RAPID7

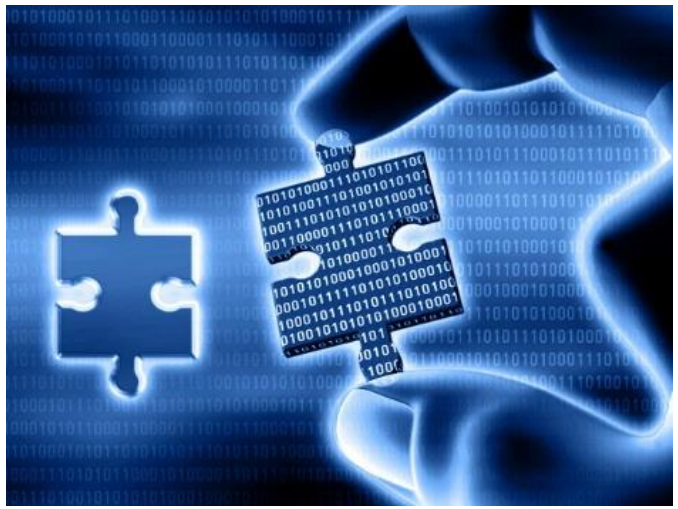
NEXPOSE - METASPLOIT Enterprise

보안취약점 분석 및 관리 (NEXPOSE)
모의해킹 테스트 솔루션 (METASPLOIT)

INSEC security

솔루션 소개에 앞서.....

취약점이란 무엇인가에 대한 정의 부터.....



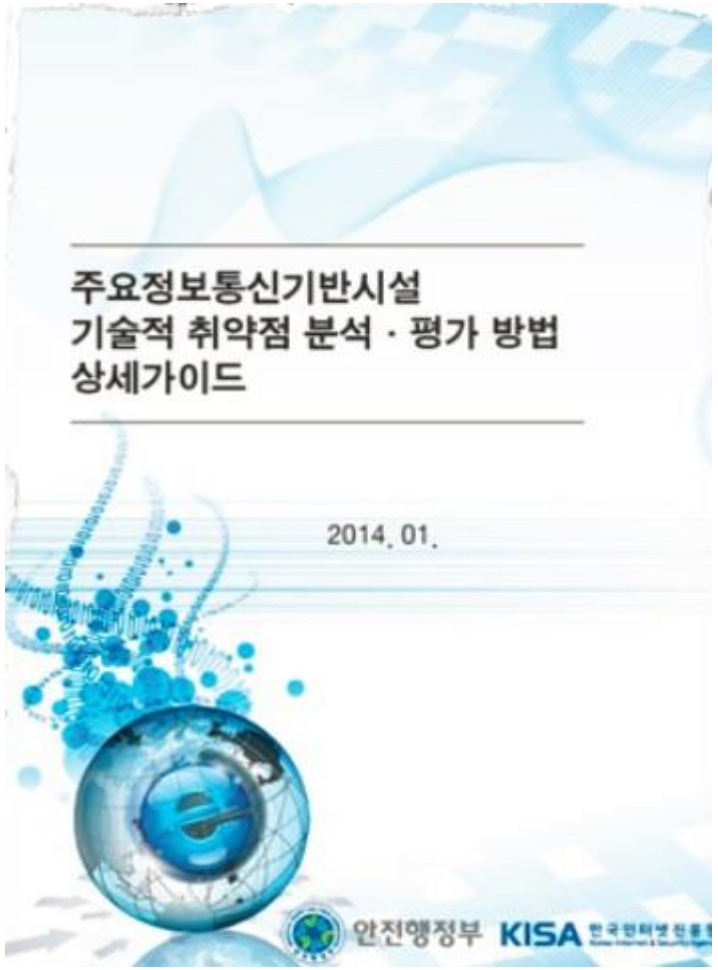
취약점이란...

취약점 Vulnerability	취약점을 악용하면..
사전적 의미로 H/W, S/W의 결함이나, 설계상의 헛점 	불법적인 사용자의접근을 허용 고객의 정상적인 서비스를 방해 중요데이터의 유출 및 변조, 삭제  

기존 고객의 대응방안

연간위험관리 활동 (정보보호컨설팅)
현 조직의 상황을 파악하기 위한 기술적 분석중 하나

정보통신기반보호법

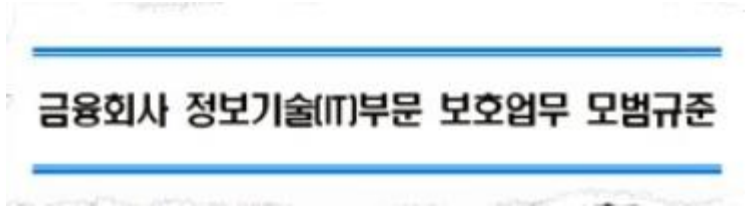


정보통신기반 보호법 제 9조

주요정보통신 기반보호시설 관리기관은 매년 취약점 분석/평가를 실시하여야 함

총 **313**개의 기술적 점검항목에 대해 취약여부를 점검

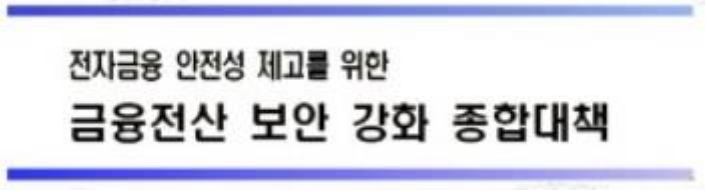
전자금융거래법 + 금융위원회 Compliance



2012.10

전자금융기반시설에 대해 매년 정기평가 실시

금융회사의 취약점 분석, 평가 결과 및 이행실태를 점검



2013.07

CEO 책임하에 취약점 점검 및 보완조치 이행 철저 시스템
계정 사용권한, 접근기록 등 중점 관리 및 통제

금융 전산시스템까지 취약점 점검 확대
정보보안 조직은 임직원의 IT 보안법규 준수 여부를
정기적으로 점검하고, **결과를 CISO 및 CEO에 보고**

각종 인증체계(ISMS, ISO27001,PIMS)

ISMS
(정보보호인증체계)

공개서버의 취약점 점검을 주기적으로 수행하고, 발견된 취약점을 조치

ISO27001
(정보보안관리시스템 인증체계)

정보시스템 취약점 점검절차를 수립하여, 장기적으로 정검을 수행

PIMS
(개인정보보호인증체계)

취약성 진단도구등을 이용하여 서버의 취약성 및.. 수시로 점검

개인정보처리시스템이 절차에 따라 운영되는지 점검을 정기적으로..

취약점 진단의 현황

얼마나 자주	1-2회 / 1년	자산의 신규 도입, 서비스의 변경
점검 대상	샘플링	진단 시스템 중복, 동일한 구성인지?
방법은?	스크립트	취약점 진단 결과 암호화, 관리자계정
비용은?	Man/Month	이제는 전수진단을 해야…

1. 시간과 비용의 리소스의 한계 → 취약점 샘플링 진단
2. 변동되지 않는 자산의 중요도 → 진단 샘플 자산도 매번 동일

미진단 인프라자산 → 취약점 관리 부재 → 위험 상존으로 해커의 우회도구로 악용 가능

이젠 바뀌어야 합니다...

취약점 진단 자동화

시간, 비용 리소스 절감

인프라 전수진단 : 잔여 취약점 제거

정책 및 지침의 이행 보장 : 법규 및 컴플라이언스 완벽 대응

래피드7은 어떤 기업인가?

- 2000년 미국 보스톤에 설립
  - 복잡한 보안 과제를 위한 단순하고 혁신적인 솔루션 개발
- 세계적 입지
  - 78개 국가의 3천 개 이상의 기관이 신뢰하는 기업

    (포춘 1000대 기업 25% 이상이 포함됨)
- 세계 최고의 IT 보안데이터 및 분석솔루션
  - 18분기 연속 사상 최대 수익 기록 (계속 증가 중)
- 고객에 초점을 둔 기업
  - 일류 기술 판매업체와 필적할 만한 순 추천고객지수(NPS)

왜 래피드7인가?

세계 최고 수준의 취약성 평가 역량

SC MAGAZINE AWARDS 2014 WINNER Honored in the U.S.

취약성 관리 솔루션 최우수상 수상

Gartner

<2013년 시장전망>에서 최고 등급인 'Strong Positive(매우 긍정적)' 등급을 받음

보안연구 분야에 대한 통찰의 리더십

RAPID7 LABS

메타스플로잇의 연구책임자이자 창설자 HD Moore가 지휘

200,000

오픈소스 보안커뮤니티에 대한 활발한 기여

오늘날의 위협 환경 이해

metasploit®

세계에서 가장 많이 사용되는 침투테스트 소프트웨어

userinsight

속임을 이용한 공격을 파악하는데 가장 효과적인 솔루션

의미있는 고객 파트너십

200+

올해, 200개 이상 고객업체가 12 참여프로그램에 참여함

96%+

지원 사례들은 일선 담당자를 통해 해결되었으며 고객 97%가 이에 만족함

78개 이상 국가에 3천 개 이상 고객업체 보유

기술/통신

vmware
IBM
Telefónica
symantec
Booking.com
kt
LG CNS
CISCO

도소매

adidas
REVLON
kmart
NIKE
COACH
Yum!
BEST BUY
SKECHERS

에너지

Anadarko Petroleum Corporation
ExxonMobil
FirstEnergy
WorldFuel Services

교육

Carnegie Mellon
Columbia University
The Hong Kong Polytechnic University 香港理工大學
University of Technology Sydney

금융서비스

MoneyGram International
CapitalOne
Sumitomo
ING

미디어 엔터테인먼트

NETFLIX
facebook.
sky
zynga

보건

UnitedHealth Group
NOVARTIS
DaVita.
醫院管理局 HOSPITAL AUTHORITY

공공부문 정부기관

Ministry of Defence
Homeland Security
Ministry of Foreign Affairs Singapore

제조

BOEING
Kellogg's
Westinghouse
BOSCH

기타

Hertz
Etihad Airways
Tatts Group
Merlin Entertainments Group

국내 고객

- 기업 : 현대자동차, 현대모비스, 현대다이모스, SK 플래닛, 다음커뮤니케이션즈, 한진그룹, 한화그룹, LG CNS, SPC Network, Smartro,
- 금융 : KOSCOM, 금융결재원, 금융감독원,IBK 기업은행, 현대증권, 하나 SK 카드
- 공공 : 관세청, 국정원, 방위산업청, 육군, 공군
- 기타 : ETRI, KT, KT DS, 이글루시큐리티, 안랩
- 교육 : 명지대학교

래피드7 제품 포트폴리오

보안 관리

nexpose®

controlsinsight

- 취약점, 컨피규레이션, 컨트롤에 대한 통합 리스크 관리
- 컴플라이언스 관리 간소화

사용자 리스크 관리

userinsight

mobilisafe

- 온프레미스(on-premise), 클라우드, 모바일 환경에 대한 사용자 행동 모니터링
- 빠른 사건 파악과 조사

침투 테스트

metasploit®

- 취약점 파악과 방어 확인을 위한 네트워크 공격 시뮬레이션
- 피싱 노출 관리 및 테스트 사용자 인식

래피드7의 목적

상황적이고 실용적인 통찰력, 훌륭한 사용 경험

고객이 최소한의 노력을 들여

오늘날의 복잡한 보안 환경을

관리할 수 있도록

데이터, 분석, 통찰력을 제시한다.

