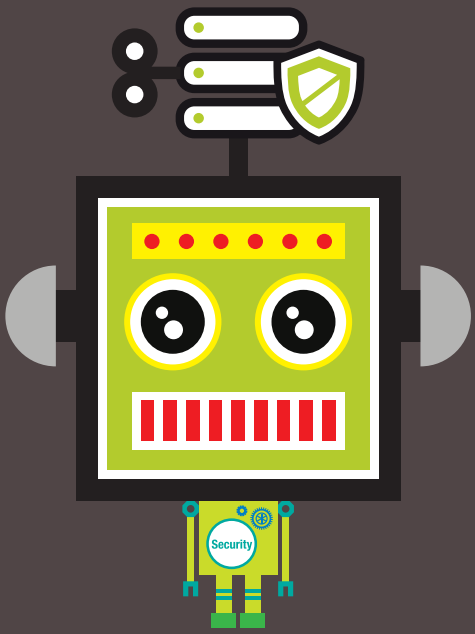


네트워크 침입 탐지/방지 시스템

IDS/IPS

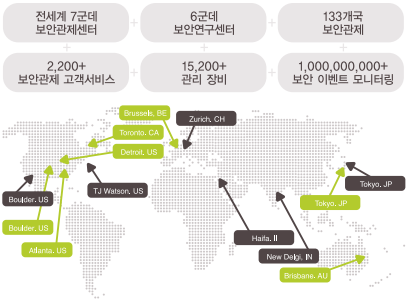
최근 일련의 보안 사고로 알 수 있듯이 보안 위협들은 날이 갈수록 지능화되어가고 있고, 기업의 보안 팀은 보안을 유지하면서도 성능을 저하시키지 않는 방안에 대해 고민이 깊어져 가고 있습니다.

기존의 네트워크 보안 환경, **이런 고민을 갖고 있지 않으십니까?**

- 사전방어, 애플리케이션 방어의 부재를 극복하기 위한 대책이 필요합니다.
- 새로운 취약점 공격의 출현 주기가 빨라짐에 따라 새로운 패치 적용 전 공격을 방어하기 위한 방법은 없을까요?
- 날로 지능화되고 발전해 가는 zero-day 공격, 스파이웨어, Bots, 트로얀, 웜, P2P, Instant Messenger, DoS 등의 공격에 대한 방어가 필요합니다.
- 보안 정책 및 이벤트 관리를 위한 전문성 및 보안 관리에 따른 부담 경감 방안이 없을까요?

IBM Security Network Intrusion Detection/Prevention System(IDS/IPS)
특징 및 장점

IBM 보안 연구소, 경쟁사와 비교되지 않는 보안 연구 인력, 신속한 공격 패턴 업데이트



업계 최고의 트래픽 분석 PAM (Protocol Analysis Module) 엔진 탑재

- PAM엔진은 업계 최다인 165개의 프로토콜 분석과 다양한 공격기법을 통해 정확한 공격 및 방어 능력 보유
- PAM엔진의 탐지 기술
  – 20가지의 다양한 탐지기법을 개별 또는 복합적으로 사용해 분석 및 탐지

취약점 분석 기반의 Signature

- 취약점 기반이란 해당 공격을 야기하는 프로토콜에 대한 취약점을 연구하여 Signature를 제작함으로 변종/신종 공격 탐지에 용이한 시그너쳐
- IBM의 Security Network IPS는 IBM X-FORCE 보안 연구소에 의해 검증된 취약점 기반의 Signature를 사용
- 일반적인 공격코드(패턴 매칭) 기반의 Signature는 공격 코드를 분석하여 공격 트래픽의 특정 String을 탐지하도록 Signature를 제작함으로 해당 string 변경 시 쉽게 우회 가능
- 탐지된 보안 이벤트에 대한 상세한 파라미터 제공

	약점 (Vulnerability)기반 Signature	공격코드 (Exploit code) 기반 Signature
지원 벤더	ISS Proventia Network IPS	타 벤더
알려지지 않은 웜, 변종 웜, 공격 코드 등	탐지/차단 가능 (Zero-day Prevention)	탐지/차단 불가
회피 가능성 (변종 공격 포함)	우회하기 어려움.	우회하기 쉬움
개발 용이성	어려움. (특별한 기술과 축적된 노하우 요구)	쉬움. (공개된 공격코드에 대한 구현으로 개발 용이)
정확성/정밀도	공격코드에 의존하지 않고 해당 취약점을 탐지, 차단 하므로 적용 범위가 넓고, 변형 공격도 탐지/차단 가능	특정 공격코드에 제한적 이므로 변종공격으로 쉽게 우회 가능
Signature 소스	전담 취약점 연구조직 (150여 명) 인 X-FORCE를 통해 취약점 연구	공개된 소스 (주로 공개된 공격코드 기반)

