RAPID7

취약점 진단 도구

NEXPOSE ENTERPRISE

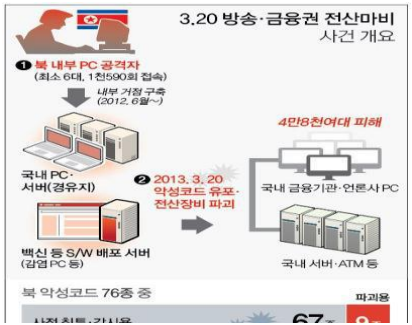
INSEC security

RAPID7

Contents

INSEC security

국내 보안의 현주소

사이버 테러	개인정보유출 피해	기술정보 유출
		
방송국, 은행 등 주요 전산망 마비	카드사, KT등 개인정보 유출	한수원, 선박 건조, 철강공정 등 기술유출
8,672억 원	**130억~970억 원**	**2조 8천억~35조 원**

! 보안 사고로 인한 손실액이 자연 재해 손실액에 약 2.5~3배 이상 큼

일상 속으로 파고든 보안 취약점

지능형 CCTV, AI 스피커 등 IoT 결합 서비스 대상 사이버 위협 증가

- IoT 결합 서비스 위협 증가

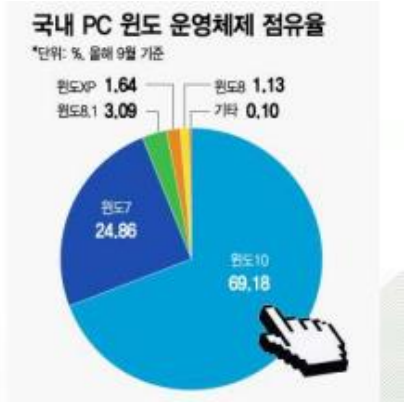
[2020년 KISA 자료 참조]

윈도우 RDP 취약점 미패치 시스템을 노린 제2의 워너크라이 등장 우려

- RDP 취약점 미패치 시스템공격

지원 중단 혹은 예정 운영체제 취약점 공격 시도

- 지원중단 예정 OS 국내 점유율



[스탯카운터 자료 참조]

랜섬웨어도 취약점을 악용합니다

알약 블로그, MS17-010 취약점 업데이트 했다면 안심해도 된다고 밝혀

[보안뉴스 원병철 기자] 현재 유럽을 강타하고 있는 페트야(Petya) 랜섬웨어가 워너크라이 랜섬웨어와 동일한 SMB 취약점 'MS17-010'을 이용한것으로 드러났다. 이스트시큐리티의 백신 브랜드 알약은 자사 블로그를 통해 페트야 랜섬웨어는 2016년 초 최초 발견되었던 랜섬웨어로, MFT(Master File Table) 영역에 대한 암호화뿐만 아니라 MBR(Master Boot Record) 영역을 감염시켜서 시스템 자체를 먹통으로 만든다고 강조했다.

▲ 페트야 랜섬웨어 스트링 코드[이미지=알약 블로그]

윈도우 SMB 보안 취약점을 이용한 패트야(Petya) 랜섬웨어 유포 사례

끊이지 않는 제로데이 취약점 공격

	Log4J	Spring4Shell
등록일	2022.01.20	2022.03.29 / 2022.03.31
CVE ID	CVE-2022-23302 CVE-2022-23305 CVE-2022-23307	CVE-2022-22963 CVE-2022-22965
내용	log4j JMSSink, Chainsaw 원격 코드 실행 및 JDBCAppender SQL 인젝션에 취약	Spring Cloud Fucntion, Spring MVC, Spring WebFlux 애플리케이션이 원격코드 실행에 취약
취약한 버전	Apache Log4j 1.x JMSSink Japache Log4j 1.x DBCAppender Apache Log4j 1.x, Apache Chainsaw 2.1.0 〈 Chainsaw	JDK 9+, Apache Tomcat, WAR, Spring-webmvc, Spring-webflux dependency
조치 방안	Apache Log4j 2.x버전으로 업데이트	Spring Framework 버전 업데이트

국내 취약점 관리 현황과 자동화 관리 방식의 비교

구 분	수동 진단 [기존 방식]	자동화 진단/관리 [Nexpose]
진단주기	년 1~2회 / 일회성 서비스	수시 진단 / 관리
수행 결과 [1일 기준]	Man / Months [50대 Max.]	Man / Months [Unlimited EA] 무제한 범위 진단 수행
수행 방법	자체 제작 스크립트(Script) 진단 수행	에이전트 없이 네트워크를 통한 원격 진단
수행 범위	샘플링(Sampling), 부분적 취약점만 진단	전수 조사, 거의 모든 알려진 취약점 진단
신규 도입 / 변경	자산의 신규도입 또는 서비스 변경 시 누락 또는 취약점 장기간 존재 위험	자산의 신규도입 또는 서비스 변경 시 즉시 진단 수행
비용 / 속도	고비용 저효율 방식으로 고급 인력 참여 기피	지속적인 비용 및 리소스 절감 저비용, 매우 빠른 진단 속도
보고서	수동으로 작성 [텍스트 형태의 결과물]	다양한 자동화 보고서 산출
조사 범위 / 깊이	인력을 통한 스크립트 기반 진단 수행 진단 범위 제한적 진단 속도 매우 느림	잘 알려진 모든 운영체제, 어플리케이션, 서버, 웹, DB, 유무선 네트워크, 보안 시스템 등 폭넓은 영역을 빠른 속도로 정확하게 진단

RAPID7

Contens

INSEC security

시스템/네트워크 취약점 점검 솔루션 – Nexpose

Nexpose 란?

