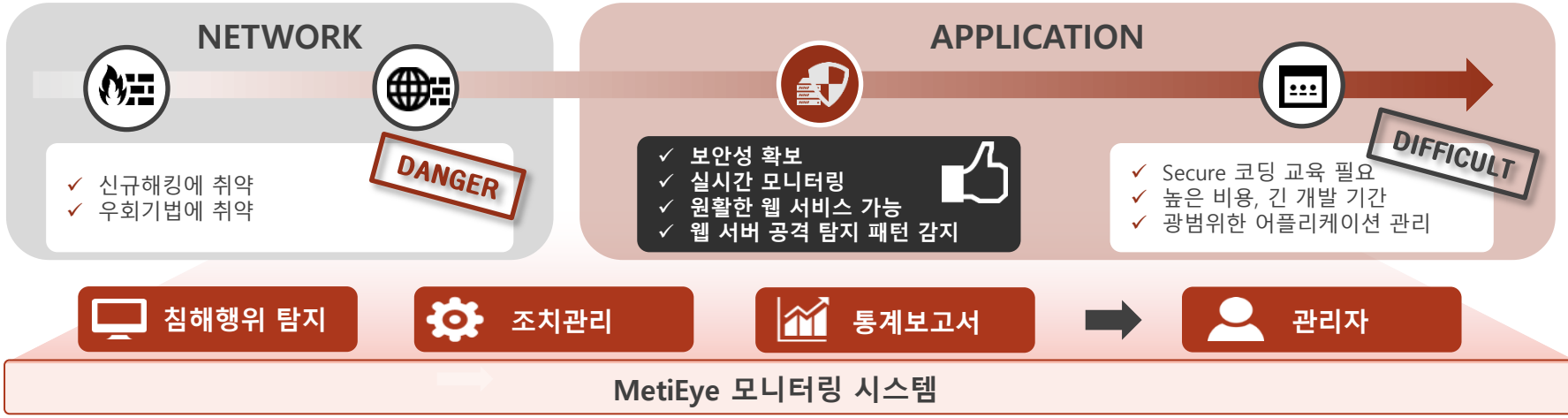
2.4. 정보보호 컨설팅 - 실적

SSR은 주요 공공기관 및 기업에 약 350건 이상의 정보보호 컨설팅을 제공하고 있습니다.
(2018년 06월 현재)

3.1. 실시간 웹 서버 방어 솔루션 - MetiEye

MetiEye는 웹서버 내 보안위협이 되는 악성파일 및 스크립트(웹쉘)의 출현 및 홈페이지 무단 위,변조 등을 실시간 탐지/차단하여 안전한 웹 서비스 운영 환경을 지원합니다.

▶제품개요



▶주요기능

웹쉘/악성 URL탐지	웹 소스 변경관리	파일생성 (업로드)제한	원격관리	엔터프라이즈급 관리UI

▶특장점

풍부한 해킹패턴수집/적용역량	기존 방식 대비 18배 수준의 빠른 탐지 속도
휴리스틱 탐지 기능을 통한 신, 변종 웹쉘 탐지	해시값 매칭 탐지 & 지속적인 해시값 업데이트
4-Free (Install, Resource, OS, ACL Free)로 인한 가용성	2중 암호화 설계 적용으로 안정성 보장

▶솔루션 지원

기술연구소	개발자 대다수 **보안컨설팅 수행 경력** 보유
컨설팅 사업본부	신규 및 변종 **웹쉘 패턴 개발 시 휴리스틱 엔진에 반영**

3.1. 실시간 웹 서버 방어 솔루션 – MetiEye (특장점)

실전 모의해킹 컨설턴트(웹쉘 개발 노하우 보유)에 의해 연구, 개발된 유일한 제품으로 정형화된 패턴탐지를 넘어 압도적인 탐지 능력으로 경쟁사 대비 높은 퍼포먼스를 자랑합니다.

▶ 차원이 다른 탐지 능력

1 업계 최고의 패턴수집/ 적용역량

정형화된 정규식 패턴 탐지 외 웹쉘 행위를 파악해 미등록 패턴 탐지 가능

2 지능형 탐지

신, 변종 웹쉘을 자동으로 탐지하는 지능형 휴리스틱 탐지

3 해시값 매칭 탐지

알려진 웹쉘에 대한 해시값을 판별하여 자동탐지 검역

4 빠른 속도의 알고리즘

S.R.O.A 아키텍처의 기존 대비 약 18배 향상된 빠른 탐지속도

▶ 최적화 아키텍처

5 서버 부담이 적은 초경량 Agent

4Free Agent 기술로 서버부담 최소화, 도입 피로의 최소화 가능

6 보안성 설계

1차, 2차 암호화를 통한 Agent, Manager 간 커뮤니케이션 간 안정성 보장

3.1. 실시간 웹 서버 방어 솔루션 – MetiEye (비교)

메티아이는 컨설팅전문업체에서 개발한 솔루션으로 실제 웹해킹에 대한 전문적인 노하우가 반영된 제품입니다.