현대 기업 및 속임 기반의 공격

많은 양의 보안데이터를 수집하고 분석함

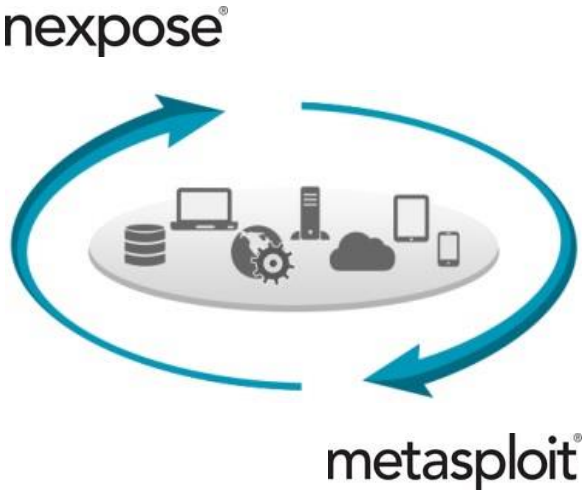
nexpose®

RAPID7

포괄적 가시성

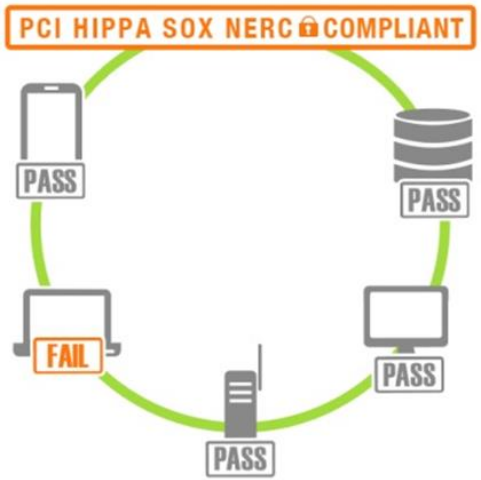
- 조직내 IT인프라 전체에 대한 자산과 애플리케이션 검출
- 취약점, 규정 통합 평가

위협, 리스크 안내



- 메타스플로잇으로 폐쇄 루프형 취약점 검증
- RealRisk™과 RealContext를 통한 인텔리전트 평가

간소화된 컴플라이언스



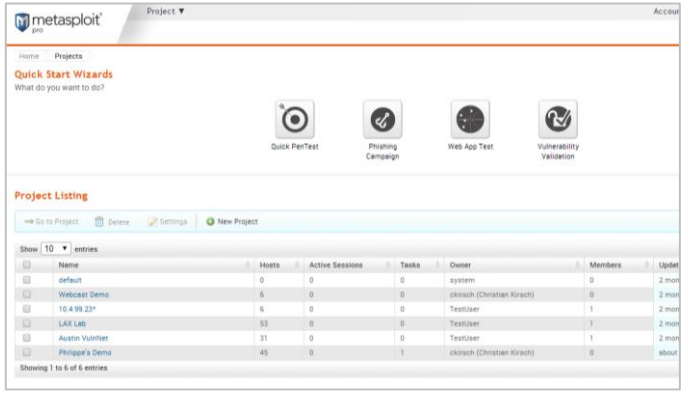
- PCI DSS, FISMA, HIPPA, SOX, GLBA, NERC CIP, CIS
- 맞춤형 컴플라이언스 벤치마크와 보고

INSEC security

metasploit®

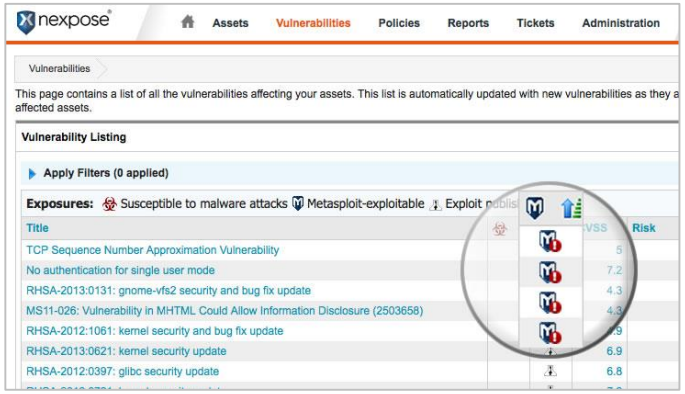
RAPID7

침투 테스트



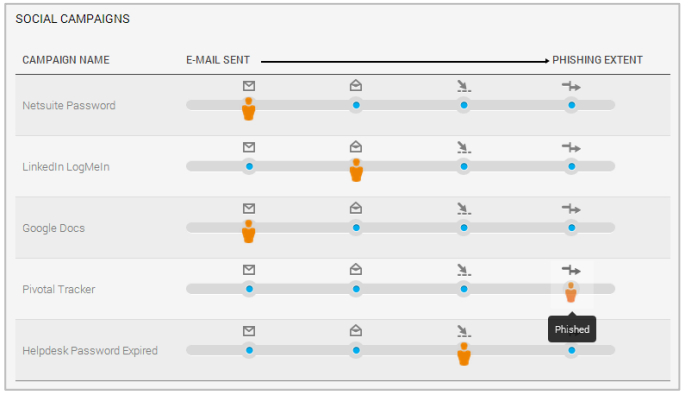
- 기업 네트워크로의 안전한 공격 시뮬레이션
- 고급 회피기술 및 취약 자격 증명 테스트

취약점 검증



- 고객 환경에서의 실제 리스크 확인 및 입증
- 치료를 위해 넥스포즈와 폐쇄형 루프 통합

피싱 시뮬레이션



- 사용자의 보안 인식 및 교육 정도 측정
- 피싱 공격에 대한 기술 통제 테스트

INSEC security

취약점 검증 (상호연동)

1. 익스플로잇 가능성 있는 취약점 파악

2. 넥스포즈로부터 스캔 결과 자동 전송

nexpose® enterprise

metasploit® pro

5. 치료를 위해 검증된 취약점 우선순위 분석

3. 익스플로잇 가능성 증명을 위해 간이 마법사 사용

4. 넥스포즈로 결과 자동 재전송

EXPLOIT : 공격용 코드 (즉 악의적인 목적을 위해 만든 소스코드)

효과적인 우선순위 분석

- 래피드7 RealRisk™ 스코어
  - 익스플로잇성, 연식, 멜웨어 키트의 가용성에 대한 CVSS를 기준으로 함
- 래피드7 RealContext 태그
  - 비즈니스 상황에 따른 리스크 평가와 치료 정렬 개선
- 최고의 치료 보고
  - IT팀에 기관의 리스크 감소 방법 명확히 제시

Top 10 Remediations by Risk

April 19, 2013 09:14:21 PDT

Executive Remediation Report - New York

Applying	Will Remediate	Affecting
10 Top Remediations	35% Vulnerabilities including: 11% published exploits, 34% available malware kits	57 Assets

Remediations	Remediated Vulns			Affected Assets	Risk
Upgrade to latest version of Adobe Flash Player	3339	180	132	19	1912199
Upgrade to the latest version of Apple iTunes	2329	25	6	6	986587
Upgrade to the latest version of Mozilla Firefox	1784	64	8	10	848020
Upgrade to the latest version of Apple Java	764	50	36	7	418958
Upgrade to the lastest version of the Java Runtime Environment	746	57	199	15	387860
Upgrade ESX to the latest version	975	63	11	7	358931
Upgrade to the latest version of Adobe AIR runtime	540	18	10	5	323282
Download and install Microsoft patch windowsserver2003-kb2792100-x86-enu.exe (4278824 bytes)	382	231	52	11	221713
Upgrade to the latest version of PHP	488	58	0	4	214124
Upgrade to the latest version of Mozilla Firefox ESR	405	0	0	4	181849

