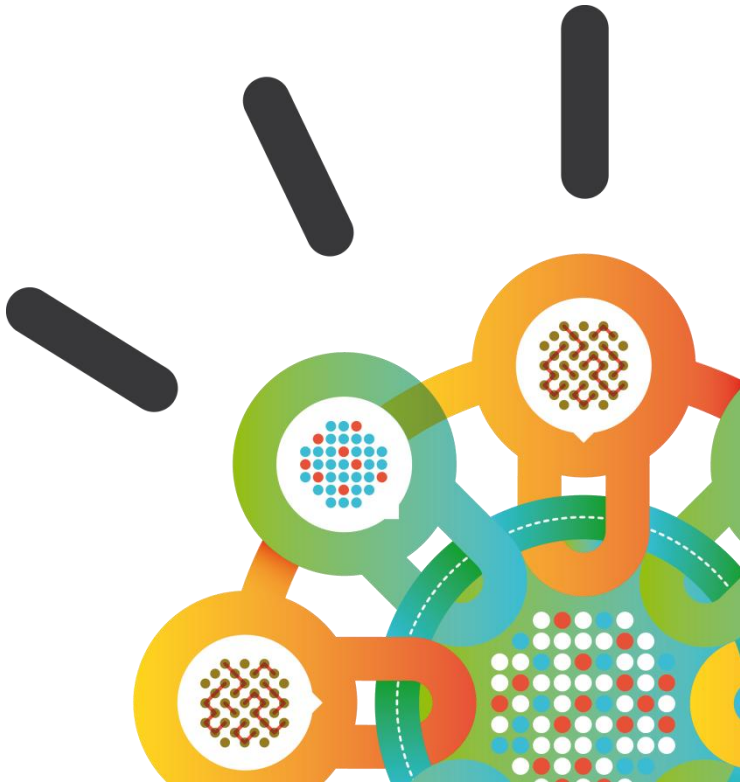
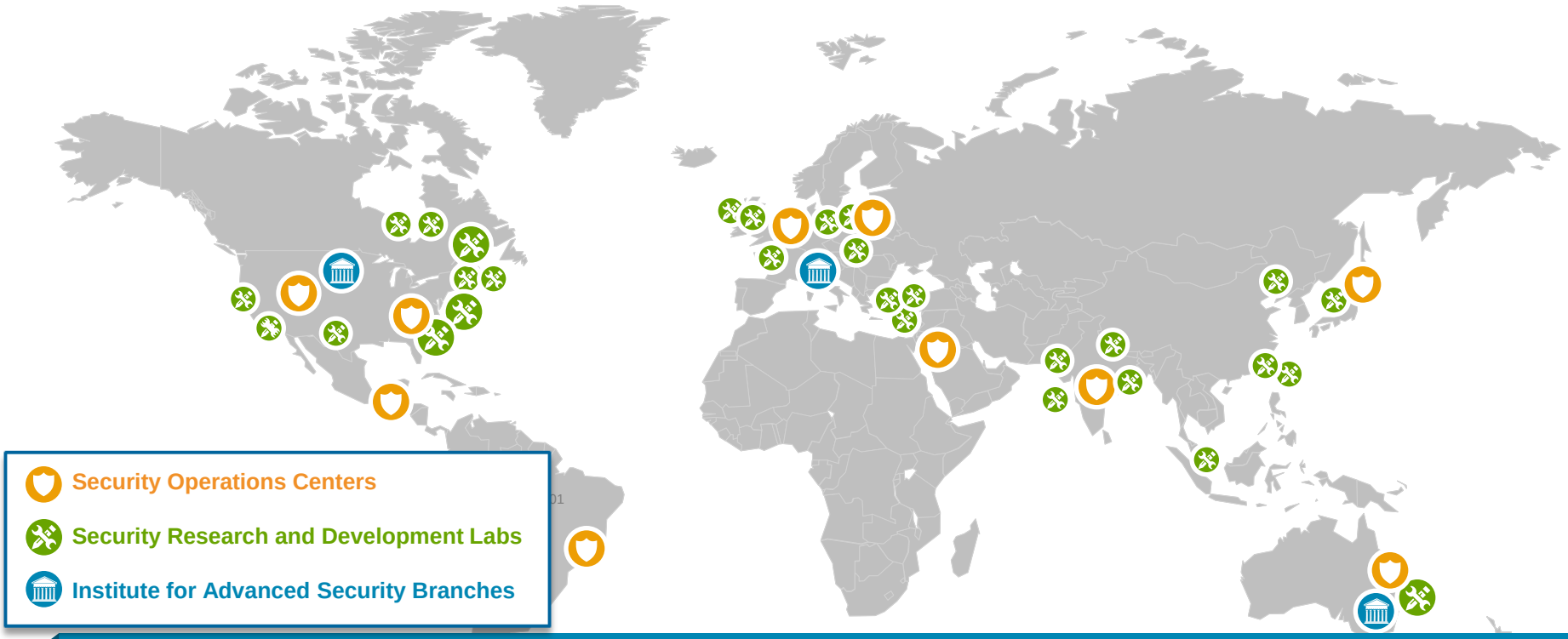
Security Intelligence.
Think Integrated.