솔루션의 태생이 다르다. – 정보보호 전문서비스 기업

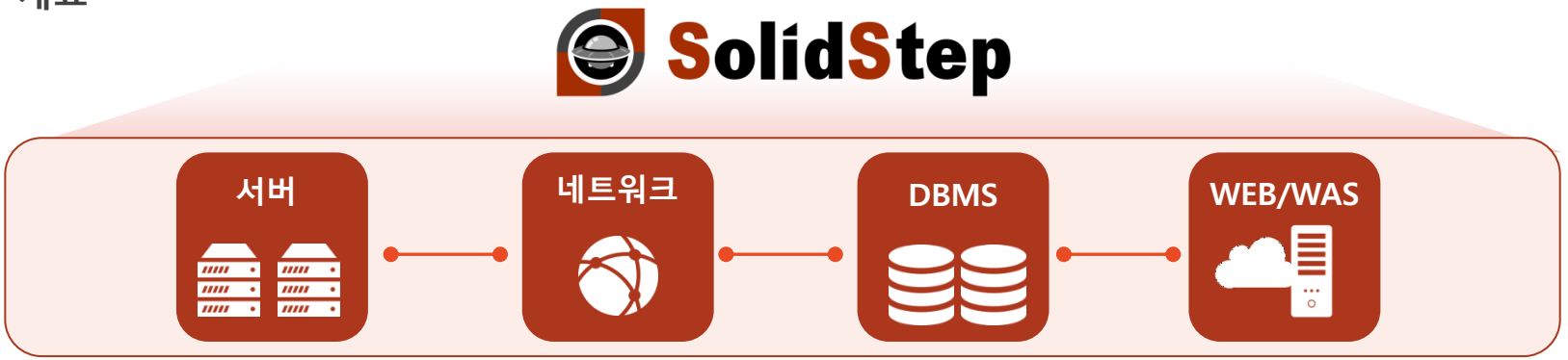
	MetiEye	타사 제품
개발인력	정보보호 컨설턴트 (해커)	IT Developer (개발자)
패턴 수집	내부 개발 + 외부 수집 (공급)	외부 공급에 의존 (내부역량 부재)
QA & Text	실전 웹쉘 공격 테스트	내부 구성 점검 (Coding Error)
신규 대응	최신 트렌드 연구 및 웹쉘 개발	외부 공급에 의존 (내부역량 부재)
사후 지원	컨설팅 트렌드를 반영한 업데이트	일반 유지보수 (H/W, S/W)

실제 웹쉘을 사용하여 모의해킹을 수행하는
전문 컨설턴트에 의해 개발되었습니다.

3.2. 인프라 취약점 진단 솔루션 - SolidStep

SolidStep은 서버, 웹, 네트워크, DBMS 시스템의 보안진단을 전수 자동화 수행하여, 전문인력 이상의 결과 보고서를 제공하고 누적된 통계 확인으로 보안수준의 향상을 측정 가능합니다.

▶제품 개요



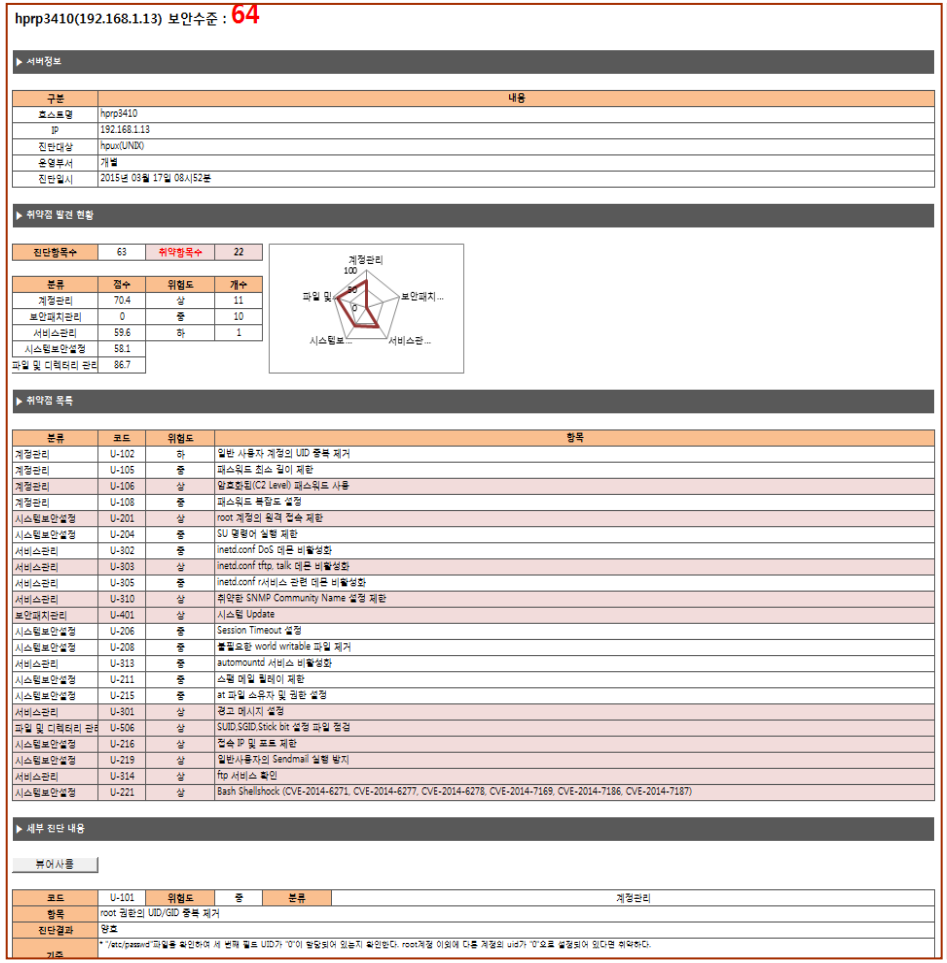
계정관리 | 파일 및 디렉토리 관리 | 서비스 관리 | 패치 및 로그관리 | 기능 및 옵션 관리 | 환경구성 관리 | 통계보고서

▶SSR의 솔루션과 일반 보안업체의 진단방식 비교

	방식	단위	정확도	속도	공수	금액	관리	보고서	안정성
기존 진단	샘플링	1M/M 100여대	±75%	보고서완료	1	1	기존결과와 비교불가	결과수정 시 재진단 필요	수집 데이터 평문저장
SolidStep	전수 검사	무한대	100%	단시간에 보고서출력	1/300	1/10	누적통계 보고서 가능	다양한 양식의 보고서 출력	수집 결과 암호화

3.2. 인프라 취약점 진단 자동화 솔루션 - SolidStep

SolidStep은 PC, 서버, 웹, 네트워크, DBMS 시스템의 보안진단을 전수 자동화 수행하여, 전문인력 이상의 결과 보고서를 제공하고 누적된 통계 확인으로 보안수준의 향상을 측정 가능합니다.