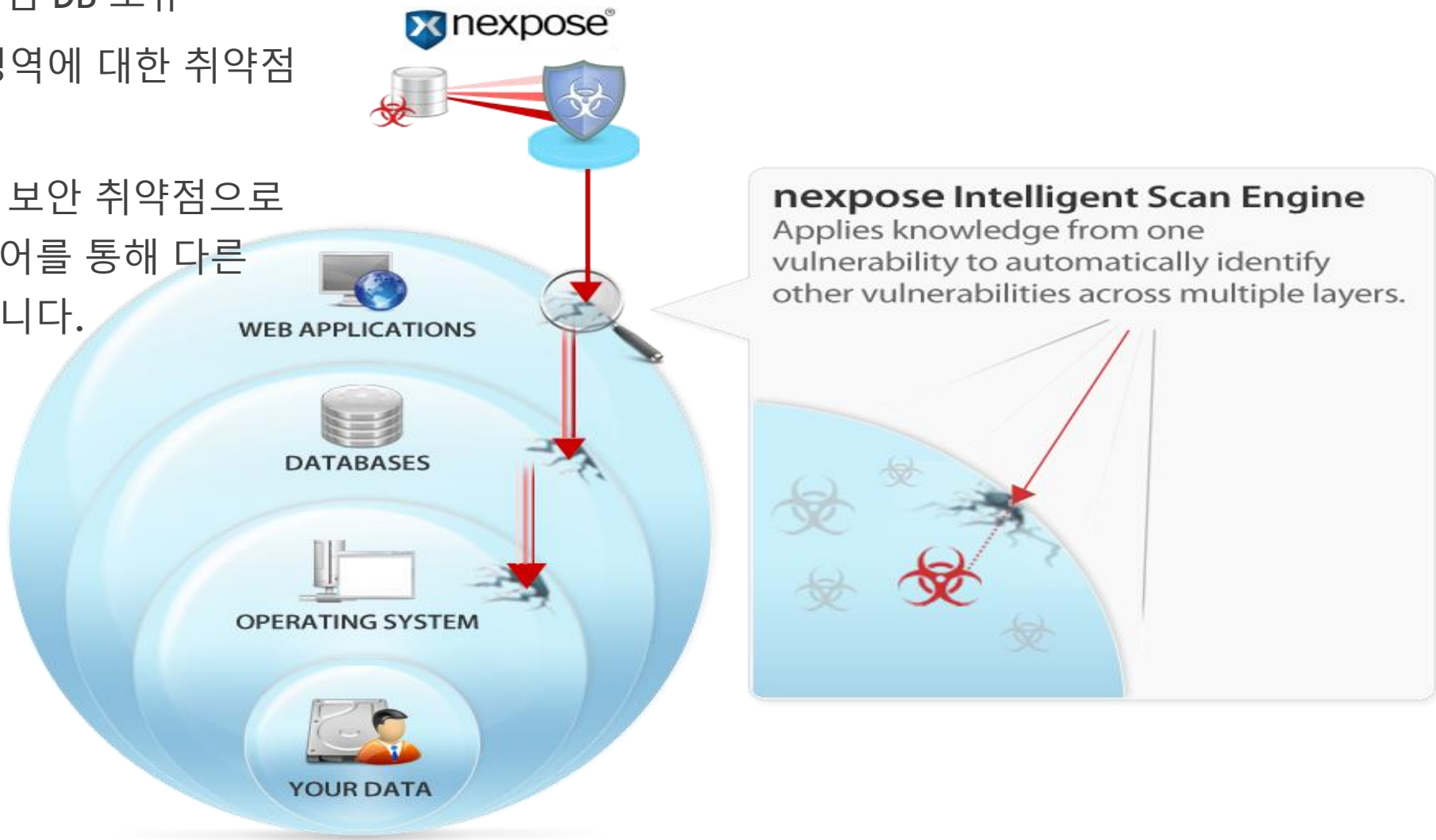
CVSS: 보안위협 판정을 위한 기준(해외에서는 취약점을 DB로 관리하고, 해당취약점에 대한 점수를 매김)


nexpose®


INSEC
security

취약점 분석 방법

- 전체 IT영역에 대한 취약점 DB 보유
- 단일 플랫폼에서 모든 영역에 대한 취약점 분석
- NEXPOSE 지능형 엔진은 보안 취약점으로부터 자동으로 다중레이어를 통해 다른 취약점을 확인하도록 합니다.



점수로 우선사항을 설정

- 우선순위 설정을 위한 위험 정보
  - 준수 (CVSS) or 진짜 위험?

멀웨어

이용 가능

고위험의 취약점,
즉각적인 행동

Vulnerability Listing

Exposures: Susceptible to malware attacks | Metasploit-exploitable | Exploit published

Title			CVSS	Risk	Published On	Severity	Instances	SANS	Exceptions
MS11-027: Cumulative Security Update of ActiveX Kill Bits	☣	M	10	919	Tue Apr 12 2011	Critical	1		Exclude
MS11-003: Cumulative Security Update for Internet Explorer	☣	M	9.3	919	Wed Feb 09 2011	Critical	1		Exclude
CIFS Account Password Never Expires			6.8	750	Mon Nov 01 2004	Severe	4		Exclude
CIFS Minimum Password Length Policy Not Enforced			6.8	750	Mon Nov 01 2004	Severe	1		Exclude
IRDP (ICMP Router Discovery Protocol) enabled			7.5	738	Wed Aug 11 1999	Critical	1		Exclude
IP Source Routing Enabled			7.5	738	Mon Sep 20 1999	Critical	1		Exclude
SMB signing disabled			7.3	703	Mon Nov 01 2004	Severe	2		Exclude
MS11-019: Vulnerabilities in SMB Client Could Allow Remote Code Execution		M	10	679	Tue Apr 12 2011	Critical	1		Exclude
SMB signing not required			6.2	679	Mon Nov 01 2004	Severe	2		Exclude
MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution			10	671	Tue Apr 12 2011	Critical	1		Exclude

Showing: 1 to 10 of 27 Rows per page: 10 1 of 3

Open a ticket

전통적인 CVSS

조직에 대한 위험점수

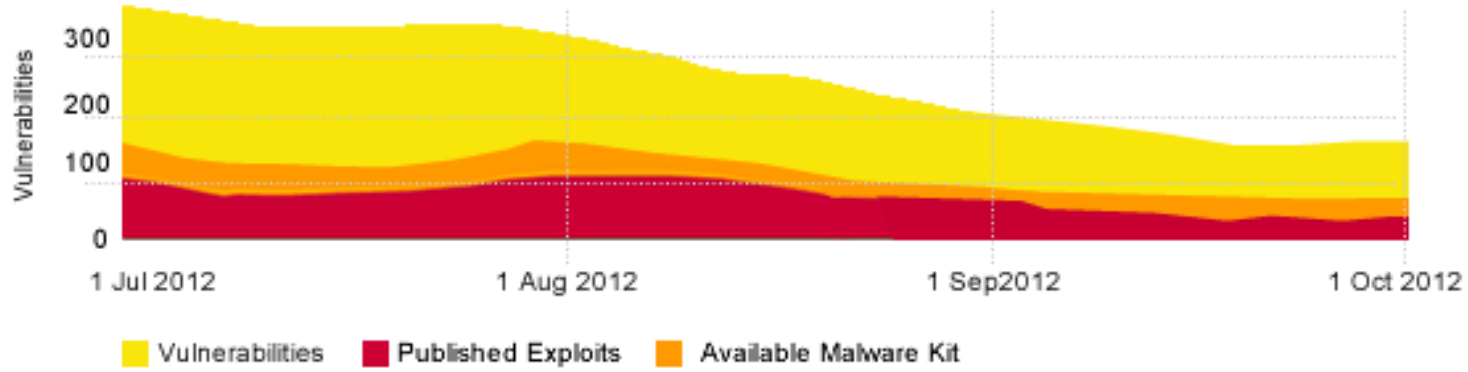
치료 순서 설정을 위한
점수

조직내의 보안지수 변화

Vulnerability Trend Report

Oct 1, 2012 14:01:47 PDT

Start date: Jul 1, 2012 | End date: Oct 1, 2012



Vulnerabilities in Sites

New: new vulnerabilities discovered
Reduced: vulnerabilities that were remediated or not found again

Datacenter 1

Total	Exploits	Malware Kits	Assets
100 (↓30)	0 (↓20)	0 (↓5)	1700
New +6 | Reduced -36	-21	New:	(previously 1650)

Datacenter 2

Vulnerabilities	Exploits	Malware Kits	ssets
170 (↓10)	10 (↓10)	5 (↓15)	200
New +6 | Reduced -1	New +0 | Reduced -10	New +0 | Reduced -15	viously 1200)

취약점 위험 관리의 기대효과

- 높은 위험에 대한 가시성 확대
  - 주요 취약점의 치료방법 효율화
  - 한정된 자원에 집중
  - 취약점 분류에 따라 전문가를 효율적으로 배치

① Top 25 Remediations by Risk

HO_REMTOP10_20130513

May 13, 2013 17:35:47 JST

② Applying 13 Top Remediations

③ Will Remediate 100% Vulnerabilities including: 100% published exploits, 0% available malware kits

Affecting 1 Assets

④

Remediations	Remediated Vulns			Affected Assets	Risk
Download and install Microsoft patch windowsxp-kb2508429-x86-enu.exe (664960 bytes)	4	6	0	1	3097
Download and install Microsoft patch windowsserver2003.windowsxp-kb2508429-x64-enu.exe (1044864 bytes)	4	6	0	1	3097
Download and install Microsoft patch windowsxp-kb982214-x86-custom-enu.exe (665464 bytes)	3	6	0	1	2368
Download and install Microsoft patch WindowsXP-KB971468-x86-ENU.exe (664952 bytes)	2	4	0	1	1593
Download and install Microsoft patch WindowsServer2003.WindowsXP-KB971468-x64-ENU.exe (1026944 bytes)	2	4	0	1	1593
Configure SMB signing	2	0	0	1	1469
Download and install Microsoft patch windowsxp-kb2705219-v2-x86-enu.exe (686608 bytes)	1	5	0	1	841
Download and install Microsoft patch windowsserver2003.windowsxp-kb2705219-v2-x64-enu.exe (1224216 bytes)	1	5	0	1	841
Disable NULL sessions	1	0	0	1	750
Download and install Microsoft patch windowsserver2003.windowsxp-kb2685939-x64-enu.exe (781568 bytes)	1	3	0	1	437
Download and install Microsoft patch windowsxp-kb2723135-v2-x86-enu.exe (572944 bytes)	1	3	0	1	437
Disable ICMP timestamp responses on Windows XP/2K3	1	0	0	1	0
Disable ICMP timestamp responses	1	0	0	1	0

취약점 위험 관리의 기대효과

가시성 확대

- 시스템 및 네트워크의 취약점 파악
- “양호” 상태의 변경 원인 파악 (예: 구성)
- 목표 지수를 이용하여 인지, 행동, 의무 수행

위협 대비

위험의 우선순위 관리

- 방어에 필요한 데이터 산출
- 단순한 취약점만이 아닌, 이용가능성에 따른 치료방법의 우선순위 설정
- 위험 해결을 위한 수치화가 가능한 대책 마련