2014년 최신 보안 동향 분석 및 보안 인텔리전스 대응 방안



성명/직급	박 형근 전문위원	소속	한국 IBM
수상	▪ 1997 국군기무사령부 사령관 표창 수상(제111호) - 국군기무사령부 전산 보안 체계의 취약점 발굴 보고	이메일	phk@kr.ibm.com
주요 경력	• 고려대학교 화학공학과 학사 졸업(93학번, 2000년 졸업) • 2000년 – 현재 한국IBM 재직 • 現 한국IBM IBM Security 보안팀 기술 리더 및 한국 IBM X-Force 연구소 한국 대변인 • 現 서울사이버대학교 정보통신학부 외래교수 • 現 미래창조과학부 미래전략 IT 자문 위원 • 現 국제 OWASP 한국챕터 고문 • 現 정보보안 전문 커뮤니티 시큐리티플러스 대표 운영자 • CISSP, CISA, CGEIT 국제 자격증 보유 • 現 ISC2, ISACA, 국제보안포럼, OpenGroup 정회원	저서	• 2010 OASIS 웹 서비스 품질 요소 표준 중 웹 서비스 보안 품질 분야 표준 저술 (OASIS) • 2010 '경영자, 보안 담당자, 개발자, 감사자가 반드시 알아야 하는 정보 보안 취약점과 지침' 기획, 감수 및 출간 (시큐리티플러스) • 2011 개인정보보호 실천 가이드 (인포더, 공저) • 2012 퍼블릭 클라우드 컴퓨팅 사용 기업이 고려해야 할 보안 위험과 대응 방안에 대한 小考 (정보호호학회 2012.11 제22권 제7호)
		강의	• 국가정보보안교육원 정보보안 과정 출강 - APT 사고 사례 및 대응 방안 • CIOCISO매거진 2012 CISO 전략 과정 출강 - 정보보호 프레임워크와 아키텍처 - 정보보호 성과 관리 • IBM교육센터 보안 과정 다수 출강 - IBM 보안프레임워크와 아키텍처 • 서울사이버대학교 해킹과 보안 과정 출강
		SNS	• 트위터: http://twitter.com/#!/securityinsight • 페이스북: http://www.facebook.com/hyungkeun.park • Linkedin: http://kr.linkedin.com/pub/hyung-keun-park/1/890/113

IBM 보안 역량



6,000+ IBM researchers, developers, and subject matter experts focused on security

3,000+ IBM security patents

전 세계 **IBM** 보안 시장 점유율

2012 Enterprise Security Market Share	
1	Cisco
2	Symantec
3	**IBM**
4	Check Point Software
5	McAfee (Intel)
6	EMC
7	Trend Micro
8	Microsoft
9	HP
10	Juniper Networks

Source: IDC Worldwide IT Security Products 2013-2017 Forecast and 2012 Vendor Shares, December 2013, IDC #245102

공격의 최적화와 전략적 대상 선정

5억건 이상, 2013년도 개인정보 유출 사고!!!