hprp3410(192.168.1.13) 보안수준 : 64

▶ 서버정보

구분	내용
호스트명	hprp3410
ip	192.168.1.13
진단대상	hpux(UNIX)
운영부서	개별
진단일시	2015년 03월 17일 08시52분

▶ 취약점 발견 현황

진단항목수	63	취약항목수	22

분류	점수	위험도	개수
계정관리	70.4	상	11
보안패치관리	0	중	10
서비스관리	59.6	하	1
시스템보안설정	58.1		
파일 및 디렉터리 관리	86.7		

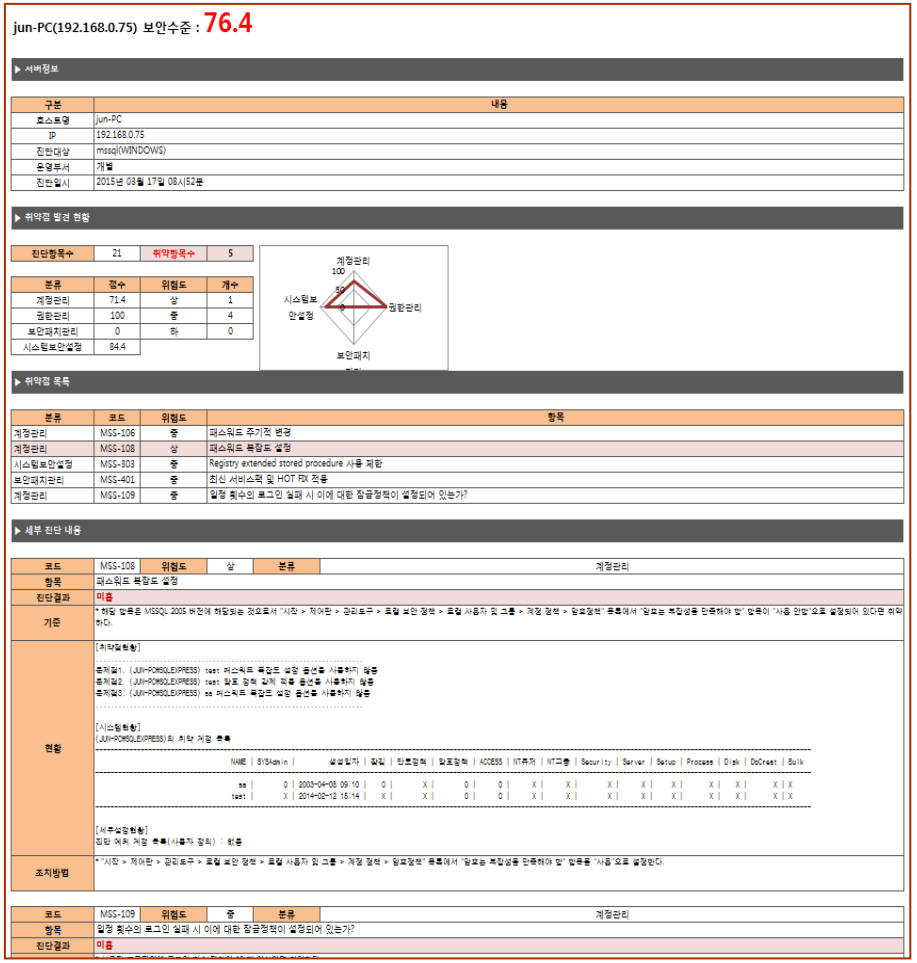
▶ 취약점 목록

분류	코드	위험도	항목
계정관리	U-102	하	일반 사용자 계정의 UID 중복 제거
계정관리	U-105	중	패스워드 최소 길이 제한
계정관리	U-106	상	암호화된(C2 Level) 패스워드 사용
계정관리	U-108	중	패스워드 복잡도 설정
시스템보안설정	U-201	상	root 계정의 원격 접속 제한
시스템보안설정	U-204	중	SU 명령어 실행 제한
서비스관리	U-302	상	inetd.conf DoS 데몬 비활성화
서비스관리	U-303	상	inetd.conf tftp, talk 데몬 비활성화
서비스관리	U-305	중	inetd.conf r서비스 관련 데몬 비활성화
서비스관리	U-310	상	취약한 SNMP Community Name 설정 제한
보안패치관리	U-401	상	시스템 Update
시스템보안설정	U-206	중	Session Timeout 설정
시스템보안설정	U-208	중	불필요한 world writable 파일 제거
서비스관리	U-313	중	automountd 서비스 비활성화
시스템보안설정	U-211	중	스팸 메일 릴레이 제한
시스템보안설정	U-215	중	at 파일 소유자 및 권한 설정
서비스관리	U-301	상	경고 메시지 설정
파일 및 디렉터리 관리	U-506	상	SUID,SGID,Stick bit 설정 파일 점검
시스템보안설정	U-216	상	접속 IP 및 포트 제한
시스템보안설정	U-219	상	일반사용자의 Sendmail 실행 방지
서비스관리	U-314	상	ftp 서비스 확인
시스템보안설정	U-221	상	Bash Shellshock (CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187)

▶ 세부 진단 내용

뷰어사용

코드	U-101	위험도	중	분류	계정관리
항목	root 권한의 UID/GID 중복 제거				
진단결과	양호				
기준	* "/etc/passwd"파일을 확인하여 세 번째 필드 UID가 "0"이 할당되어 있는지 확인한다. root계정 이외에 다른 계정의 uid가 "0"으로 설정되어 있다면 취약하다.				



jun-PC(192.168.0.75) 보안수준 : 76.4

▶ 서버정보

구분	내용
호스트명	jun-PC
ip	192.168.0.75
진단대상	mssql(WINDOWS)
운영부서	개별
진단일시	2015년 03월 17일 08시52분

▶ 취약점 발견 현황

진단항목수	21	취약항목수	5

분류	점수	위험도	개수
계정관리	71.4	상	1
권한관리	100	중	4
보안패치관리	0	하	0
시스템보안설정	84.4		

▶ 취약점 목록

분류	코드	위험도	항목
계정관리	MSS-106	중	패스워드 주기적 변경
계정관리	MSS-108	상	패스워드 복잡도 설정
시스템보안설정	MSS-303	중	Registry extended stored procedure 사용 제한
보안패치관리	MSS-401	중	최신 서비스팩 및 HOT FIX 적용
계정관리	MSS-109	중	일정 횟수의 로그인 실패 시 이에 대한 잠금정책이 설정되어 있는가?