효율성 증가

자동화

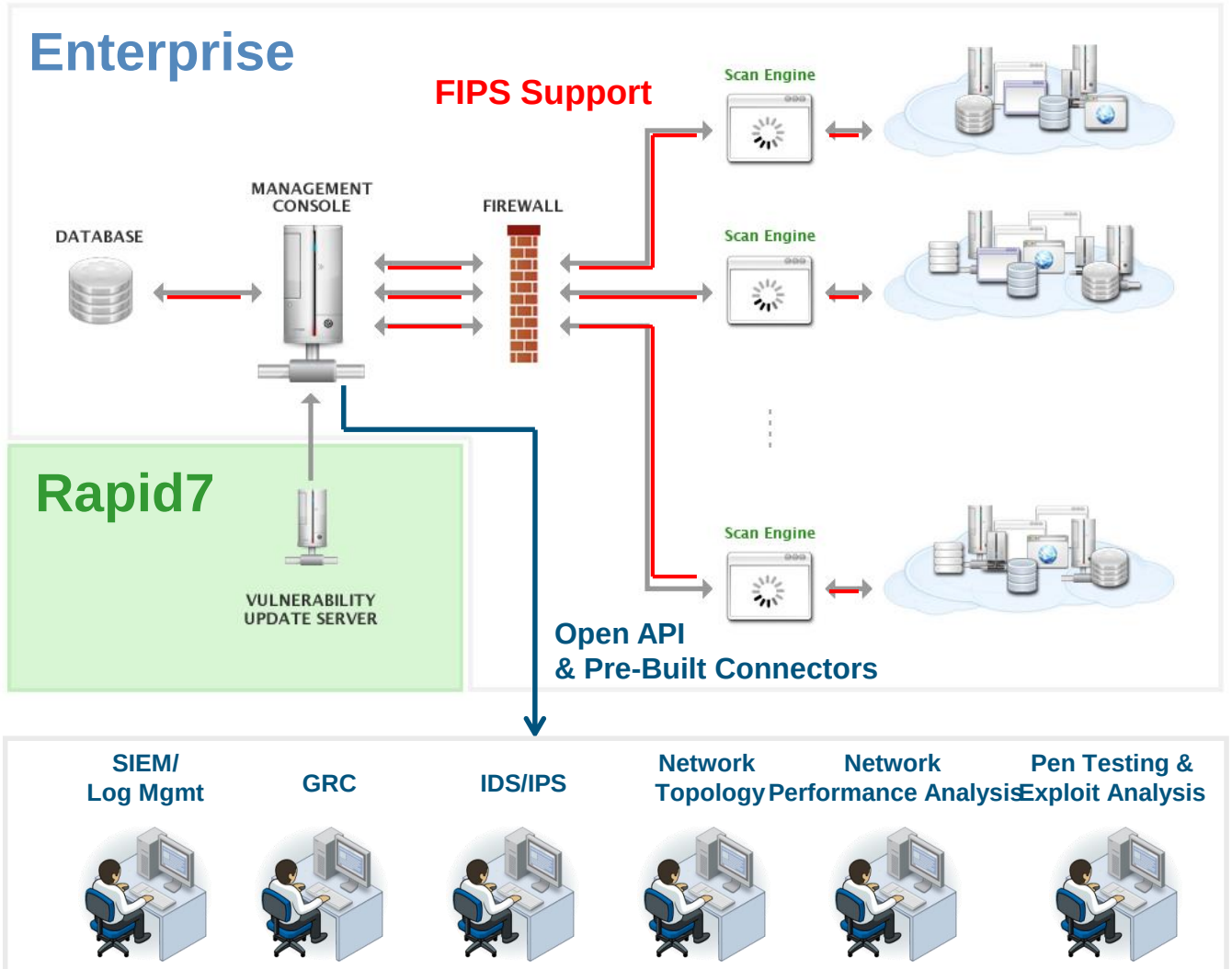
- 평가와 치료 주기의 자동화
- 데이터 정확성 증가를 위한 지속적인 평가 가능
- 업무연관 IT위험의 영향 산출

업무로 연계

NEXPOSE 아키텍쳐

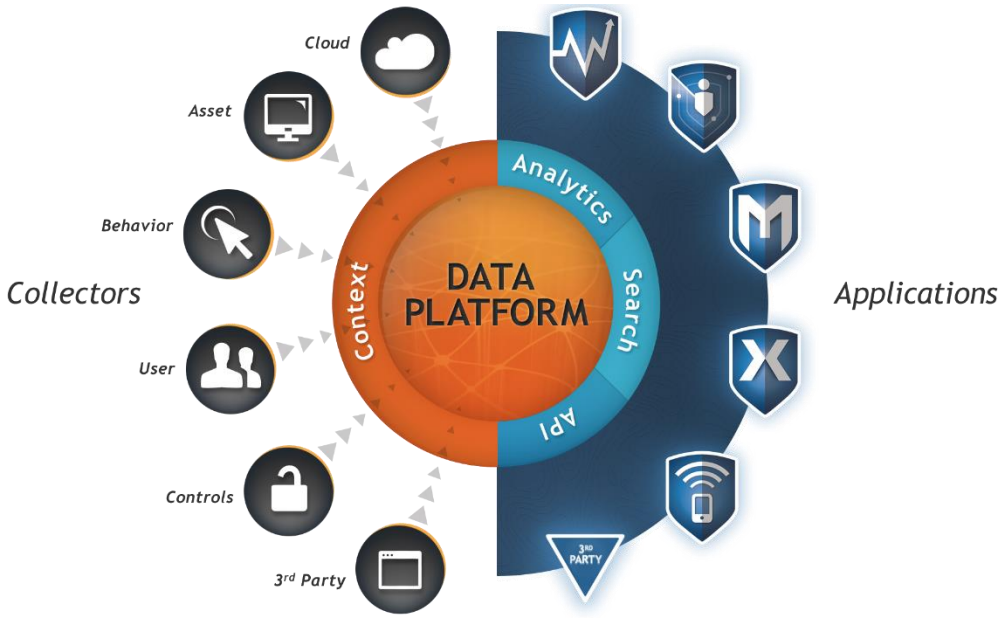
- 검색엔진의 분산 아키텍쳐를 통한 높은 확장성
- 단일 플랫폼을 통한 중앙 집중식 관리 및 보고 확립
- 유연한배포옵션 : 소프트웨어, 어플라이언스 및 관리 서비스
- 통합 확장을 위한 API 제공

NeXpose 는 고객의 요구 사항을 지원하기 위해 확장가능한 모든 솔루션을 제공합니다.



FIPS (Federal Information Processing Statandards) : 미국 연방 정부 기관에서 사용하는 정보처리 기계와 방식을 표준화 하기 위해 미국 국립 표준 기술연구소(NIST)가 제정하는 표준 규격. (데이터암호표준 : DES, 3DES)

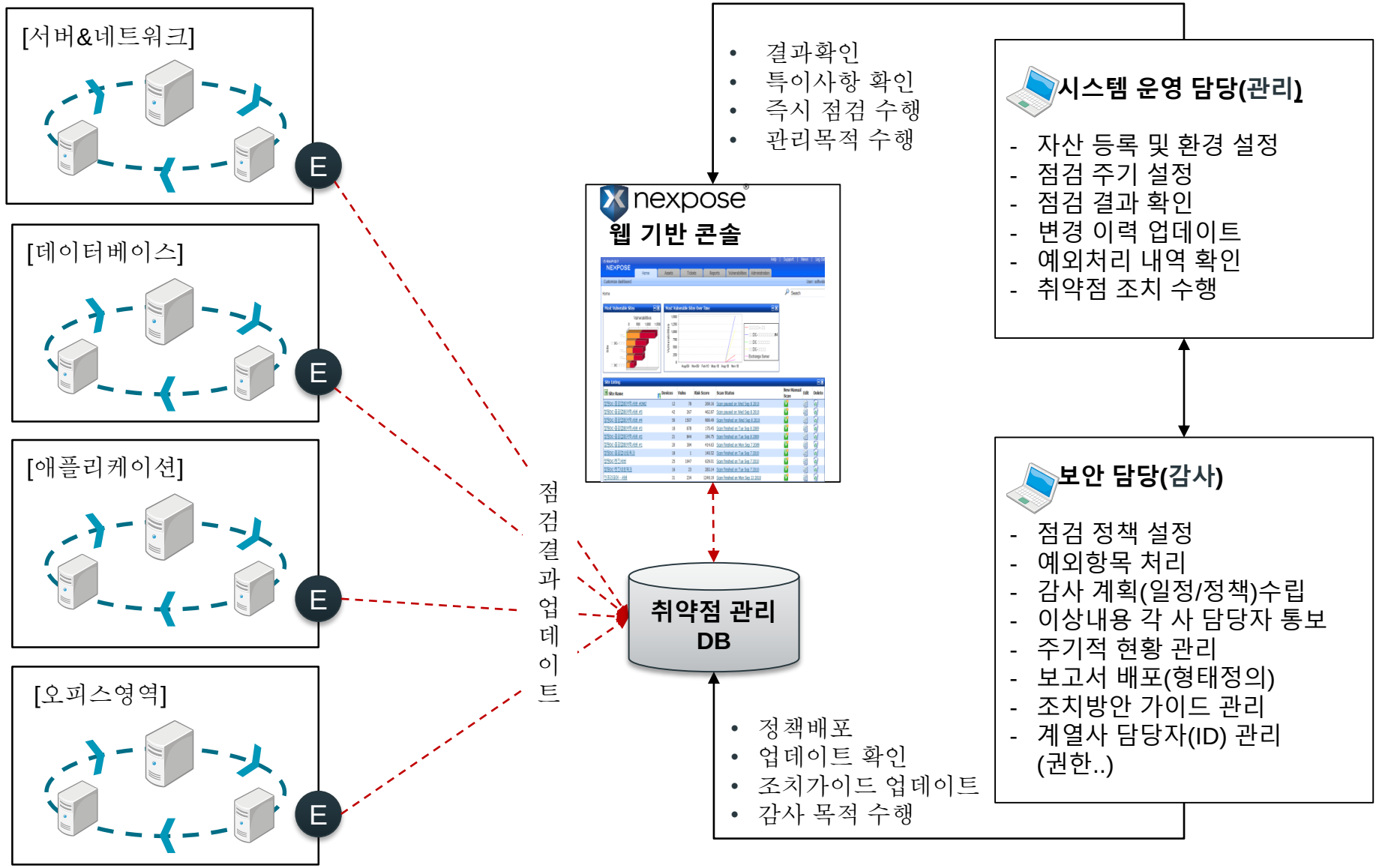
주요 장점



- IT인프라 100% 스캔
- 실제 위험 노출 상황에 대한 정확한 이해
- 취약점 우선순위를 신속하고 정확하게 파악
- 취약점의 익스플로이트 가능성 확인
- 최고 수준의 통합 취약점 스캔 기술
- 지속적인 취약점 업데이트
- 종합적인 규제 준수 및 정책 확인
- 단계별 문제 해결 계획 배포
- 가상화 자산의 지속적인 검색
- 사전 정의 및 맞춤이 가능한 강력한 보고서 및 대시보드
- 내부 조직의 보안지수 트렌드 비교

시스템아키텍쳐 및 구성

RAPID7 시스템 구성



INSEC security

점검 방식

NeXpose 는 해당 시스템에 **에이전트를 설치 하지 않고(Agentless)** 원격에서 점검이 가능하며, 취약점 조치 후 한번의 클릭으로 간단하게 이행점검을 실시 할 수 있습니다.