Nexpose는 OS, DB, Application, Server, Network 등
IT 자산의 취약점을 한번에 점검해주는 보안 취약점 진단 솔루션입니다.
Agentless 방식으로 취약점 보안설정, 보안통제 영역의 위험을 통합적으로 진단합니다.

Nexpose 특장점

1. 높은 스캔 정확도
2. 동적 자산 자동 식별 (DHCP, VMWARE, AWS, MOBILE)
3. 동적 자산 그룹 자동 업데이트 (DAGS)
4. CLOSE LOOP 취약점 검증 (WITH METASPLOIT PRO)
5. REALRISK™ AND REALCONTEXT™ (실제 위협 반영)
6. 최우선 해결 조치 보고서
7. 적응형 보안 (자산의 변경, 새로운 위협에 자동 대응)
8. 풍부한 OPEN API 제공으로 유연한 연동 확장

취약점 관리의 이점

01

보안 취약점 관리 비용이 감소

✓ 사용자는 보안 취약점 관리를 위해 높은 비용의 보안 컨설팅 서비스를 고려 할 필요가 없어지게 된다. 또 내부의 전담 기술 인력을 통한 운영과 유지보수에 대한 부담도 함께 감소하게 된다.

02

보안 수준의 실시간 확인 및 보안 취약점의 관리 내역 조회가 가능

✓ 기업은 시간의 제약 없이 원하는 때마다 보안 취약점 진단을 진행하여 보안 수준을 확인하거나 과거의 진단 내용을 확인할 수 있다. 또 조치 내역을 기록하여 취약점에 대한 대응 결과를 관리할 수 있다.

03

최신 최약점 대응 및 표준화 영역으로 확장 가능

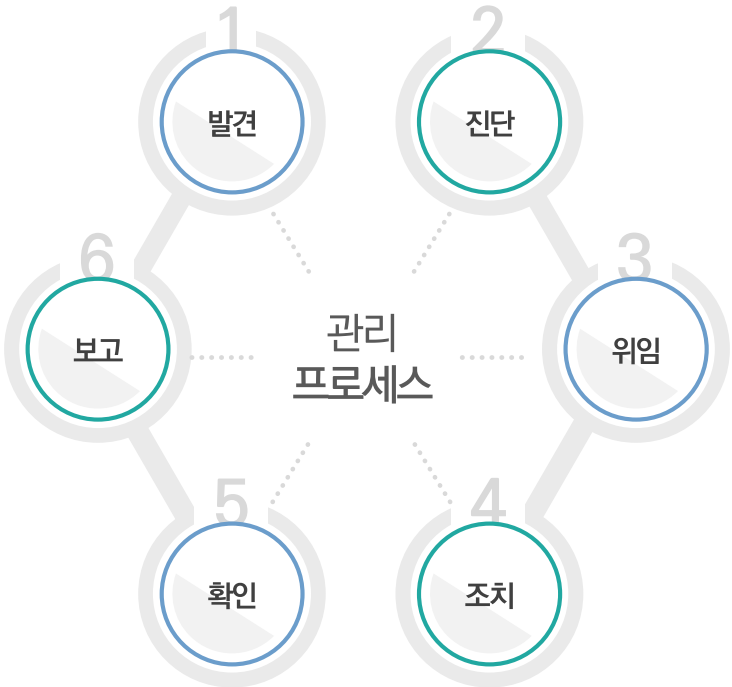
✓ 최신 보안 취약점을 보다 빠르게 분석하고, 분석 결과에 부합하는 진단 방법을 표준화 가능하게 적용해 수많은 위협에 유연하게 대처할 수 있다.