▶ 세부 진단 내용

코드	MSS-108	위험도	상	분류	계정관리
항목	패스워드 복잡도 설정				
진단결과	미흡				
기준	* 해당 항목을 MSSQL 2005 버전에 해당되는 것으로서 "시작 > 제어판 > 관리도구 > 로컬 보안 정책 > 로컬 사용자 및 그룹 > 계정 정책 > 암호정책" 폴더에서 "암호는 복잡성을 만족해야 함" 항목이 "사용 안함"으로 설정되어 있다면 취약하다.				
현황	[취약점현황] 추천점1. (JUN-PC\SQLEXPRESS) test 패스워드 복잡도 설정 옵션을 사용하지 않음 추천점2. (JUN-PC\SQLEXPRESS) test 암호 정책 강제 적용 옵션을 사용하지 않음 추천점3. (JUN-PC\SQLEXPRESS) ss 패스워드 복잡도 설정 옵션을 사용하지 않음 [시스템현황] (JUN-PC\SQLEXPRESS)의 취약 계정 현황 NAME | SYSAdmin | 생성일자 | 잠김 | 만료정책 | 암호정책 | ACCESS | NT유저 | NT그룹 | Security | Server | Setup | Process | Disk | DbCreat | Bulk ss | 0 | 2003-04-08 09:10 | 0 | X | 0 | 0 | X | X | X | X | X | X | X | X test | X | 2014-02-12 15:14 | X | X | 0 | 0 | X | X | X | X | X | X | X | X [서주설정현황] 진단 여부 계정 목록(사용자 정의) : 없음				
조치방법	* "시작 > 제어판 > 관리도구 > 로컬 보안 정책 > 로컬 사용자 및 그룹 > 계정 정책 > 암호정책" 폴더에서 "암호는 복잡성을 만족해야 함" 항목을 "사용"으로 설정한다.				

코드	MSS-109	위험도	중	분류	계정관리
항목	일정 횟수의 로그인 실패 시 이에 대한 잠금정책이 설정되어 있는가?				
진단결과	미흡				

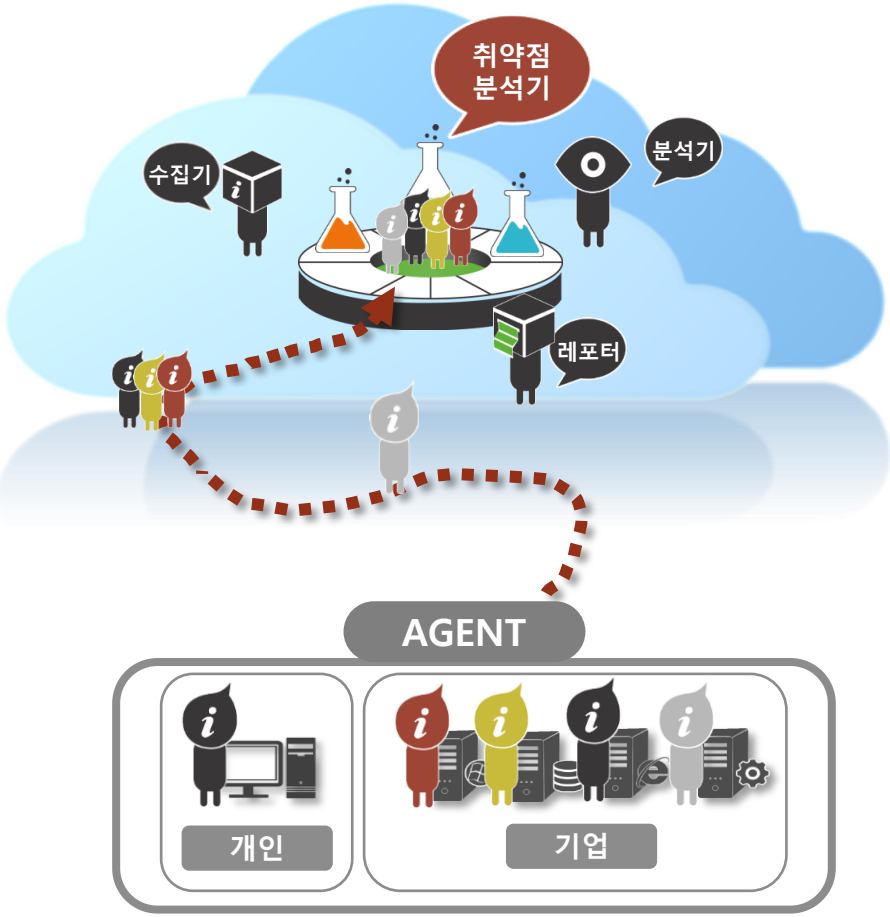
3.2. 인프라 취약점 진단 자동화 솔루션 – SolidStep (특장점)

SSR 고유의 정보보호 컨설팅 Knowhow를 반영하여 개발된 SolidStep의 핵심 역량으로
지속적으로 수행되는 보안수준 관리에 있어 타사 대비 높은 경쟁력을 확보할 수 있습니다.