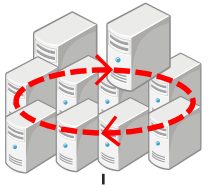
기본 점검 방식

NeXpose 는 접근할 대상에 대하여 일반 적인 Windows, Unix 프로토콜을 사용하여 네트워크를 통해 모든 스캔작업을 수행합니다. 이러한 아키텍쳐는 불필요한 설치 작업을 최소화 하여 보안과 안정성 및 편리성을 제공합니다.

에이전트 설치 없음

- 대상 선정
- 대상 아이피 입력
- 대상의 계정입력(옵션)
- 정책 설정 및 적용
- 수행 명령

[점검대상]



취약점 발견

취약점 조치

이행 점검
(원 클릭)

※ 원격 접속 타입

SMB/CIFS/TELNET/SSH/MSSQL/MYSQL/ORACLE/DB2/POP/FTP/CVS/SNMP 등 18개 타입 지원

RAPID7 점검 방식

32bit, 64bit 운영체제에 모두 설치가 가능하며, 윈도우 및 리눅스 플랫폼에서 운영 할 수 있습니다. 또한 시스템 운영에 필요한 OS 및 각종 응용프로그램 서비스, 데이터 베이스 등 총 50,000 여 개의 이상의 취약점을 점검 할 수 있습니다. (2011년 03월 업데이트 기준)

설치 세부 사양

1. 하드웨어 스펙 (노트북 가능)

- 서버 : IPS, IDS 등이 설치 되지 않은 독립적인 구성
- CPU : 2GHz 이상 / HDD : 80GB 이상 / NIC : 100 Mbps
- RAM : 2GB(32 bit), 8GB(64 bit)
- 네트워크 구성 : 40814, 80, 443, 37780 (Outbound)

2. 설치 가능 플랫폼

플랫폼	운영체제
윈도우	MSWindows Server 2003 SP2 / R (영문버전)
리눅스	• Red Hat Enterprise Linux5 • Ubuntu 8.04 LTS • SUSE Linux Enterpirse Server 10

점검 가능한 플랫폼

구분	점검 플랫폼
서버	NetBSD OpenBSD Red Hat Solaris SuSE Sun Microsystems UNIX Windows 등
네트워크	Cisco Finger Microsoft Networking Misc NFS Netware 등
서비스	Bind/ CVS DHCP DNS FTP LDAP Lotus Notes/Domino Mail Malware Microsoft Exchange Microsoft IIS 등
데이터베이스	AS/400 /Apple/ BSD/ Debian/ FreeBSD/ Linux/ Mac OS X/ Microsoft/ DB2 / Database 등
웹애플리케이션	SQL Injection / Cross-Site Scripting / 비암호화 확인등 PCI-DSS 에서 요청하는 OWASP Top 10 지원

* 추가 업데이트 예정

취약점 진단 프로세스

1. 취약점 관리 표준 수립
   - EUC, 서버/네트워크,DB, 애플리케이션등 대상 별 보안 수준을 고려한 기준 수립
   - 적용 대상 선정 (점검 범위, 기간 등)
   - 보안 항목, 진단 항목 도출
2. 자동 취약점 탐지
   - 점검 대상 파악
   - 진단 스케쥴링
   - 보안 진단 정책 수립 및 적용
3. 취약점 테스트 및 검증
   - 취약점 테스트 확인
   - 취약점에 대한 검증
4. 취약점 조치 및 이행점검
   - 취약점 수정 및 조치계획 수립
   - 조치된 취약점에 대한 이행 점검 수행
5. 보고서
   - 취약점 보고서 배포

RAPID7 Network & Server 취약점 점검

- **14,000**개 이상의 취약점을 확인하기 위한 **54,000**개가 넘는 점검 목록 보유
- Microsoft 지원 : 매월 목요일 발표되는 마이크로 소프트 보안 패치에 대하여 24시간 이내 취약점 업데이트 제공
- 설치되어 있는 패키지 중 취약한 패키지 탐지 및 수정방안 제공
- Backported 지원으로 인한 오탐 최소화
- 에이전트가 필요 없는 점검 지원
  - 계정정보 및 비 계정정보 이용 점검 지원
  - 높은 취약점 점검 수행 능력
  - 각 OS별 폴리시 지원 (Windows group policy, Unix Policy)
  - 안전 점검을 통해 장애 발생 최소화 (휴먼에러 최소화)
- 다른 일반 커버리지 영역
  - Adobe Flash, Adobe Reader, Cisco IOS, Mozilla, Firefox, Solaris
  - Sun JVM, Unix, 3Com

UNIX® Sun microsystems
redhat. IBM
Microsoft
cisco Novell
3COM

INSEC security

RAPID7 DATABASE 취약점 점검

- 계정정보 및 비 계정정보 이용 점검 지원
- DATABASE 취약점 검사
  - 기본 패스워드 검사
  - 기본 구성환경 설정 검사
  - 보안패치 확인
  - 버퍼 오버플러우
  - 리스너 제어 확인
  - 권한 상승
- 지원 DBMS
  - Oracle
  - Microsoft SQL Server
  - Sybase
  - MySQL
  - IBM DB2, DB/400
  - Lotus Notes / Domino
  - PostareSQL

ORACLE IBM PostgreSQL SYBASE Microsoft Informix SOFTWARE MySQL

"Database Servers represent 75% of all breached records"

Source: Verizon

INSEC security

RAPID7 DATABASE 취약점 점검

- 4세대 웹 스파이더 탑제
  - 서버 및 클라이언트 단 스캔
  - 인증 및 비 인증 모드에서 웹 애플리케이션 점검 기능
  - SQL 인젝션을 포함한 OWASP TOP10 지원
  - 디렉토리 경로 조작 및 취약점 검출
  - 파라메터 조작 및 취약점 검출

- 동적인 Web2.01 / AJAX 점검 지원
- 기존 취약점 진단과의 차별성

"취약점의 58%가 웹 애플리케이션에 영향을 줌"

"취약점의 73%가 쉽게 악용될 수 있음"

출처: 시만텍

	Web Scanners	NeXpose
Browser-Based Scanning		√
Web Application Vulnerability Pass-Through		√
Database Scanning		√
Third Party Application and Database Scanning		√
Operating System Scanning		√
Command Execution	√	√
Parameter Injection	√	√
SQL Injection	√	√
Cross-Site Scripting	√	√
Directory Traversal	√	√
Abnormal Input	√	√
Parameter Overflow/ Buffer Overflow	√	√

INSEC security

취약점 점검 항목

국내 정보보호 전문업체 및 공공기관 체크 리스트의 기준으로 작성된 체크 리스트이며, 해당 내용을 포함하여, 설치되어 있는 패키지 프로그램등 자동화 진단이 보유하고 있는 취약점 진단을 추가적으로 수행할 수 있는 장점이 있습니다.

항 목	상세 내역
계정관리 영역	불필요한 계정의 사용 및 패스워드 없는 계정의 로그인 허용 여부등을 판별합니다. (계정과 패스워드가 동일 취약점, 쉬운 패스워드로 설정되어 있는 계정 등)
파일 시스템 관리 영역	파일의 접근 권한 및 Path 환경 변수에 대한 체크등을 통하여 파일 시스템에 대한 보안 설정을 확인합니다.
네트워크 서비스 영역	NFS를 통하여 원격에서 불필요한 마운트가 되어 있는지, 침해 사고 위험성이 높은 NFS 서비스 사용 여부등 네트워크 영역에서 잘못된 보안 설정을 확인합니다.
주요 응용 프로그램 설정 영역	Samba, OpenSSH 버전 또는 Command 쉘을 웹에서 사용하지 않도록 레지스트리 값 설정등을 체크하여 응용영역에서 발생할 수 있는 취약점을 확인합니다.
웹서버 보안 영역	아파치, IIS 등의 웹서버 등의 설정 및 보안패치 여부를 확인합니다.
웹 애플리케이션	크로스 사이트 스크립팅, SQL 인젝션, 암호화 처리 확인 등 기본적으로 입력값 검증을 통해 웹 애플리케이션 취약점을 점검. (OWASP 지원)
관련 패치 영역	최신 OS 버전체크 및 핫픽스 적용 여부등을 확인합니다.

RAPID7 업계 최초의 공격 코드 공개

점검 완료 후 해당 취약점에 대한 공격 코드가 외부에 노출되어 있는 취약점을 찾아 나열 할 수 있습니다.
이는 가장 먼저 조치해야 할 취약점에 대한 우선순위를 확인하는데 꼭 필요한 작업입니다.

1. 공격코드가 외부에 노출되어 있는 취약점 확인

2. 공격 코드는 METASPLOIT (모의해킹도구)을
   통해 실제 해킹이 가능

3. 모의해킹 도구를 통한 실제 검증 가능

담당자는 다양한 취약점 중
우선조치 취약점을 먼저 확인 할 수 있음.