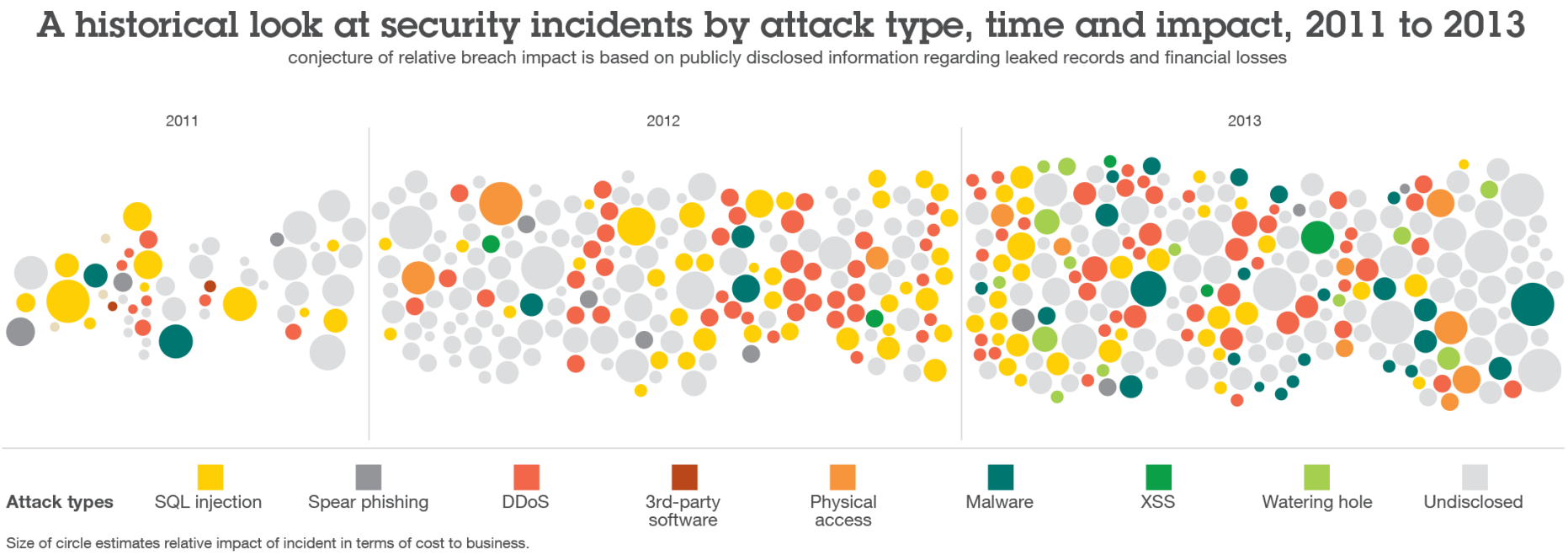
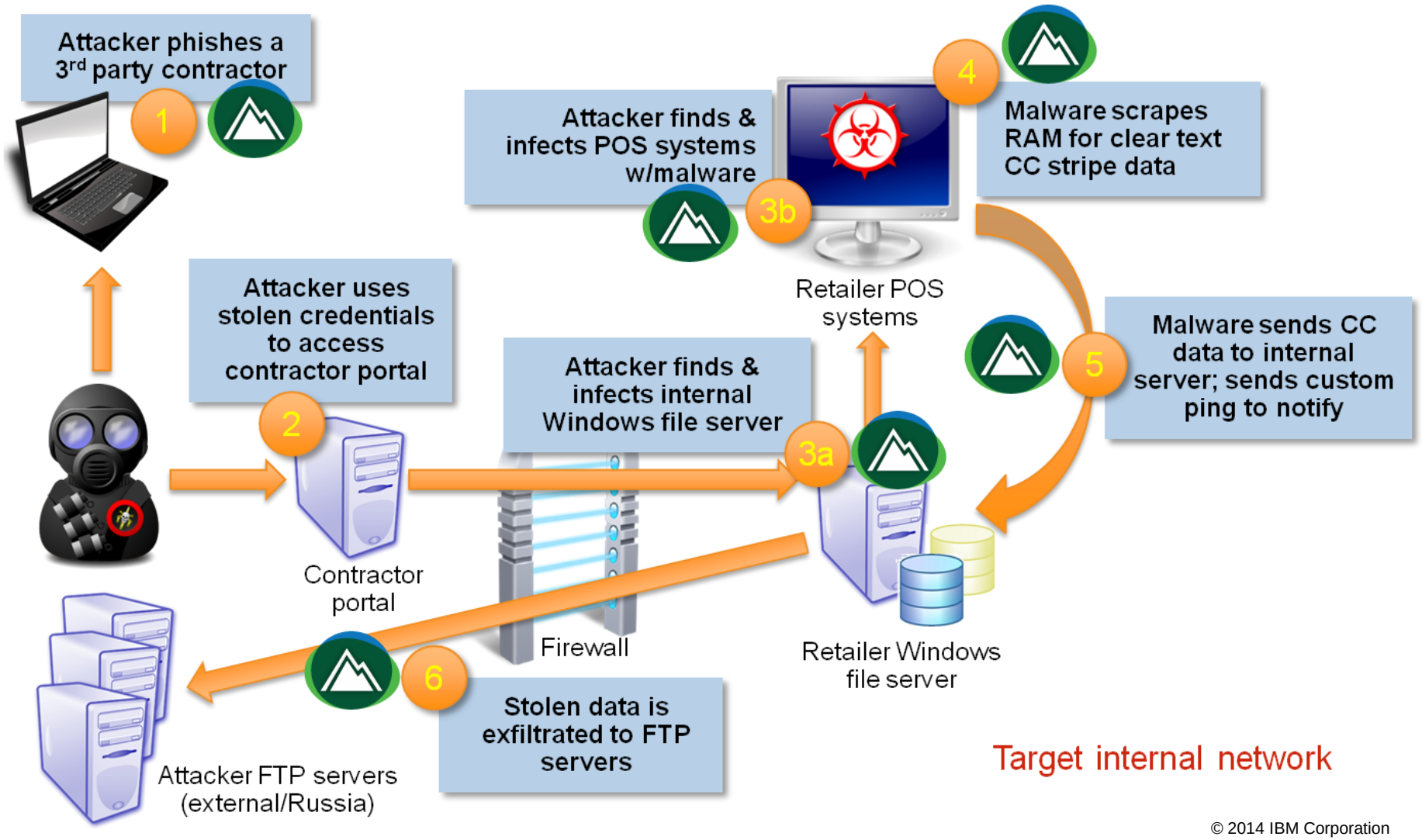