RAPID7

Contens

INSEC security

Nexpose 관리 프로세스

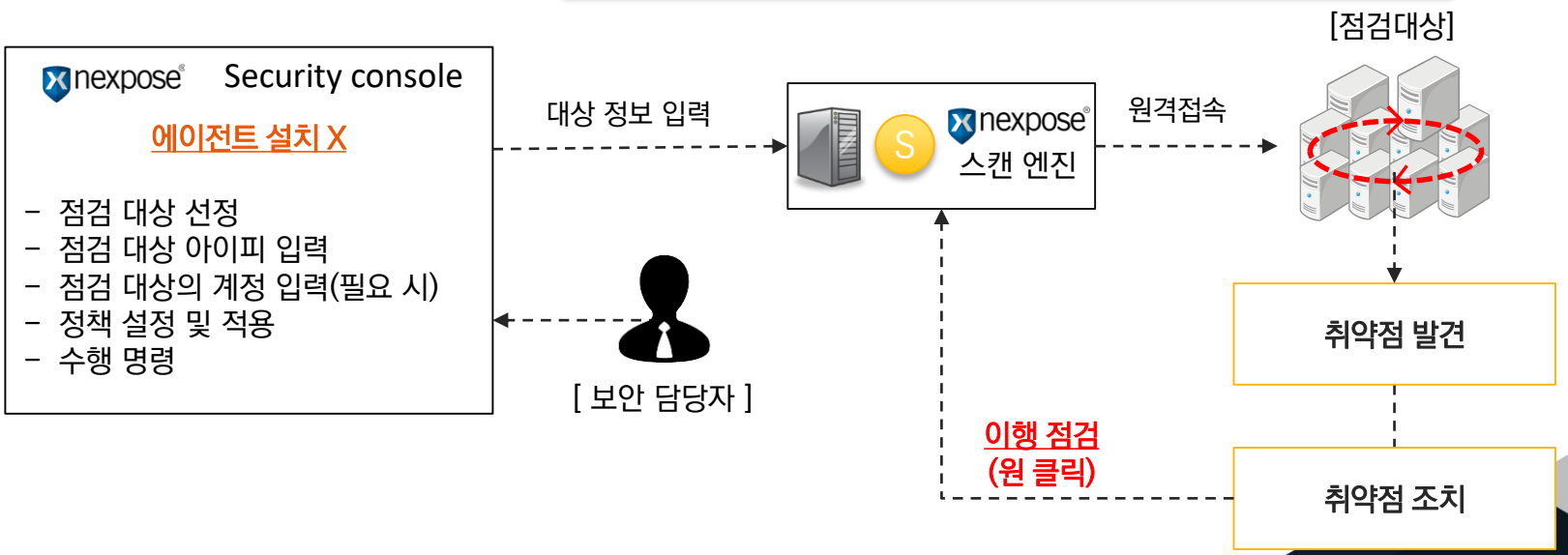


1. 발견 – IT 자산을 식별하고 분류
2. 진단 – 취약점 스캔 수행
3. 위임 – 고위험 순으로 취약점 조치 권고 전달
4. 조치 – 패치, 업그레이드, 대체 방안 등 조치 이행
5. 확인 – 취약점 제거 이행 검증을 위한 스캔
6. 보고 – 책임자에 위험 진단 처리 결과 보고

Nexpose 점검 방식

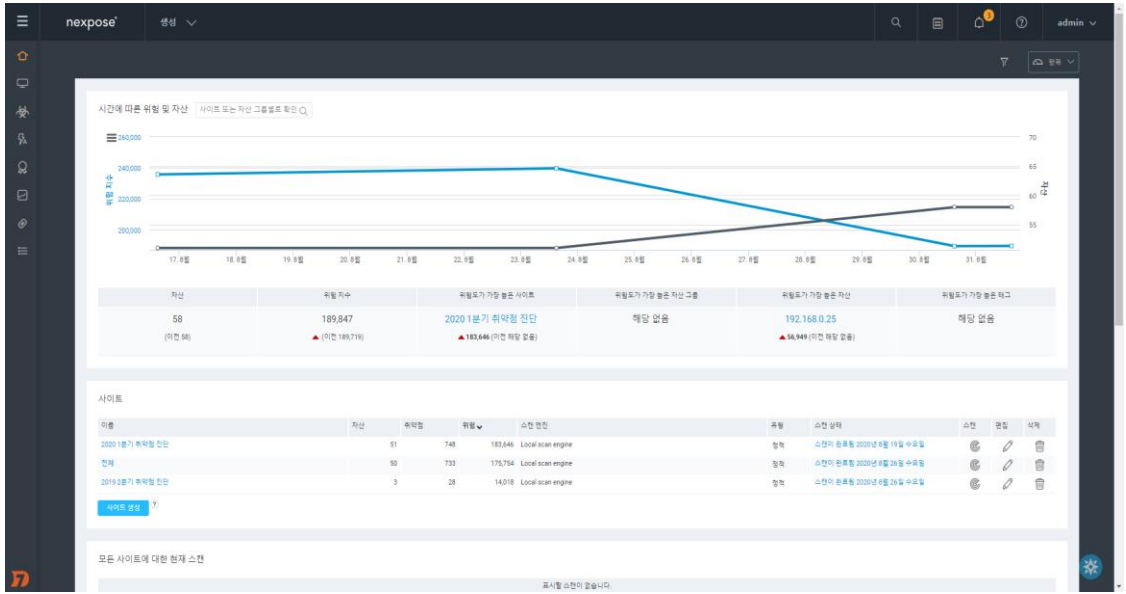
기본 점검 방식

Nexpose 는 접근할 대상에 대하여 일반적인 TCP/IP 프로토콜을 사용하여 네트워크를 통해 모든 스캔작업을 수행합니다. 이러한 아키텍쳐는 불필요한 설치 작업을 최소화 하여 보안과 안정성 및 편리성을 제공합니다.