100% 조치 가능한 결과	고객사 내부 보안지침과 100% 일치하는 진단을 수행하여 보안팀 및 운영팀 모두 수용 가능한 진단 결과 도출
보안컨설팅 노하우 적용	200건 이상의 보안컨설팅 경험의 전문컨설턴트에 의해 수행하는 인프라 보안진단 이상의 고도화 진단 수행
독보적인 진단 구조	진단 대상 시스템의 안정성을 최대로 확보하는 '수집-분석' 분리 구조 * SSR만이 가지고 있는 유일한 구조이며 특허 진행 중
다양한 운영 환경 지원	Agent, Agentless, Offline 방식 등 고객사 환경 및 문화에 맞는 다양한 운용 방식 제공, 동종 제품 대비 가장 많은 플랫폼 지원 (PC, Server, DBMS, WEB/WAS, Network)

3.3. 인프라 취약점 진단 클라우드 서비스 – SolidStep Cloud

SolidStep Cloud는 저렴한 비용으로 소상공인과 스타트업, 중소기업 등 작은 규모의 IT 인프라를 보호하는 최상의 서비스를 제공합니다.



인프라 취약점 점검 영역

SolidStep Cloud Service

플랫폼 별 라이센스 구매
(커스터마이징)

최적화 서비스 대상 Cloud

소상공인 | Start-UP | 중소기업

3.3. 인프라 취약점 진단 클라우드 서비스 – SolidStep Cloud

플랫폼별 라이센스 구매 방식을 도입하여 사업의 핵심요소를 안전하게 보호할 수 있도록 인프라 취약점 진단관리의 방향성을 제시합니다.

▶ 서비스 혜택

고급 취약점 진단 서비스
대기업, 금융기관에서 사용하는 핵심 취약점 진단을 동일하게 수행

+

합리적인 가격
1/10 수준의 저렴한 가격으로 Cloud 기반 취약점 진단 Service를 제공

+

컴플라이언스 100% 대응
개보법, 신보법, 정통망법 등 국내 주요 법규 항목을 100% 완벽 대응

+

고객맞춤 라이센스 구매
고객의 IT 인프라 환경에 맞게 라이센스 구매 가능

▶ 최적화 고객

3.3. 인프라 취약점 진단 클라우드 서비스 – SolidStep Cloud

SaaS형태(Software as a Service)의 인프라 취약점 진단 클라우드 서비스로서 제공 가능한 가장 넓은 진단 범위를 자랑합니다.

타입	플랫폼	지원 버전
OS	Windows	* PC계열 - Vista/7/8/10, 서버계열 - 2003/2003 R2/2008/2008 R2/2010/2012
	Linux	* glibc2.4 ~ 4.5, Redhat 계열, Debian 계열
	IBM - AIX	* 5.1 ~ 7.2
	HP - UX	* PA-RISC 11.00 이상, itanium11.23 이상
	Oracle Solaris	* SPARC 5.7 ~ 5.9, x86 10 ~ 11
DBMS	Oracle	* Oracle database 8/9/10/11/12 (12C 제외)
	MSSQL	* Microsoft SQL server 2000 ~ 2014
	MySQL	* MySQL 5.0 ~ 5.6
	IBM - DB2	* DB2 9/10
	Sysbase	* Sysbase Database ASE 15.7 ~ 16.0
	Tmax - Tibero	* Tibero 5 ~ 6
	Altibase	* Altibase Database 6 ~ 6.5
	Postgre SQL	* PostgreSQL 9.1 ~ 9.6 (PPAS 지원)
	MariaDB	* MariaDB 5.1 ~ 5.5, 10.0 ~ 10.2
WEB	Apache	* Apache 1 ~ 2
	IIS	* IIS 6 ~ 8
	Tmax WebToB	* Tmax WebToB 4.1
	Oracle Http Server	* 11g, 12g
	Iplanet	* Iplanet 6.1
WAS	Apache Tomcat	* Apache Tomcat 5 ~ 9
	Oracle Weblogic Server	* Oracle Weblogic Server 10 ~ 11
	Tmax JEUS	* Tmax JEUS 5 ~7
	IBM WebSphere	* IBM WebSphere 8
	Nginx	* Nginx 1.4 ~ 1.10
	Jboss	* Jboss 5 ~ 7
	Resin	* Resin 2 ~ 3
NETWORK	Cisco	* IOS XE, XR 가능
	Juniper	* Junos OS 12.1X45 ~ Junos OS 16.1
	HP(3COM)	* 3Com H3C - 지원 모델명 4500, 5500, 4200G, 4500G, 4800G, 5500G, 7750, 7900E, 8800
	Alteon	* Alteon OS - version 23.2.2, version 24.0.7
	Alcatel	* Alcatel AOS - 지원 모델명 6400, 6850, 6850E, 6855,. 9000E
	Extreme	* ExtremeXOS

3.4. 사회공학적 해킹 (악성메일) 대응 훈련 솔루션 – MudFix

MudFix는 이메일을 통해 반복적으로 보안인식을 제고시켜, 사회공학적 해킹을 대비하고 조직의 보안수준을 측정 및 관리하는 솔루션 입니다.

보안 인식 제고 반복훈련 MudFix 로 대비!

3.4. 사회공학적 해킹 (악성메일) 대응 훈련 솔루션 – MudFix

다양한 훈련양식을 제공하며 유출파일의 시각화를 통해 보안인식을 제고시키고, 행위분석 기반 각 단계별 보안수준을 측정하여 해킹에 대응하고 있습니다.