VoIP 방어

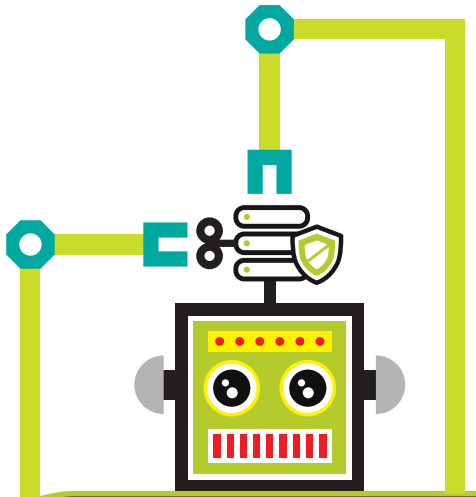
- PAM 엔진에서 SIP, MGCP, H.323, SCCP, H.225, H.245, Q.931, T.120 and STUN 프로토콜에 대한 완벽한 파싱 지원
- 애플리케이션 레벨의 프로토콜을 포함하여 프로토콜 인식을 위한 트래픽의 패킷 레벨 분석
- 알려진 공격, 알려진 취약점에 대한 unknown 공격, 비정상적인 사용 등을 인식하기 위해 패킷 내의 데이터를 분석
- VoIP환경(IP, H.323, SIP, SCCP)에서의 DoS공격 차단
- ICSA로 부터 보안업계 최초로 VoIP 성능에 대해 ICSA 인증 획득(3rd Party Validation)
- Cisco Call Manager, SpyPe, Netmeeting과 같이 널리 사용되는 VoIP 제품의 취약점에 대한 방어 또한 제공

IDS/IPS **인증 및 수상**

- **국제공통평가(CC)인증**
  Proventia Network IPS 제품 – EAL 2 인증
- **기타 인증 및 수상**

IDS/IPS **고객 사례**

국내 주요 인터넷 포털 회사, 국내 주요 은행, 증권, 대학 등 약 50개 이상

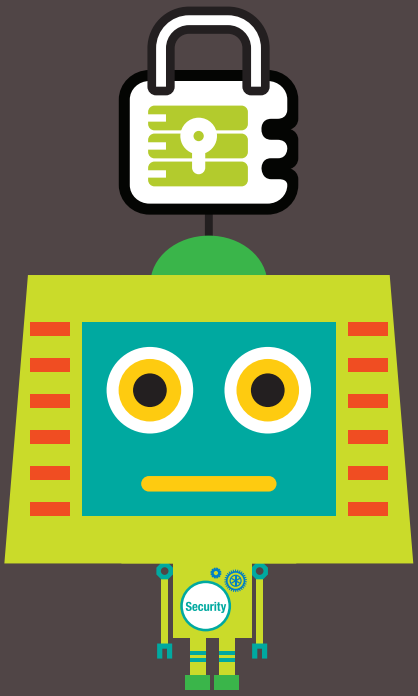


지금 시작하십시오

중소 중견 기업을 위한 IPS/IDS 특가 프로모션이 진행 중에 있습니다.

IPS/IDS 관련 추가 자료를 받아보세요!

IBM 박범중 과장
bjpark@kr.ibm.com ＼ 02-3781-8318 ＼ 010-4995-8318



데이터 보안

IBM InfoSphere Guardium

실시간 DB 접근 제어와 컴플라이언스가 단순해집니다

데이터 침해와 유실의 75% 이상이 DB서버로부터 발생하고 있다는 사실을 알고 계셨습니까?

포레스터 리서치에 의하면, Guardium은 해외 TOP 500대 기업 고객에게 239%의 ROI와 5.9개월의 손익분기점을 제공, 업계에서 압도적 우월성을 차지하는 NO.1 솔루션으로 평가되고 있습니다. DBMS의 종류에 상관없이 적용 가능한 Guardium으로 귀사의 전사 데이터베이스 보안 및 컴플라이언스, 라이프사이클을 관리하십시오.