효율적인 통합 보안 진단 기능

➢ 한번의 스캔으로 전체 진단



✓ 간단한 설정

✓ 통합된 스캔
OS, 어플리케이션, 서비스
웹, 데이터베이스, 보안설정

✓ 압축된 리포트

취약점 우선순위 결정 기능

➢ 우선순위 설정을 위해 신뢰성 있는 다각적 위험 정보 제공

고 위험 취약점에 즉각적인 조치

멀웨어 공격 위험

Exploit 공격 위험

취약점

> 필터 적용 (0 적용됨)

제목			CVSS	CVSSv3	위험	게시일	수정일	심각도	인스턴스	예외
Microsoft CVE-2017-0146: Windows SMB Remote Code Execution Vulnerability	☣	Ⓜ	9.3	8.1	919	Tue Mar 14 2017	Fri Aug 23 2019	상	1	예외 처리
Default or Guessable SNMP community names: public			10		916	Wed Jan 01 1997	Wed Dec 04 2013	상	1	예외 처리
Microsoft SQL Server Obsolete Version			10		914	Thu Jul 01 1999	Thu Jul 09 2020	상	1	예외 처리
Default or Guessable SNMP community names: private			10		913	Tue Feb 08 2000	Thu Nov 10 2016	상	1	예외 처리
SMTP credentials transmitted unencrypted			7.3		868	Mon Nov 18 1996	Thu Jun 19 2014	중	2	예외 처리
IMAP credentials transmitted unencrypted			7.3		868	Mon Nov 18 1996	Thu May 29 2014	중	1	예외 처리
POP credentials transmitted unencrypted			7.3		868	Mon Nov 18 1996	Wed Jun 18 2014	중	1	예외 처리
SMB signing disabled			7.3		843	Mon Nov 01 2004	Wed Feb 21 2018	중	4	예외 처리
SMBv2 signing not required			6.2		839	Mon Nov 01 2004	Wed Feb 21 2018	중	10	예외 처리
SMB signing not required			6.2		839	Mon Nov 01 2004	Wed Feb 21 2018	중	4	예외 처리