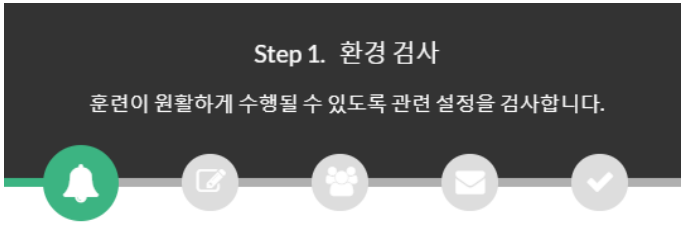
기능

대상관리

대상자 등록,
정보 확인,
태그 설정

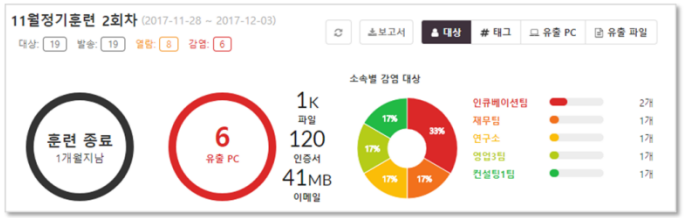
훈련실시

훈련의 접근성
극대화 및
필수요소 최소화

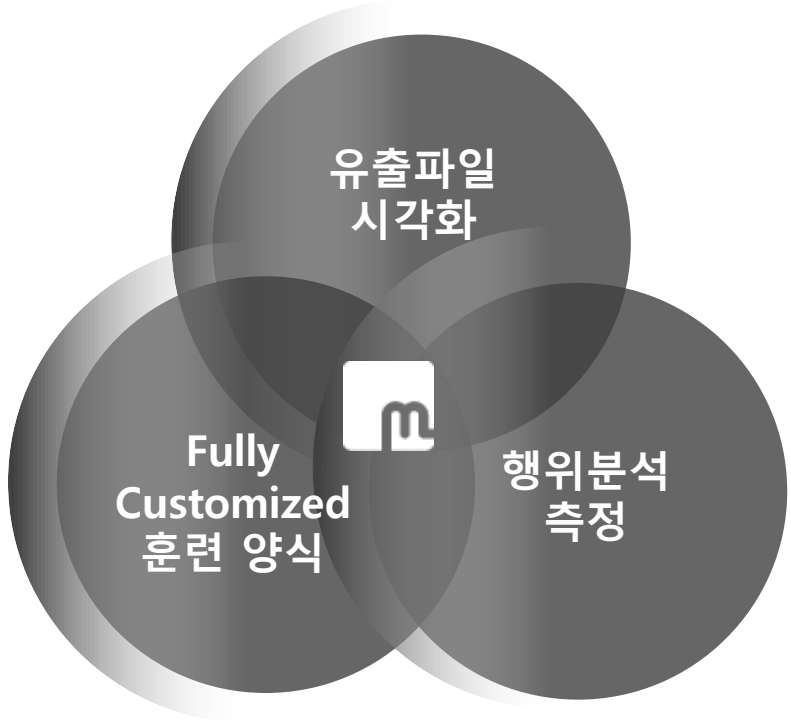


결과확인

개별/전체
진행상황,
훈련정보,
훈련결과



특장점



3.4. 사회공학적 해킹 (악성메일) 대응 훈련 솔루션 – MudFix

SaaS방식(Software as a Service) 또는 구축형 방식을 도입한 솔루션으로 반복적인 훈련으로 해킹 및 악성코드, 랜섬 웨어 감염 등을 예방합니다.

1. 감염 대상의 데이터 추출
2. 최신 트렌드를 반영한 훈련 양식
3. 보안수준의 상향평준화
4. 합리적인 가격
5. 고객맞춤형 서비스

3.5. 국내외 솔루션 구축 사례 - SolidStep

SolidStep은 금융권 및 IT비즈니스를 수행하는 기관 및 기업 등 다양한 환경에 구축되었고, 단일 사업 최대규모의 설치, 운영 레퍼런스를 보유하고 있습니다.

공공기관	문화체육관광부, 교육부, 국군사이버사령부, 국군기무사령부, 국가보훈처, 국방과학연구소, 한국공항공사, 한국동서발전, 중부발전, LH한국토지주택공사, 한국석유공사, 국민연금공단, 서울시농수산식품공사, 한국예탁결제원, 한국교육개발원, 한국재정정보원 세종특별자치시, 서울시교육연구정보원, 국방기술품질원, 국가평생교육진흥원, 한국원자력환경공단, 한국원자력안전기술원, 한국원자력안전위원회, 한국항공우주연구원, 청주공항, 울산과학기술원, 한국신용정보원, 전라남도청, 경상북도개발공사, 서귀포시, 부산항만공사, 연천군, 식품의약품안전처,외 20여곳
대기업 / 일반기업	현대기아차 , SK Telecom, KT, LG U+,한화 S&C, LG생활건강, 현대오토에버, 삼성전자로지텍, 하나 IDT, 코오롱베니트, LG화학, 코웨이, CJ오쇼핑 W쇼핑, 현대모비스, SK브로드밴드, 이수그룹, 롯데백화점, 나이스정보통신, 현대자동차 미주법인&유럽법인, 안랩, KTDS 현대위아, 골프존, SK네트웍스, 아시아나항공,코리아케이블텔레콤, 굿네이버스
금융권	금융감독원, 한국증권금융, IBK기업은행, KB국민은행, 우리은행, 하나금융그룹, 한화투자증권, 키움증권, 동부증권 경남은행, KB손해보험, KB생명보험, 한화손해보험, 한국신용정보원, 신협, NH농협생명 DGB생명보험, 보험개발원, 서울외국환중계, ING생명보험, 우리카드, 메리츠화재, 신한생명, 교보생명보험, BC카드, KG이니시스, NH농협손해보험, KB손해사정, 롯데카드, 흥국생명, 웰컴저축은행, KG모빌리언스, 스마트로, 브이피, 에이앤디신용정보
교육기관 / 병원	울산과학기술대학교, 부산카톨릭대학교, 한국해양대학교, 진주경상대학교, 서울과학기술대학교, 전국교육대학교 제주국제학교 ,강원대학교, 두원공과대학교, 대구보건대학교, 울산대학교, 신라대학교

납품계약 **60,000대** 이상 설치, **500,000회** 이상 진단 수행. (컨설팅 포함 진단 횟수: **수 십만 회 수행**)