Figure 1. A historical look at security incidents by attack type, time and impact, 2011 to 2013

Source: IBM X-Force® Research and Development

Target Data Breach Case Study

Anatomy of the Target Retailer Breach



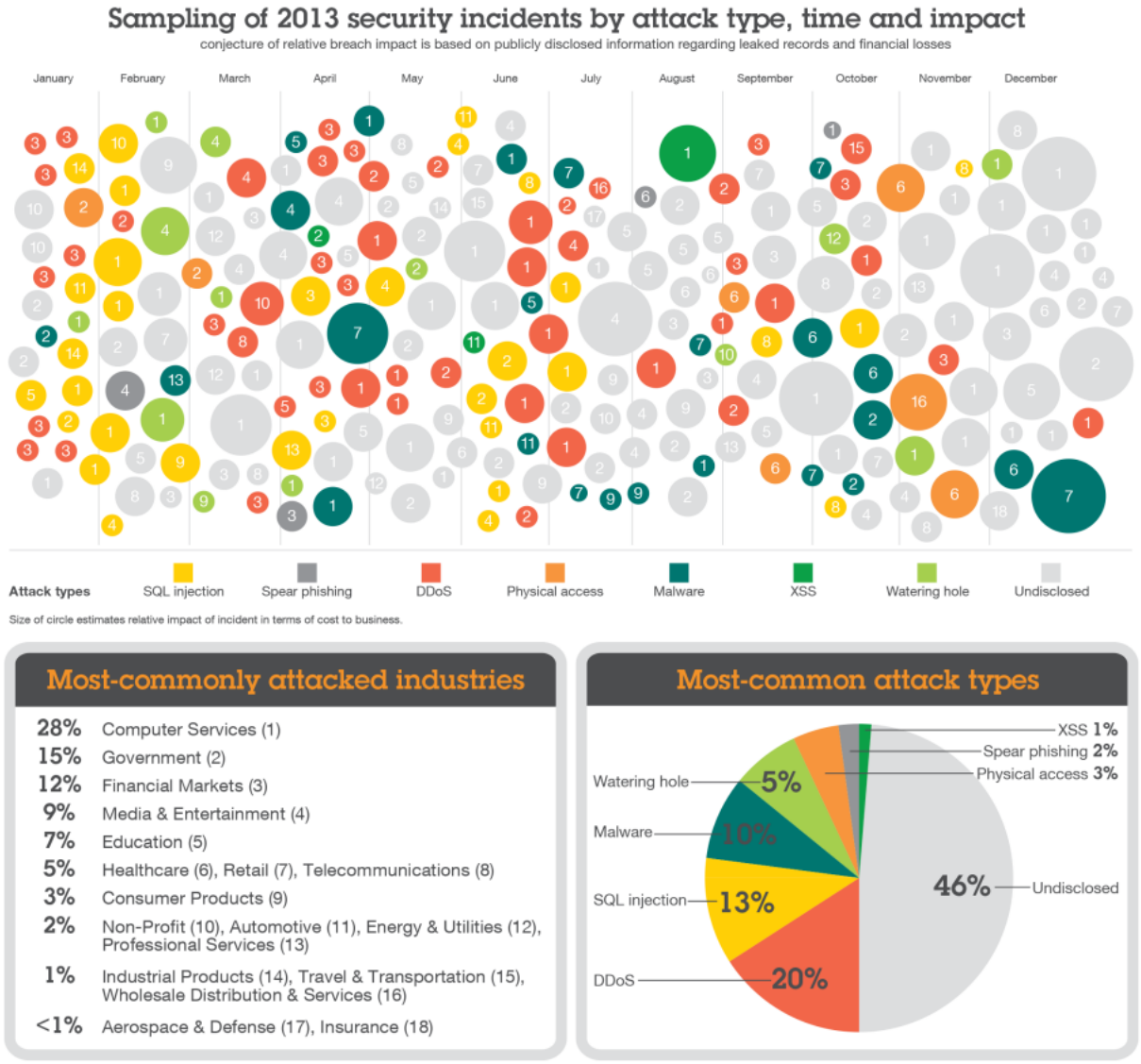


Figure 2a. Sampling of 2013 security incidents by attack type, time and impact

Source: IBM X-Force® Research and Development

자바 취약점 증가

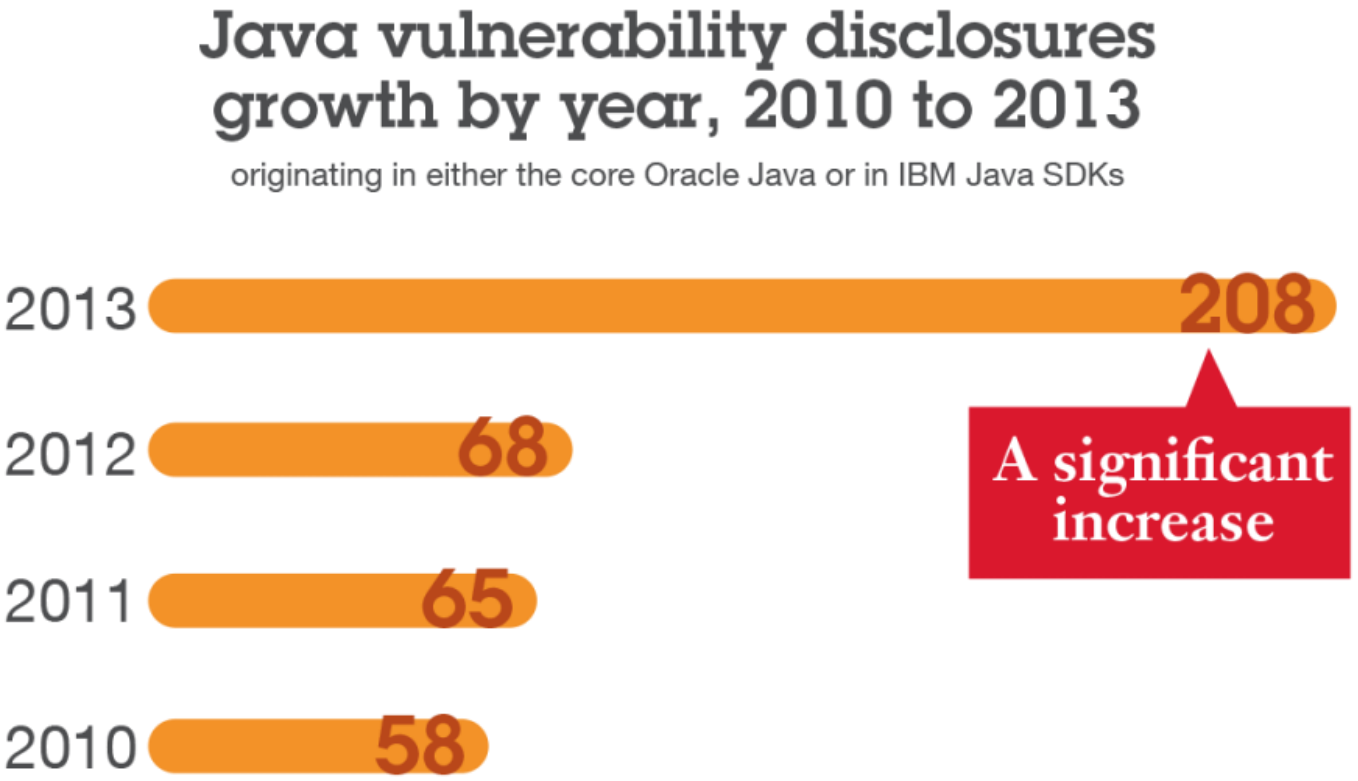