Vulnerability Listing	
Vulnerability	Exploitabilit
JRE Audio and Image File Buffer and Integer Overflow Vulnerabilities	-exploitable
JRE Multiple Overflows	-exploitable
JRE Deserializing Calendar Objects	-exploitable
Microsoft Office Web Components Code Execution Vulnerability	-exploitable
MS10-018: Cumulative Security Update for Internet Explorer	-exploitable
MS09-072: Cumulative Security Update for Internet Explorer	-exploitable
MS10-002: Cumulative Security Update for Internet Explorer	-exploitable
Microsoft DirectShow Streaming Video ActiveX Control Buffe Overflow	-exploitable
JRE Deployment Toolkit Vulnerability	-exploitable
JRE Java Web Start JNLP Vulnerability	-exploitable
JRE Untrusted Application Privilege Escalation Vulnerability	-exploitable
APSB10-07: Adobe Reader Unspecified Privilege Escallation	-exploitable
MS09-053: Vulnerabilities in FTP Service for Internet Information Services Could Allow Remote Code Execution	-exploitable
APSB10-02: Adobe Reader Doc.media.newPlayer Memory Corruption Vulnerability	-exploitable

[취약점 리스트 중 공격이 가능한 취약점만 나열]

INSEC security

RAPID7 평가 비교 자료

	Company	Cost	Deployment Options	Implementation	Accuracy	Ease of Use
RAPID7	Rapid7 NeXpose	Best Value	Software, Appliance or Managed Service	Customer Install or Consultant Install	High	Organized, Actionable Scanning and Reporting
QUALYS	Qualys	More Expensive	Managed Service and Appliance	Customer Installs	Moderate	Difficult to Follow Remediation
nCircle	nCircle	More Expensive	Appliance	Engineer Required	Moderate	Difficult to Navigate Screens and Run Scans
McAfee	McAfee Foundstone	More Expensive	Appliance	Engineer Required	Moderate	Scan Results are Difficult to Read and Execute
IBM	IBM ISS	More Expensive	Software, Appliance or Managed Service	Customer Installs	Moderate	Microsoft Focused
TENABLE Network Security	Tenable Nessus	Free with Subscription	Managed Service	Customer Installs	Low	Must Manually Export Results with Scripts and Pivot Tables

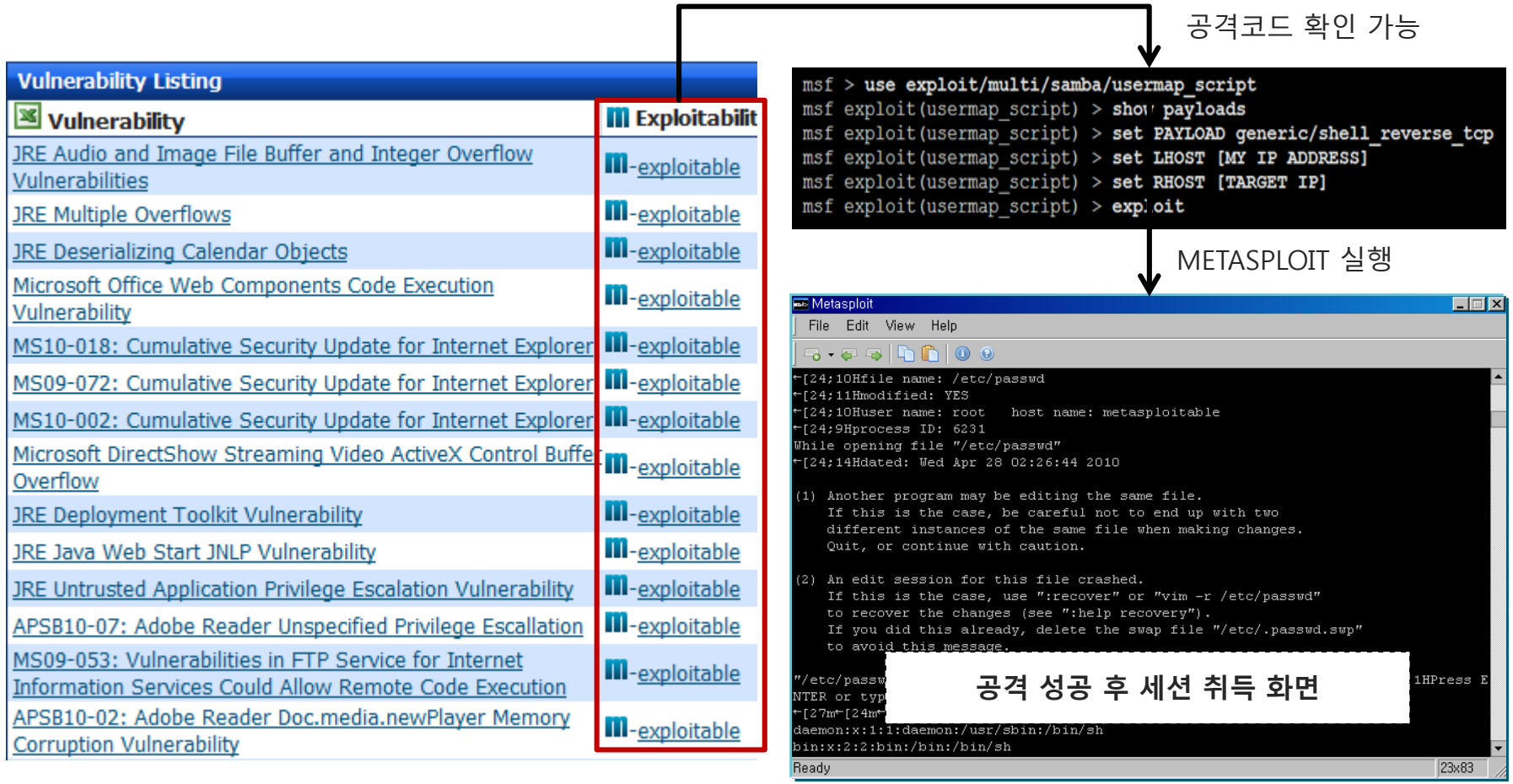
RAPID7 Metasploit Express places 1st in HackMiami Penetration Testing Competition

Category	METASPLOIT express	CORE SECURITY TECHNOLOGIES	IMMUNITY KNOWING YOU'RE SECURE
Interface	★★★★	★★★★	★★½
Exploits	★★★★½	★★★★	★★★
Reporting	★★★★½	★★★½	★★★
Additional Features	★★★½	★★★★½	★★★
Value	★★★★★	★★	★★★★
Total Score	★★★★½	★★★½	★★★

INSEC security

취약점 검증 방법

METASPLOIT 을 통한 공격 성공 화면 으로 이와 같이 간단한 작업으로 해킹은 손쉽게 성공할 수 있습니다.



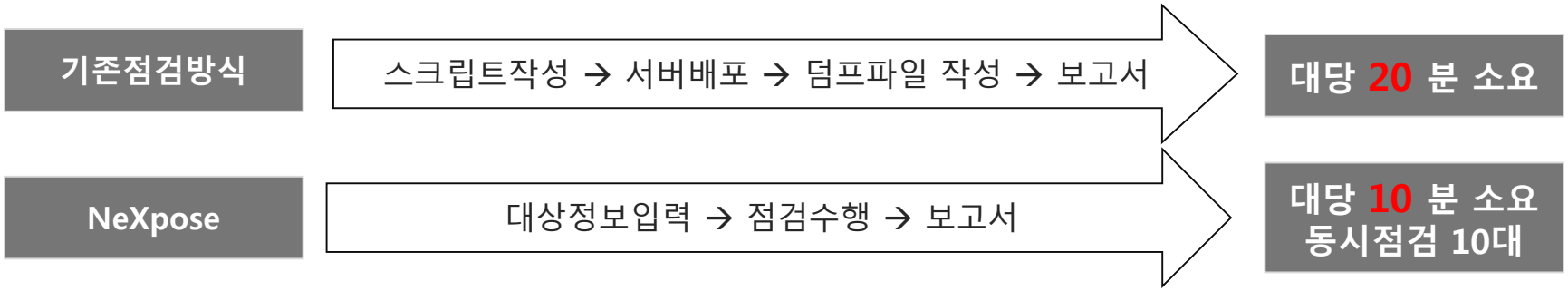
Vulnerability Listing

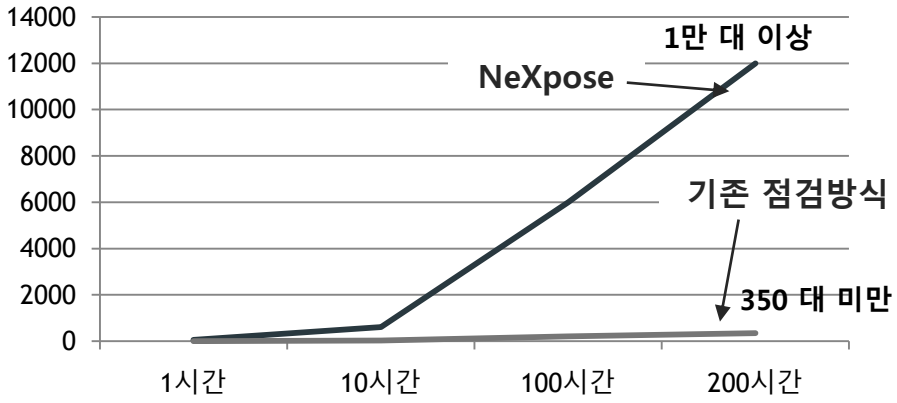
Vulnerability	Exploitabilit
JRE Audio and Image File Buffer and Integer Overflow Vulnerabilities	-exploitable
JRE Multiple Overflows	-exploitable
JRE Deserializing Calendar Objects	-exploitable
Microsoft Office Web Components Code Execution Vulnerability	-exploitable
MS10-018: Cumulative Security Update for Internet Explorer	-exploitable
MS09-072: Cumulative Security Update for Internet Explorer	-exploitable
MS10-002: Cumulative Security Update for Internet Explorer	-exploitable
Microsoft DirectShow Streaming Video ActiveX Control Buffer Overflow	-exploitable
JRE Deployment Toolkit Vulnerability	-exploitable
JRE Java Web Start JNLP Vulnerability	-exploitable
JRE Untrusted Application Privilege Escalation Vulnerability	-exploitable
APSB10-07: Adobe Reader Unspecified Privilege Escallation	-exploitable
MS09-053: Vulnerabilities in FTP Service for Internet Information Services Could Allow Remote Code Execution	-exploitable
APSB10-02: Adobe Reader Doc.media.newPlayer Memory Corruption Vulnerability	-exploitable

[취약점 리스트 중 공격이 가능한 취약점만 나열]