356 중 1 ~ 10 표시 | CSV로 내보내기 페이지당 행 수: 10 1 36 중

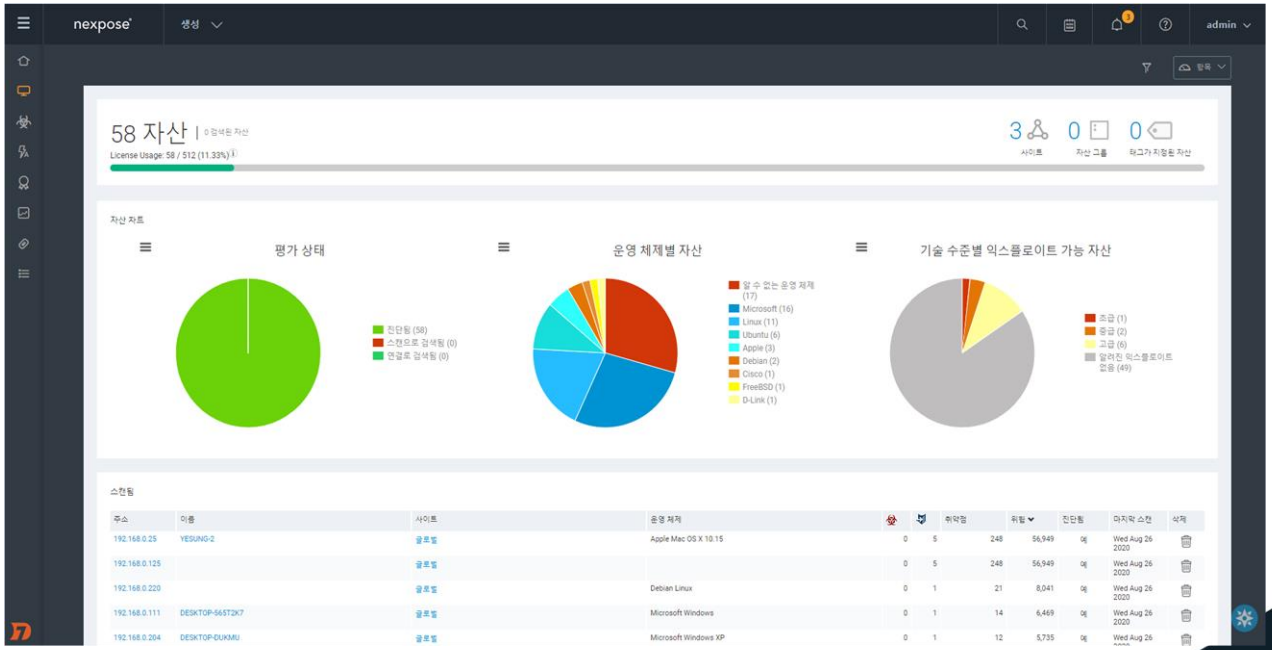
조치순서 결정을 위한 기준

전통적 CVSS

전체 조직에 대한 취약점 별 위험점수

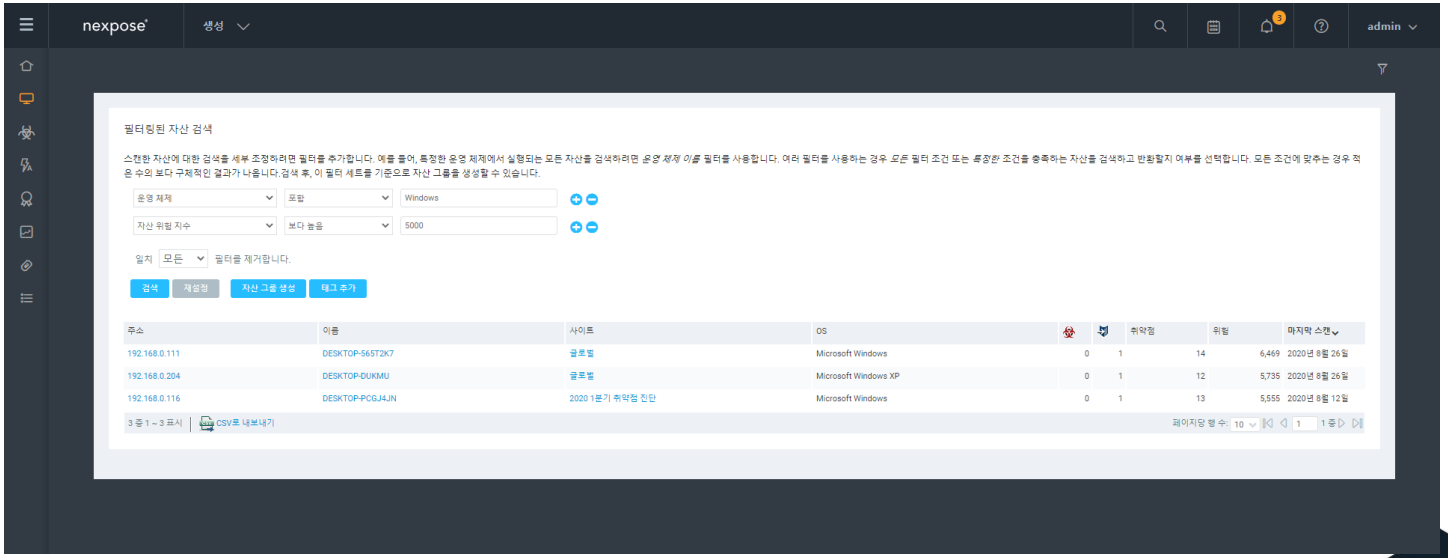
자산 정보의 분류 기능

- 새롭게 발견된 자산, 취약점 진단을 완료한 자산, OS 별 분포, 공격 기술 난이도에 따른 침해 가능한 자산의 분포를 한눈에 보여주는 자산 현황 대시보드