컴플라이언스는 기업의 지속가능성과 경쟁력을 좌우하는 **중요한 팩터로 자리매김하고 있습니다**

- 시스템 관리에 대한 서비스 목표수준(SLA) 기대치가 높아짐에 따라 IT 부서는 복구 시간 목표 및 복구 지점 목표에 부응하기 위해 애쓰고 있습니다.
- 허가되지 않은 재무 데이터 변경과 특정 권한을 보유한 유저에 대한 실시간 감시가 어렵습니다.
- 보안영역은 너무 전문적이어서 DBA나 엔지니어를 제외하고는 일반 보안부서를 규명하여 보안정책을 세워 쉽게 관리하기가 어렵습니다.
- SQL injection등 다양한 해킹수법의 발전으로 이를 대비하기가 어렵습니다.
- DB패치와 취약성 찾아내기가 어렵습니다.
- 애플리케이션 사기 방지에 대한 대책이 없습니다.
- 컴플라이언스 준수를 위해 과도한 시간과 비용이 들어갈 뿐만 아니라 이를 통과하기가 어렵습니다.

IBM InfoSphere Guardium **특징 및 장점**

Local Access 감시	• DB에 설치된 S-Tap은 성능에 지장 없이, 애플리케이션과 DB 변경 없이, 실시간으로 그리고 지속적으로 DB에 있는 모든 활동을 철저히 감시
이기종 플랫폼지원	• 다양한 DBMS플랫폼 지원
운용비용절감	• 컴플라이언스 감시프로세스와 리포트 자동화 (6개월 이내로 투자액 회수).
확장성	• Central Policy Manager(CPM)을 통하여 여러 tier의 아키텍처를 한곳에서 통제가 가능하도록 정책 수립
직무 분리	• 감사 정보는 별도의 어플라이언스(collector)에 저장, 내부자나 해커가 로그 정보를 임의로 변경 불가 • DBA들에 의해 쉽게 변형될 수 있는 DBMS상의 native 로그에 의존적이지 않기에 철저한 직무분리 가능

지금 시작하십시오

IBM과 함께 데이터 관리 진단 워크샵을 수행하십시오

전문 ROI 분석 솔루션인 Alinean ROI Analyst 분석 툴을 사용하여 데이터 관리를 통해 얻어지는 기업의 비용 절감과 추가적인 매출 창출에 대한 비즈니스 이윤을 정량화 도출하는 워크샵으로서 이 워크샵을 통하여 귀사의 데이터 보안 관리 현황과 대응전략을 제시, 그리고 5년간의 ROI를 분석하여 드립니다.

IBM의 엔드-투-엔드 보안 포토폴리오를 확인하십시오

http://www.ibmsecurity.co.kr

IBM InfoSphere Guardium **고객 사례**

1 Washington Metropolitan Area Transit Authority (Metro)
- 대용량 DB내 DBMS 자체 로깅 및 감사 기능을 사용하지 않음으로 DB 성능 개선
- DBA 및 보안담당자 등에 대한 직무 분리
- 비인가된 내부사용자 모니터링

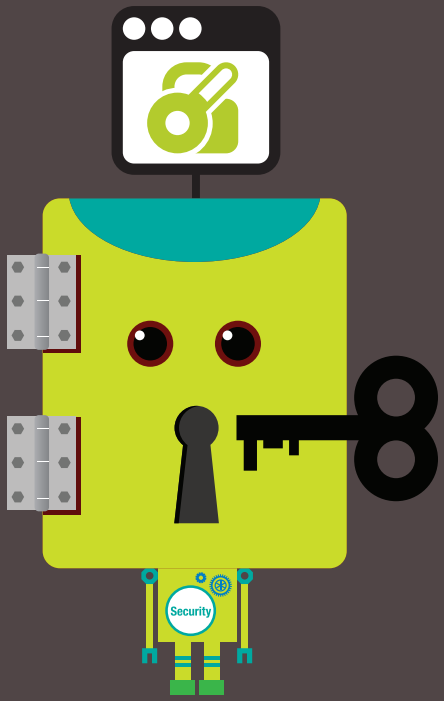
2 McAfee.com
- 카드정보 등 민감한 주요 데이터에 대한 실시간 가시성 제공
- PCI-DSS 컴플라이언스 충족
- DBMS 자체 로깅에 의한 서버 부하 제거

3 Dell
- 실시간 경고 및 중앙집중식 모니터링
- 자동화된 컴플라이언스 리포팅 기능
- 감사 오버헤드 절감을 통한 DB 성능 개선
- 티켓팅 시스템 Remedy와의 연계를 통한 데이터 관리 통제 강화
- 다양한 DBMS에 대한 통제 지원