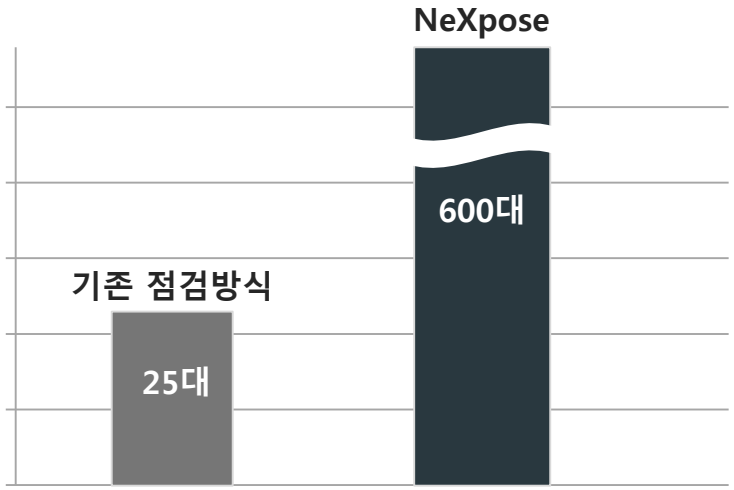
점검 시간 및 취약점 항목 비교

300대 기준 점검 시 기존의 점검방식 보다 약 20배 빠르게, 점검 항목 수는 최신 취약점 항목을 포함한 점검을 손쉽게 수행 할 수 있습니다. (기존 점검은 모든 취약점 최신 정보를 확인하기는 한계가 있음)
시간, 인력, 비용, 보안성 강화 측면 모두 완벽하게 이전 점검 방식을 획기적으로 변화 시킬 수 있으며, 각 분야의 보안 전문가가 없이 모두 수행 할 수 있습니다.





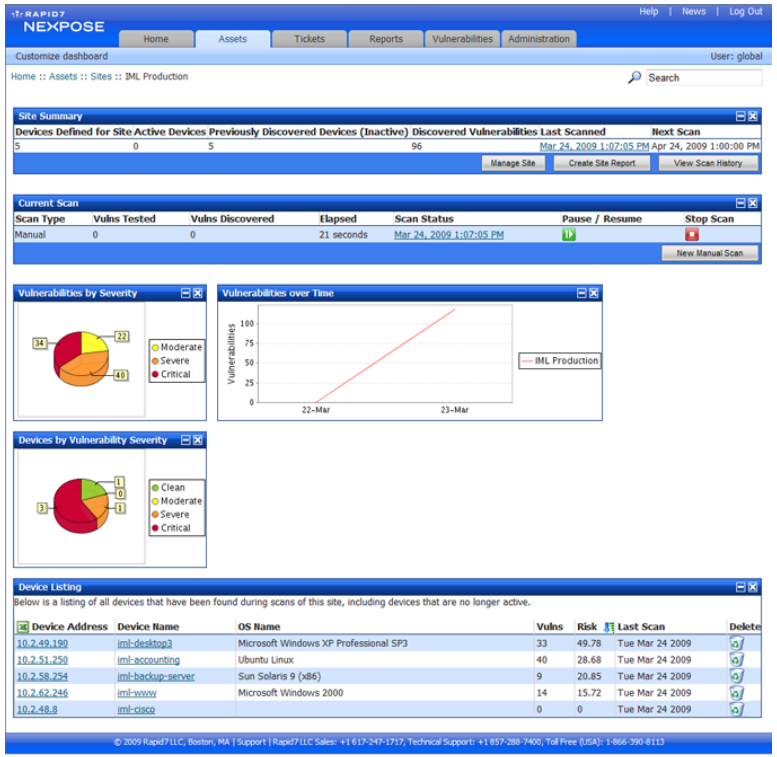
[시간에 따른 점검 장비 속도 그래프]

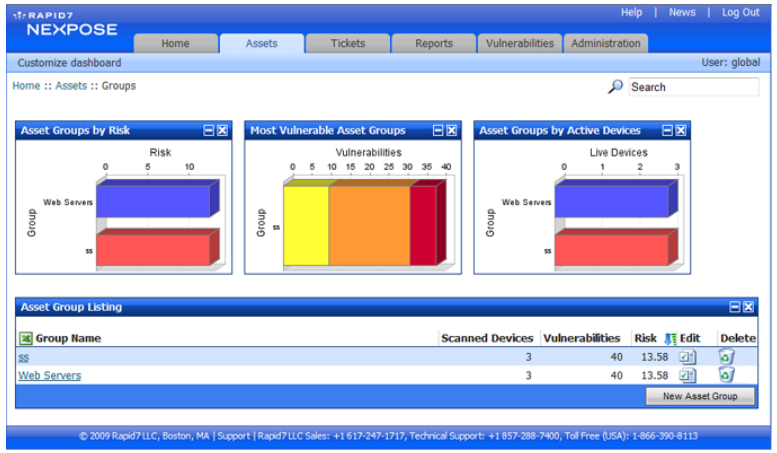


[10시간 기준 취약점 점검 대수 비교]

강력한 중앙 관리 기능

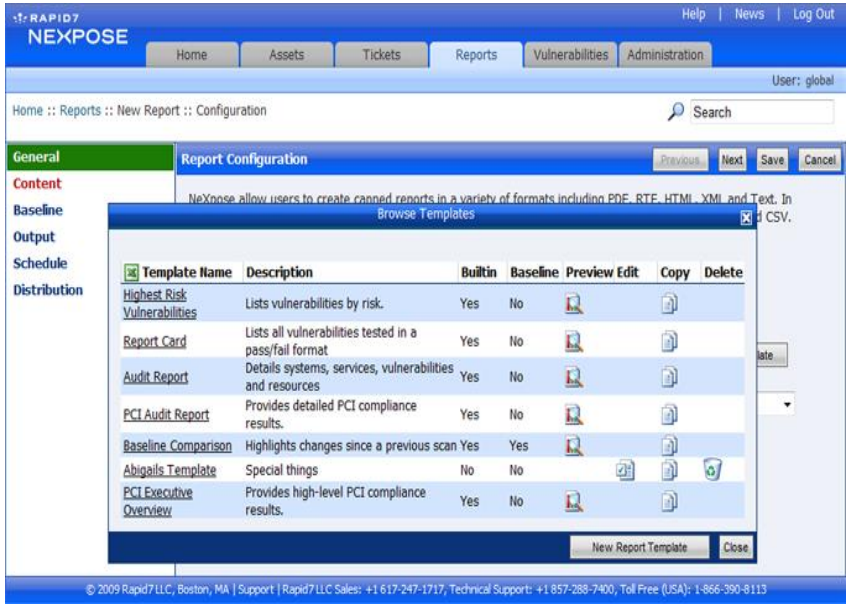
- 지리적 또는 조직적으로 분산된 네트워크 환경에 대한 중앙집중화된 관리
- 위임 받은 관리자에 대한 역할 기반 접근 제공
- 접근하는 사용자 수를 제한하지 않고 보고서 제공
- 역할 기반 그룹화를 위해 Active Directory 와 다른 저장소와의 통합을 제공

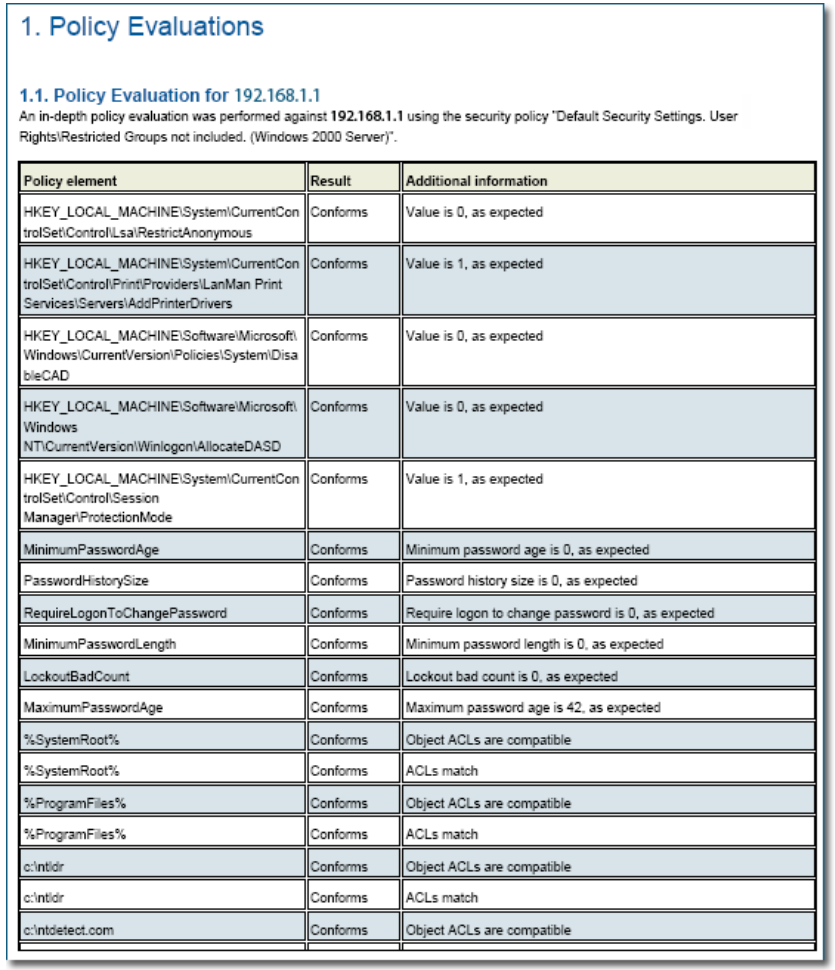




컴플라이언스 정책 지원

*PCI, HIPPA, NERC 또는 FISMA와 같은 규정이행 정책이나 기업 정책에 규제받는 시스템에 대한 빠른 지원 및 이행 상황 확인을 제공 (1,000여 개 이상의 기업에서 기 사용)





1. Policy Evaluations

1.1. Policy Evaluation for 192.168.1.1

An in-depth policy evaluation was performed against **192.168.1.1** using the security policy "Default Security Settings. User Rights\Restricted Groups not included. (Windows 2000 Server)".