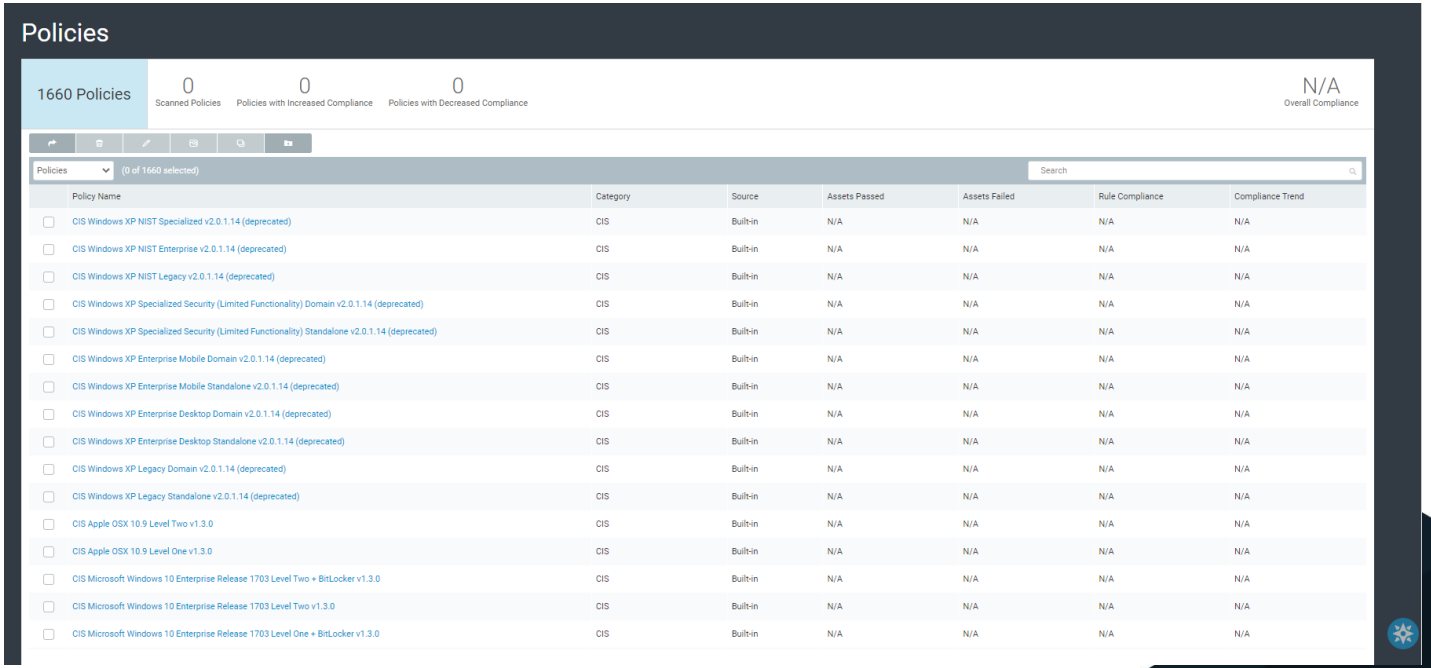
자산 정보의 분류 기능

➢ Site, Static asset group, Dynamic asset group 기능으로 지속적이고 효과적으로 자산을 분류



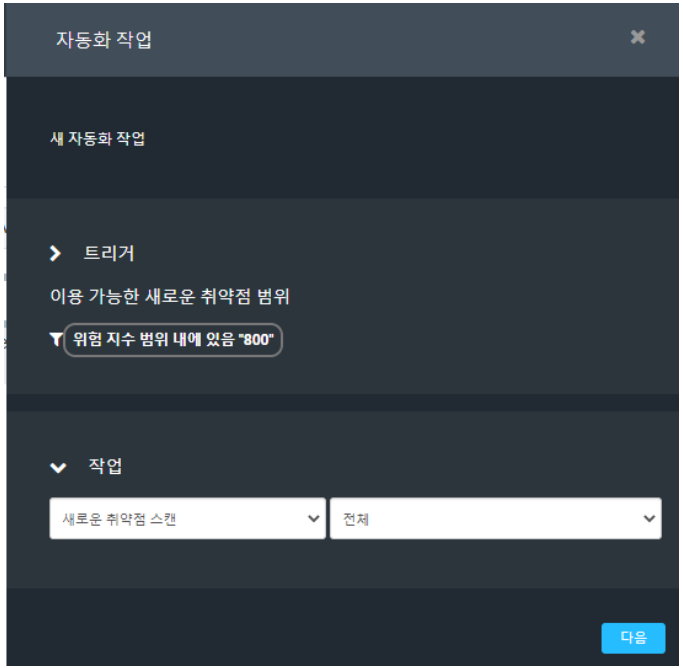
컴플라이언스를 위한 Policy 기능

- CIS, FDCC, USGCB, DISA 및 PCI, HIPAA, SOX, SCADA 등의 Compliance에 대응하는 Policy Scan과 결과를 리포트로 제공



적응형 진단 기능 – 자동화된 워크플로우

➢ 이벤트로 자동 시작되는 스캔



- ✓ 어떠한 설정 코드 생성 없이 맞춤형 이벤트 조건의 정의로 자동 진단 수행 설정
- ✓ 내부 업무 환경에 맞게 자산을 필터링 분류하여 정교하게 진단 행위를 정의
- ✓ 드롭다운 메뉴와 클릭선택으로 손쉬운 설정

보고서 기능 – 취약점 결과 정보 분류

➢ 취약점 결과정보를 분류하여 산출

- ✓ 호스트 필터: IP, SITE, STATIC GROUP, DYNAMIC GROUP 등
- ✓ 취약점 필터: 150 개의 카테고리 및 심각도에 따른 분류
- ✓ 취약점 세부정보: 리포트 대상에 따라 4가지의 분류 옵션

  예〉 위험 수준이 높은 웹 서버들로부터 발견된 심각도가 CRITICAL인 모든 웹 관련 취약점만 추출해서 리포트를 생성

보고서 기능 – 해결 조치 방법 제시

➢ 패치와 구성 변경에 대한 순서 및 단계별 조치를 제공

Set the password expiration
Estimated time: 30 minutes

Microsoft Windows 2000 Professional, Microsoft Windows XP Professional
If the account is not used, delete or disable the account. If the account is a built-in system account such as the IUSR_ or IWAM_ accounts, enable the "User cannot change password" option to stop this vulnerability from being reported (Microsoft best practices dictate that built-in system accounts NOT be allowed to change their own passwords). Otherwise, ensure that the password expires by disabling the "Password never expires" option.

1. Right click on "My Computer"
2. Select "Manage"
3. Open the "Local Users and Groups" folder
4. Open the "Users" folder
5. Double-click on the desired user
6. Uncheck "Password never expires"

한글화 지원 – UI, 보고서, 도움말, 매뉴얼

➢ 보고서, 매뉴얼, 도움말 , UI 한글 지원으로 취약점 점검 결과를 이해하기 쉬움

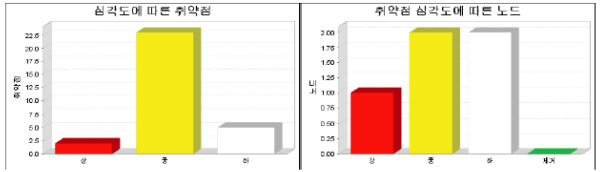
1. 개요

이 보고서는 Nexpose이 Rapid7 LLC에서 수행한 보안 감사에 대한 내용입니다. 이 보고서는 귀하의 네트워크 상태에 대한 기밀 정보를 포함합니다. 권한 없는 사용자가 이러한 정보에 액세스하는 경우, 네트워크 문제가 발생할 수 있습니다.