3.5. 국내외 솔루션 구축 사례 - MetiEye

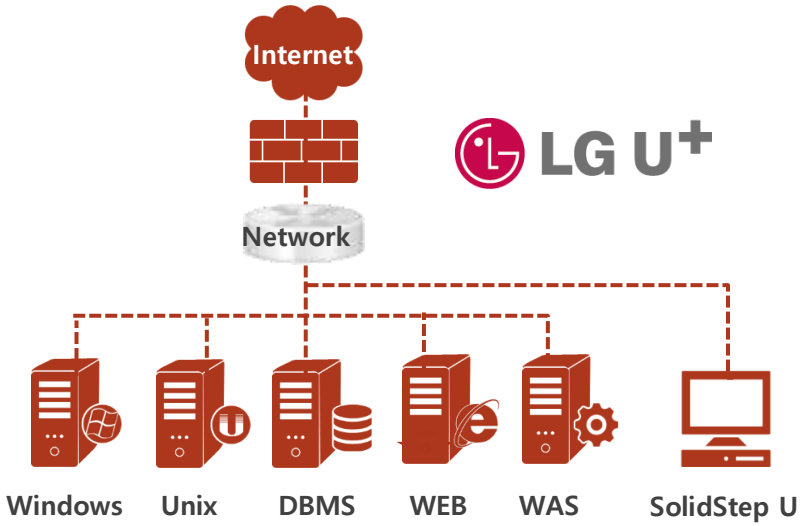
MetiEye는 금융권 및 IT비즈니스를 수행하는 기관 및 기업 등 다양한 환경에 구축되었고, 단일 사업 최대규모 수준의 설치, 운영 레퍼런스를 보유하고 있습니다.

공공기관	국토교통부, 식품의약품안전처, 국민체육진흥공단, 경기도청, 부산항만공사, 부산광역시청, 대구광역시청, 중소기업중앙회 국립대구과학관,, 한국기계거래소, 송파구청, 한국소비자원, 서울산업통상진흥원, 한국지식재산전략원, 노사발전재단, 구리시청,, 한국여성정책연구원, 한국교육개발원, 중소기업중앙회, 소방안전협회
금융권	금융감독원, 예금보험공사, KB투자증권, SK증권, 한화손해보험, ING생명, 스마트저축은행, KB생명보험, KB손해사정, 스마트로, 에이앤디신용정보, KB손해사정, 새마을금고중앙회, 한국신용정보원, 나이스디앤비
기업	LG U+, 현대중공업, 한솔그룹, 하나금융티아이, 두산, LG생활건강 대림산업, 아시아나항공, 코웨이, 무브게임즈, 안랩, 에스원 L&K Logic Korea, 모두투어, 여행박사, 옐로우캡, 리서치애드, 까페베네, 토니모리, 엔플린트,, 이너스커뮤니티, 코리아타임즈, 데일리팜, 화승, 헤럴드, 한국아이닷컴, 대하인터내셔널, 에셋플러스, 보배드림, 시큐어아이디씨, 패널인사이트, 시슬리코리아, 누리미디어, 한국섬유신문사, 한국프로골프투어, 고려아연, 천손문화원, 에스박스, 야놀자, 브랜드스토리, 에넥스, 디자인메이, 베어크리크, 인터플렉스, 보령제약, 아프리카TV, 동일고무벨트, 페이레터, 한국다이찌산쿄, 레드캡투어, 공영홈쇼핑, 이지웰페어, 원스토어, 케이토토, 유비케어,, 가비아, 두산정보통신, 파이오링크,, KT스카이라이프, 나이스디앤비, 삼화페인트
교육기관	경남정보대학교, 정철어학원, 신라대학교, 중앙대학교의료원, 울산과학기술대학교 부산카톨릭대학교, 교육지대, 재능교육, 영산대학교, 울산대학교병원, 경남과학기술대학

5,000 License 판매

3.6. 주요 적용사례 – LG U+ : SolidStep, MetiEye

3사 합병에 따른 LG U+의 다양한 시스템 환경에 대한 안정성 높은 진단요구에 맞춰 10년 이상 운영된 구형 시스템의 보안을 SolidStep 및 MetiEye로 강화하여 관리하고 있습니다.



1 3사 통합에 따른 다양한 종류의 시스템 진단 필요

- ✓Windows, AIX, Solaris, HPUX, Linux 5종 진단
- ✓아키텍처에 따른 12종류의 진단 모듈 실행

2 최고의 안정성 확보된 진단 필요

- ✓서버 운영자 직접 실행 방식 선택
- ✓10년 이상 운영된 legacy 시스템의 안정적 진단

3 격리 네트워크에 위치한 시스템 진단 필요

- ✓OFFLINE 수집 결과의 관리서버 자동화 처리

기대효과

보안컨설팅 수준의 인프라 전수검사
- 비용 및 리소스 절감

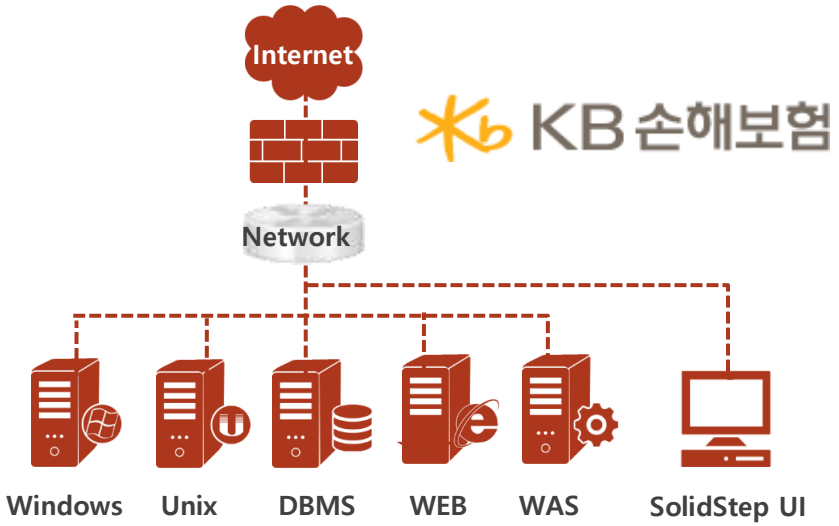
보안지침 준수 여부의 감사 및 보안수준 수치화
- 지속적 이행 점검으로 인한 보안 수준 상향 평준화