Figure 5. Java vulnerability disclosures growth by year, 2010 to 2013

Source: IBM X-Force® Research and Development

공격에 활용되는 대표적인 사용자 어플리케이션

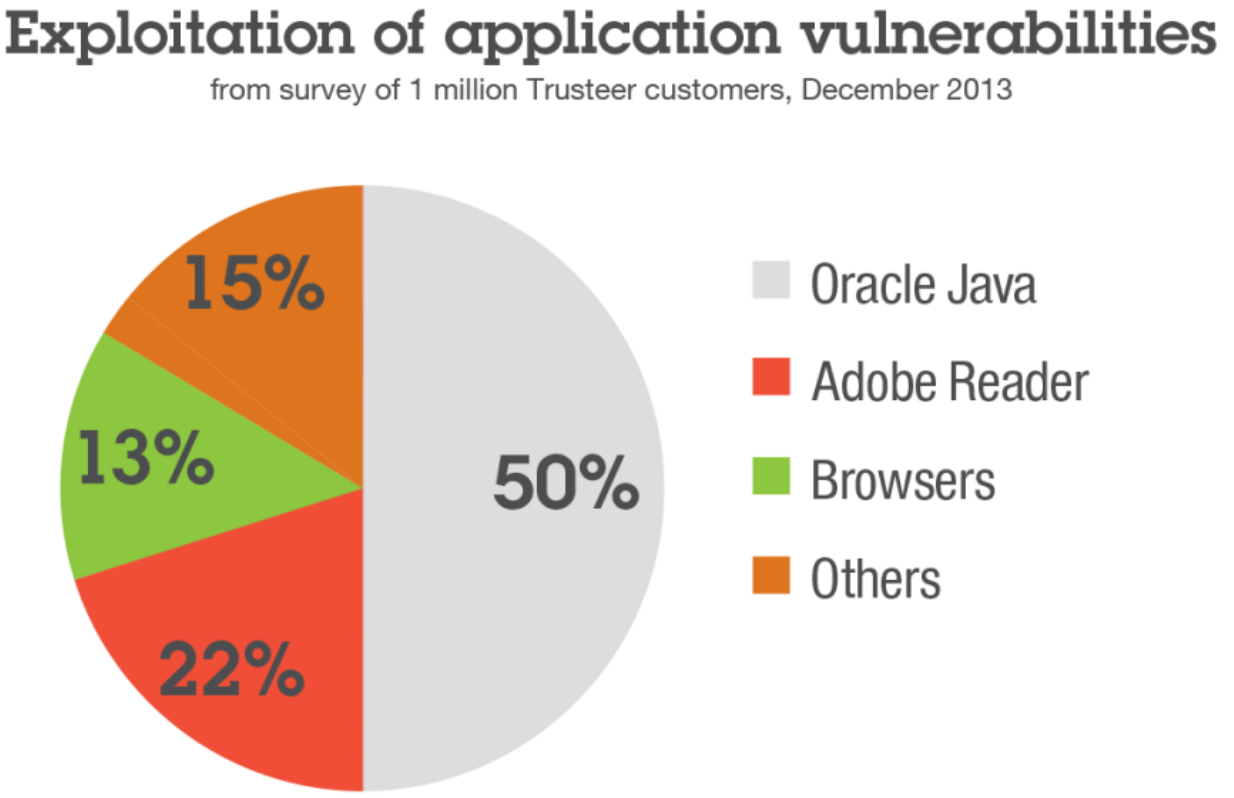
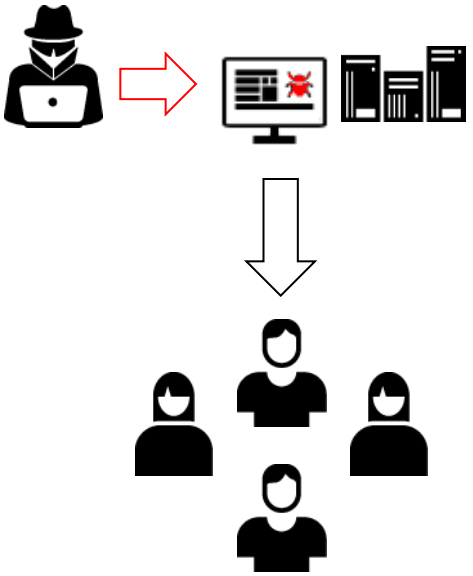