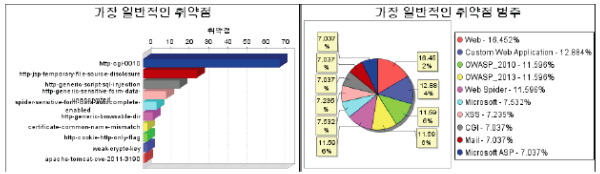
사이트 이름	시작 시간	종료 시간	전체 시간	상태
Web_Svr	February 14, 2014 21:35, PST	February 14, 2014 22:01, PST	25 분	성공

전체 자산 추세를 표시할 수 있는 충분한 이력 데이터가 없습니다.

2개의 시스템에 대한 감사가 수행되었으며 이 중 2개의 시스템이 액티브 상태이고 검색된 것으로 나타났습니다.



검색하는 동안 30개의 취약점이 발견되었습니다. 이 중, 심각도가 상인 취약점은 2개입니다. 심각도가 상인 취약점이 발견되면 즉시 조치를 취해야 합니다. 이러한 취약점은 해커에 의해 악용되기 쉬우며 영향을 받은 시스템이 조작될 수도 있습니다. 심각도가 중인 취약점은 23개입니다. 심각도가 중인 취약점의 경우 상대적으로 악용하기 쉽지 않고 해당 시스템에 액세스하기 어려울 수도 있습니다. 심각도가 하인 취약점이 5개 발견되었습니다. 하지만 차후에 귀하의 네트워크를 공격하는 데 이용될 수 있는 정보를 공격자에게 제공할 수 있습니다. 이러한 취약점은 다른 취약점만큼 시급하지 않지만 적시에 해결되어야 합니다.
심각도가 상인 취약점이 발견되었으며 보안 위험이 가장 높은 시스템은 1개입니다. 2개의 시스템에서 심각도가 중인 취약점이 발견되었습니다. 2개의 시스템에서 심각도가 하인 취약점이 발견되었습니다. 모든 시스템에서 취약점이 발견되었습니다.



http - cgi - 0010 취약점은 71번 발생한 가장 일반적인 취약점입니다. 취약점이 166개 발생한 Web 범주는 가장 일반적인 취약점 범주입니다.

위험별 25개의 주요 문제 해결 방법

3월 20, 2014 22:37:25 KST

개선조치 방안

적용	해결 예정	영향
25 주요 문제 해결	71% 취약점 포함: 55% 공개된 익스플로이트 96% 이용 가능한 멀웨어 키트	6 자산

문제 해결	해결된 취약				위험
Upgrade to the latest version of Oracle Java	143	18	46	1	70014
Upgrade to the latest version of PHP	152	32	0	1	64206
Upgrade to the latest version of Oracle MySQL	49	1	0	1	11688
MS14 - 015: Download and install Microsoft patch for KB2930275 windows6.1 - kb2930275 - x64.cab (1525463 bytes)	19	9	6	1	8703
Upgrade to the latest version of Apache HTTPD	31	5	0	2	8414
Upgrade to the latest version of Samba	9	12	0	1	5627
MS12 - 034: Microsoft 패치 windows6.1 - kb2676562 - x64.cab (6693057 bytes) 다운로드 및 설치	10	5	6	1	5218
MS12 - 034: Microsoft 패치 mpsyschk.exe (15264 bytes) 다운로드 및 설치	10	5	6	1	5218
Upgrade to the latest version of Mozilla Firefox	15	2	0	1	4703
Upgrade to the latest version of BIND	13	6	0	1	4553
Upgrade to the latest version of Apple QuickTime	12	3	0	1	4532
Upgrade VMware ESXi to the latest version	13	1	0	1	4083
MS11 - 020: Microsoft 패치 windowsxp - kb2508429 - x86 - enu.exe (664960 bytes) 다운로드 및 설치	4	6	0	1	3190
MS11 - 020: Microsoft 패치 windowsserver2003.windowsxp - kb2508429 - x64 - enu.exe (1044864 bytes) 다운로드 및 설치	4	6	0	1	3190
Configure SMB signing for Windows	4	0	0	2	3025

RAPID7

Contens

INSEC security

취약점 위험 관리의 기대효과

보안 취약점 관리

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

위협 대비

사용자 위험 관리

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

효율성 증가

모의침투 테스트

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

업무 생산성 증대

RAPID7 제품 포트폴리오

보안 관리

nexpose®

- ✓ 취약점, 보안 설정, 컨트롤에 대한 통합 리스크 관리
- ✓ 8만개 이상의 보안 취약점 점검
- ✓ 컴플라이언스 관리 간소화

침투 테스트

metasploit®

- ✓ 취약점 파악과 방어 확인을 위한 네트워크 공격 시뮬레이션
- ✓ 실제 취약점 검증이 가능한 공격 코드 (Exploit Code) 내장
- ✓ 피싱 노출 관리 및 테스트 사용자 인식

Nexpose/Metasploit 연동

➢ Metasploit과의 연동을 통해 확실한 취약점 점검 및 위험 검증을 기대할 수 있습니다.