4 유럽 소재 텔레커뮤니케이션 사업자
(이용자수:7천만명, 매출:연 300백억불)
- 12개 데이터 센터에 대해 2주 내에 보안 통제 시스템 구축 완료
- 중앙집중식 감사 시스템 완료 및 모니터링
- 주요 대외 감사 지원

5 NYSE에 상장된 무역 회사 (7천5백만 고객 보유)
- 하루 1백만 세션 감사 (GRANTS, DDLs, etc.)
- DBA의 데이터베이스 엑세스 감사
- 일단위 SOX감사 리포트 자동생성
- Ticketing 시스템과 연계한 자동화된 데이터베이스 변경관리

6 포춘 500대 기업에 드는 식품 제조사 (매출:연 150억불)
- 6개월 이내 239% ROI 도출
- 주요 테이블에 대한 실시간 알람 기능을 통한 적극적인 보안 대책 강화
- 4가지 대내외 컴플라이언스 준수
- 데이터 보안에 대한 전략 수립



웹 애플리케이션 보안

IBM AppScan

민감한 개인 정보를 주로 다루고 있는 금융 회사, 게임 업체, 인터넷 쇼핑몰 및 학교 등에서 해킹을 통한 정보 유출로 큰 피해를 보는 사례가 끊이지 않고 있습니다.

개인 정보 유출로 인한 손해는 단순히 금전적으로 수치화 할 수 있는 것이 아니며 매출 감소는 물론, 신용 손상, 법적인 책임 및 배상, 고객의 신뢰 상실로 이어져 기업의 위기를 초래할 수 있습니다. 사고가 발생한 후 해결하려고 하면 이미 늦습니다.

이제는 사전 예방을 위한 조치가 필요한 때입니다. IBM AppScan으로 귀사뿐만 아니라 협력/관계사의 보안 취약성을 점검하시고 미리 대비하십시오.

날로 높아져가는 보안 요구사항에 **어떻게 대응하고 계십니까?**

- ☑ 금전적인 이득을 목적으로 민감한 개인 정보가 유출되는 사례가 끊이지 않고 있습니다.
- ☑ 웹 애플리케이션의 취약점이 해커들의 공격 루트로 이용되는 사례가 늘어나고 있습니다.
- ☑ 준수하여야 하는 사내 보안 규정이나 정부의 보안관련 규제도 점차 많아지고 있습니다.

IBM AppScan **특징 및 장점**

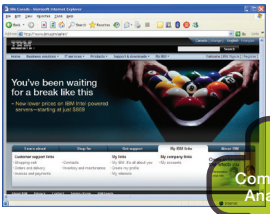
1. 웹 애플리케이션에 해커들이 시도할만한 불법적인 시도를 simulation하여 보안상 취약점을 발견하고 해결 방법에 대한 권고 사항 제공

2. 웹 취약점 감사 및 점검도구의 활용과 보안성 확보를 통하여 신뢰성과 안정성을 구비한 웹사이트 구축과 취약점 및 보안 감리 체계를 손쉽게 구축 가능

3. 취약점 점검과 대응으로 감리 및 보안검토에 투여되는 인력 및 시간비용에 대한 획기적 비용 절감

4. 개발 공정 전체에 걸친 애플리케이션 보안 검증

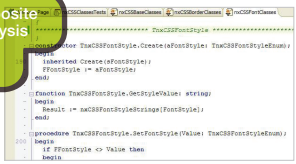
5. 동적 분석 도구와 정적 분석 도구로 발견된 취약성들을 서로 연관시킨 문제 분석으로 보다 정확한 탐지 가능



Composite Analysis

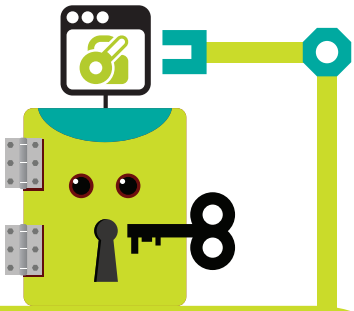
정적 분석 – 화이트박스

소스코드를 살펴서 보안이슈를 찾음



동적 분석 – 블랙박스

동작하는 애플리케이션에 대한 보안 분석



지금 시작하십시오

자세한 내용을 웹사이트를 통해 알아보세요!

http://www-01.ibm.com/software/kr/rational/products/help_ensure_n_web_secu_n_compliance.html

아무 부담없이 무료 상담을 신청하세요!

IBM 정재락 대표

jrjeong@kr.ibm.com ＼ 02-3781-8728