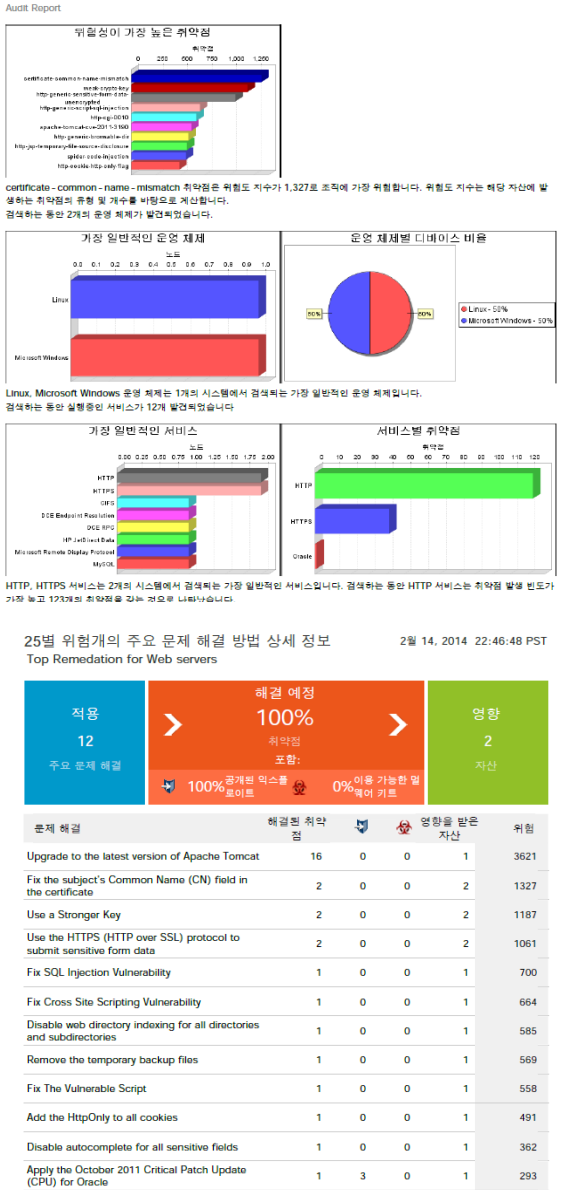
Policy element	Result	Additional information
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers	Conforms	Value is 1, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode	Conforms	Value is 1, as expected
MinimumPasswordAge	Conforms	Minimum password age is 0, as expected
PasswordHistorySize	Conforms	Password history size is 0, as expected
RequireLogonToChangePassword	Conforms	Require logon to change password is 0, as expected
MinimumPasswordLength	Conforms	Minimum password length is 0, as expected
LockoutBadCount	Conforms	Lockout bad count is 0, as expected
MaximumPasswordAge	Conforms	Maximum password age is 42, as expected
%SystemRoot%	Conforms	Object ACLs are compatible
%SystemRoot%	Conforms	ACLs match
%ProgramFiles%	Conforms	Object ACLs are compatible
%ProgramFiles%	Conforms	ACLs match
c:\intldr	Conforms	Object ACLs are compatible
c:\intldr	Conforms	ACLs match
c:\ntdetect.com	Conforms	Object ACLs are compatible

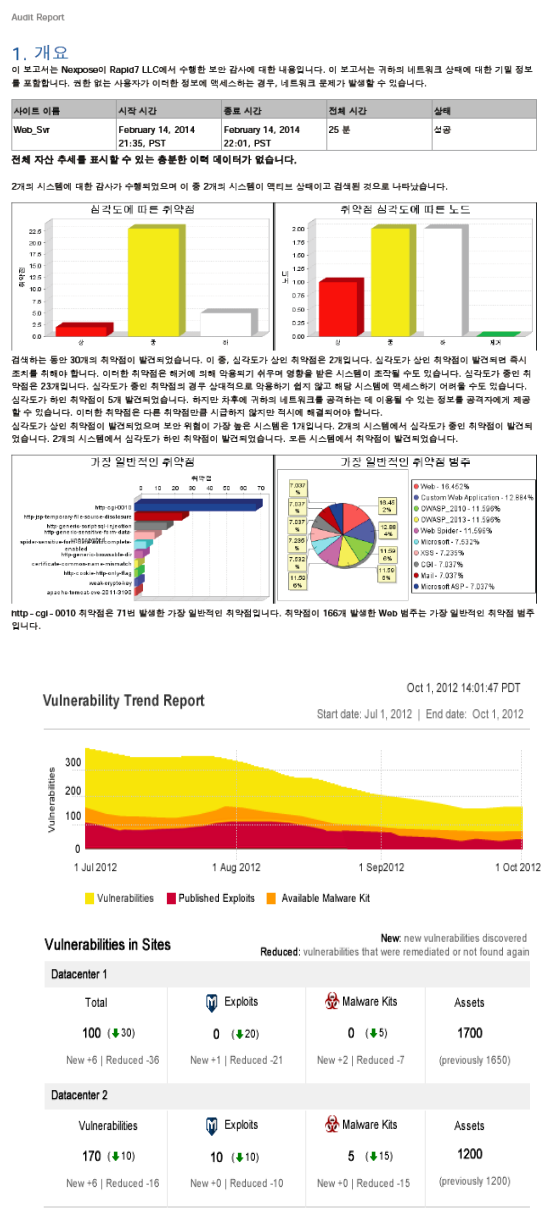
- **PCI**: Payment Card Industry
- **HIPPA**: Health Insurance Portability and Accountability Act
- **NERC** : Natural Environment Research Council
- **FISMA** : Federal Information Security Management Ac

INSEC security

RAPID7 컴플라이언스 정책 지원

- 사용자 친화적인 보고서
- 관리자 대시보드로 보안 상황에 대한 손쉬운 이해 및 확인
- 즉시 추가 가능한 보고서 기능
- 엔터프라이즈 관리/관제 시스템과의
  손쉬운 결과 Data 연동
- 다양한 보고서 생성
- 배포용 보고서와 경고를 위한 메일링 기능 제공
- XML, PDF, HTML, RTF, TXT, CSV 레포트 제공

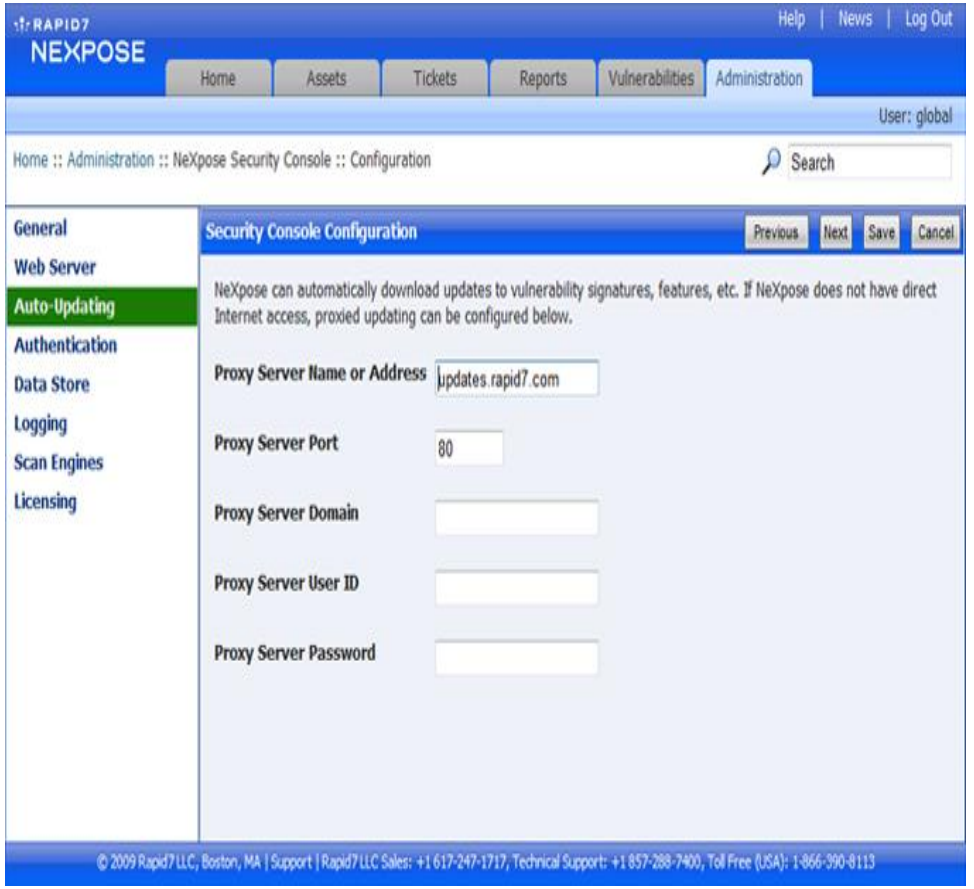




INSEC security

컴플라이언스 정책 지원

- ✓ 사용자의 확인을 필요로 하지 않는 자동 업데이트를 제공
- ✓ 즉각적인 마이크로소프트 취약점에 대한 패치 업데이트 확인
- ✓ 위협 환경의 변화에 따른 보안 상태를 유지하기 위한 정보 제공



RAPID7 사용한다면...

고객사는 **금융권과 동일한 수준**의 네트워크 시스템 보안성을 유지 가능

위험 평가 점수를 통해 내부 및 계열사별 보안수준을 한 눈에 확인 가능

NeXpose 에서 제공하는 위험 평가 점수는 신뢰할 수 있는 글로벌 산업표준 준수(**ASV 등록**)

실제 공격코드 활용하여 관리자가 발견된 취약성에 대한 "**확인 -> 검증 -> 조치 -> 평가**"가 가능

→ 발견된 취약점을 통한 악용 수준을 확인
→ 실제 문제를 확인하고 평가
→ 손쉬운 모의해킹 수행

IT 자산에 대한 전체 취약점에 대한 점검에서 보고서 배포까지 **자동화된 프로세스**로 수행 가능

XML 기반의 API 제공을 통한 확장성 있는 연동 기능을 통한 유기적 취약점 관리 가능.

Thank you!

제품문의 : 02-863-5687 대표영업 담당자 : 김성훈 부장

홈페이지 : http://www.insec.co.kr Email : sean@insec.co.kr

주 소 : 서울시 금천구 가산디지털1로 128 STX V-TOWER 505 (우) 153-803