위험 평가

nexpose®

취약점 관리와 구성 평가

metasploit®

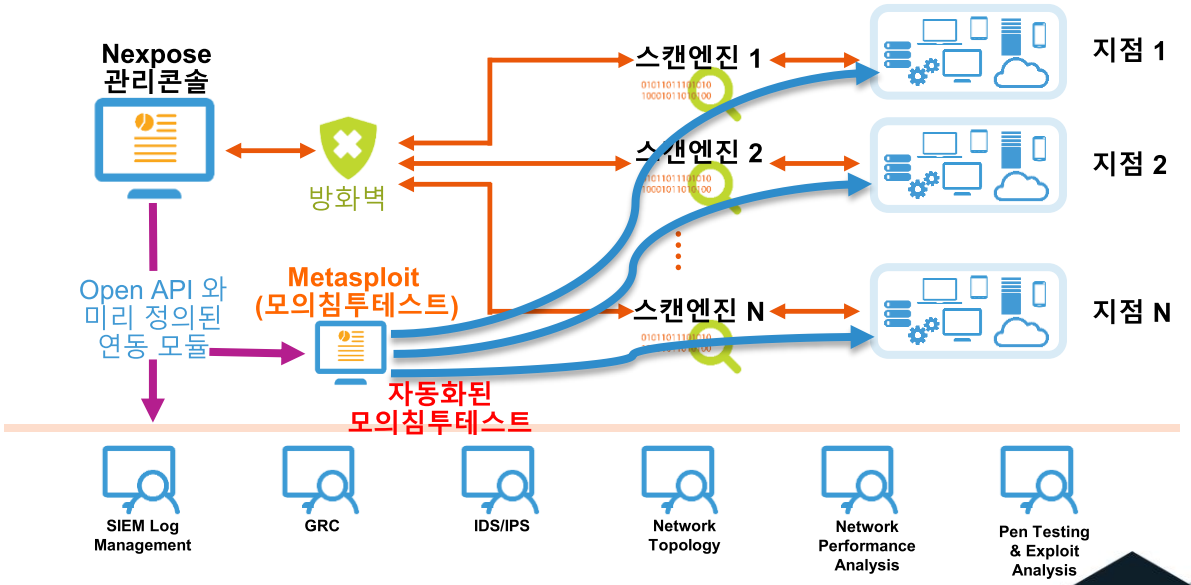
침투 테스트와 위험 검증

위험 확인

유연하게 확장 가능한 아키텍쳐

➢ 취약점 진단 관리 구성 아키텍쳐

- ✓ 다중 설치 옵션
- ✓ 에이전트 없는 스캔
- ✓ 스캔 엔진의 확장 설치
- ✓ OPENAPI™– 타제품과 연동



RAPID7

Contens

INSEC security

Rapid7 기술 파트너 에코시스템

	인증된 인테그레이션 파트너
SIEM & Log Mgmt	ArcSight, LogRhythm, 1Labs, nitrosecurity, solarwinds, splunk>, PRISM MICROSYSTEMS, Novell, DELL SecureWorks, RSA The Security Division of EMC
GRC	RSA The Security Division of EMC, brinqa, Agiliance, MODULO Solutions for GRC, R-sam
IDS/IPS	SOURCEfire
Network Topology	REDSEAL NETWORKS, skybox security, FIREMON
Virtualization	vmware
Pen Testing & Exploit Analysis	metasploit, EXPLOIT DATABASE, w3af
Other Solutions	nexpose open api

한국 고객

기업	IT 기업	금융	관공서	기타
HYUNDAI	SK planet	koscom	ncia 정부통합전산센터	olleh kt
HYUNDAI MOBIS	Smartro	금융감독원	대한민국 육군 Republic of Korea Army	kt ds
HYUNDAI DYMOS	SPC Network	금융결제원	대한민국공군 REPUBLIC OF KOREA AIR FORCE	IGLOOSECURITY
Hanwha	LG CNS	한국은행 THE BANK OF KOREA	기획재정부 MINISTRY OF STRATEGY AND FINANCE	AhnLab
HANJIN	Daum (주)다음커뮤니케이션	현대증권	한국감정원	ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute
CJ		우리투자증권	NIS 국가정보원	SAMSUNG 삼성서울병원
LG전자		하나SK카드	DAPA 방위사업청	
SAMSUNG 삼성전자		IBK 기업은행	관세청 KOREA CUSTOMS SERVICE	
		한화손해보험	국군기무사령부 Defense Security Command	

90개국 5,000여 고객

Technology/ Communication

Retail/ Wholesale

Energy

Education

Financial Services

Media & Entertainment

Healthcare

Public Sector Government

Manufacturing

Other

RAPID7

감사합니다.

INSEC security

본　　사 : 서울특별시 금천구 가산디지털1로 19 대륭테크노타운 18차 406호
Email : insec@insec.co.kr TEL : 02-863-5687 www.insec.co.kr