2012.04	2012.05	2012.06	2012.11
프로젝트시작 투입인원:1명 ✓진단방법 협의 ✓점검가이드	전수검사 투입인원:1명 ✓12개 종류 서버 6,000여대 전수검사	이행점검 투입인원:1명 ✓서버 6,000여대 이행 점검	후속대응 투입인원:1명 ✓보안가이드 개선 및 상시 점검

12개 종류 6,000대 시스템에 대해
200개의 보안항목들을 300명의 속도로 점검

3.6. 주요 적용 사례 – KB 손해보험 : SolidStep

금융위원회 전자금융감독규정의 컴플라이언스를 준수하는 항목구성으로 기존 샘플링 기반의 컨설팅 외주업무를 자동화된 솔루션으로 전수검사하여 관리하고 있습니다.



KB 손해보험

기대효과

인프라 전체에 대한 단기간 전수검사
- 비용 및 리소스 절감

금융위원회 전자금융감독규정 준수
- 기존 인력투입 컨설팅을 대체하여 컴플라이언스 대응

1 인프라 전체에 대한 단기간의 진단 필요

✓SolidStep 이용하여 1,600대 이상 진단 수행

2 관련 법규 및 전자금융감독규정 준수

✓SolidStep을 통해 기존 컨설팅 대체
✓향후 지속적인 항목 업데이트 지원

3 연간 스케줄 및 이벤트 발생 시 수시 점검

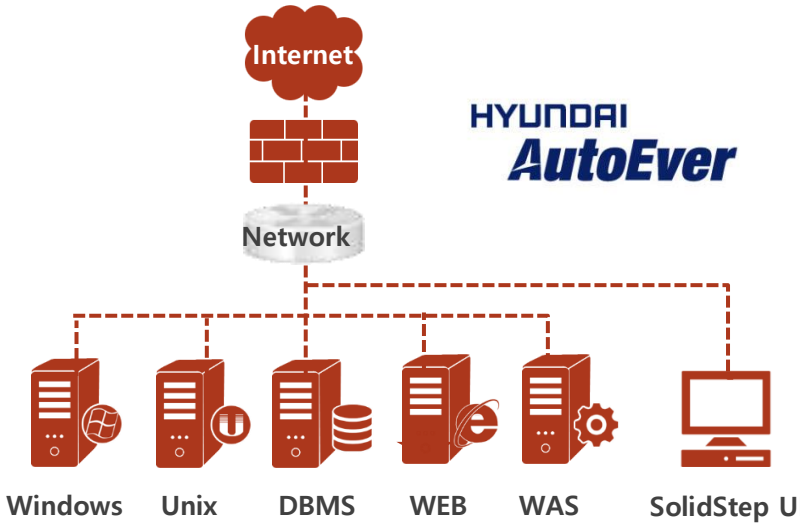
✓신규, 변경되는 시스템에 대한 즉각적인 보안 점검
✓ 지속적으로 상향되는 보안 수준의 객관적 평가 수행

2014.02	2014.03	2014.04
프로젝트시작 투입인원 : 1명 ✓ 진단방법협의 ✓ 점검가이드 개발	시범운영 투입인원 : 1명 ✓ 2013년 이행점검	정기검사 투입인원 : 1명 ✓ 1,600대 대상 전수검사 ✓ 정기 컨설팅 사업 수행

1,600대 시스템에 대해 144개의 보안항목들을 300명의 속도로 점검

3.6. 주요 적용 사례 – 현대오토에버 미주법인 : SolidStep

정부기관이 제공하는 정보로만 취약점 진단을 자체적으로 수동 점검했지만, 북미 시장분석을 통해 맞춤형 신규 취약점 항목을 개발하여 상시 점검이 가능하도록 구축했습니다.



HYUNDAI AutoEver

1 해외법인 여건 상 단기간의 구축, 진단 필요

- ✓ SolidStep 이용하여 한 달여 만에 1,300대 이상 구축, 진단 수행

2 미국 법규 분석에 기반한 진단항목 개발

- ✓ 미국 개인정보보호법, 연방정보보안관리법 등을 충족하는 항목 개발
- ✓ 국내 컴플라이언스 준수사항 및 미국 법규 모두 대응 가능

3 연간 스케줄 및 이벤트 발생 시 수시 점검

- ✓ 신규, 변경되는 시스템에 대한 즉각적인 보안 점검
- ✓ 명확한 취약점 진단관리에 대한 가이드가 없는 미국의 여건 상 향후 지속적인 취약점 항목 개발 협의

2016.10	2016.11	2016.12
프로젝트시작 투입인원 : 2명 ✓ 진단방법협의 ✓ 점검가이드 개발	시범운영 투입인원 : 2명 ✓ 2016년 이행점검	정기검사 투입인원 : 2명 ✓ 1,300대 대상 전수검사 ✓ 운영메뉴얼 개선 및 상시 점검

기대효과

인프라 전체에 대한 단기간 전수검사
- 비용 및 리소스 절감

미국 법규분석에 기반한 진단관리
- 미국 개인정보보호법, 연방정보보안관리법 등 준수

1,300대 시스템에 대해
미국법규 기준 항목들을 신규 개발, 300명의 속도로 점검

Contact Us

Brain Beyond Brands

SSR Security Strategy Research

Tel. 02-6959-0129 Fax. 02-6959-0130

Homepage. www.ssrinc.co.kr

E-mail. biz@ssrinc.co.kr

서울시 구로구 디지털로 26길 111 JnK디지털타워 1606호