Figure 4. Exploitation of application vulnerabilities

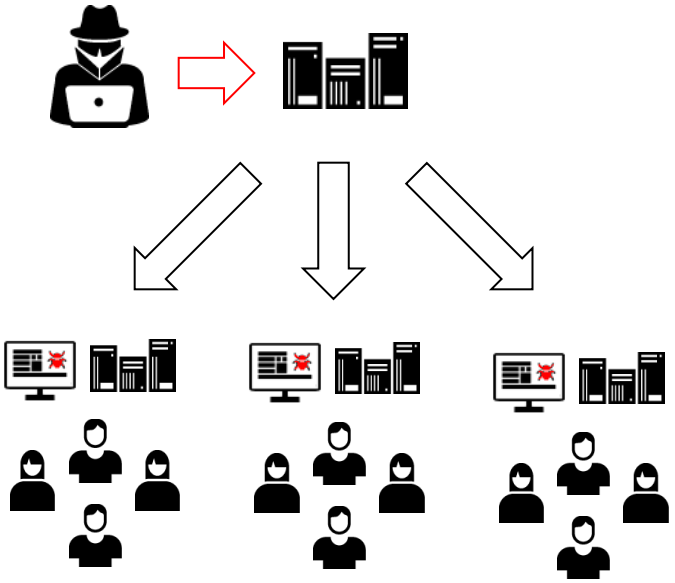
Source: IBM X-Force® Research and Development

효과적인 사용자 공격



Watering Hole

- 특정 관심사와 관련된 웹 사이트 상에 악성코드 삽입
- 취약한 중요 사람들을 공격



Malvertising

- 온라인 광고 네트워크 상에 악성코드 삽입
- 합법적인 웹 사이트 상에 악의적인 광고 서비스
- 취약한 사용자 공격

웹 취약점: 압도적인 위협

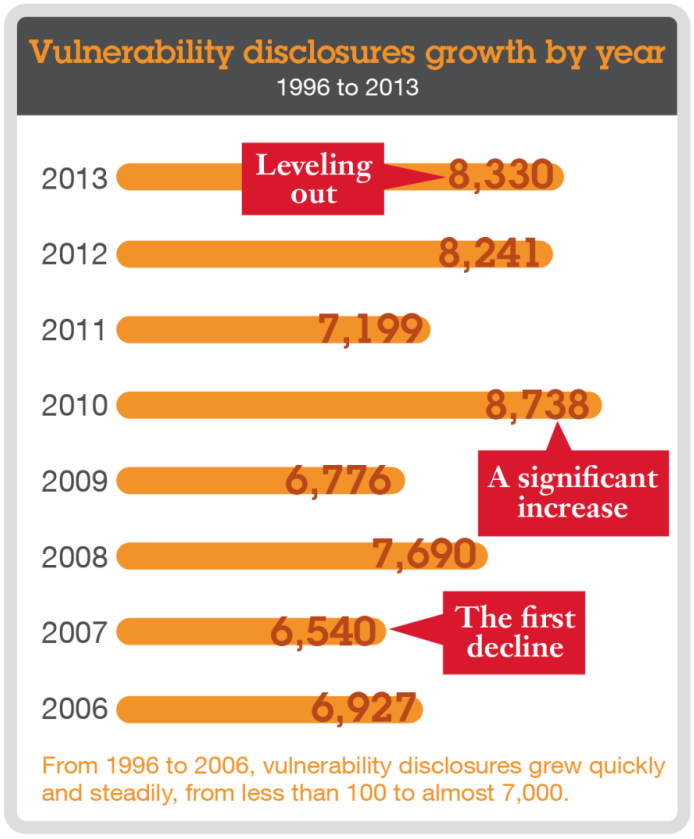


Figure 8. Vulnerability disclosures growth by year, 1996 to 2013

Source: IBM X-Force® Research and Development

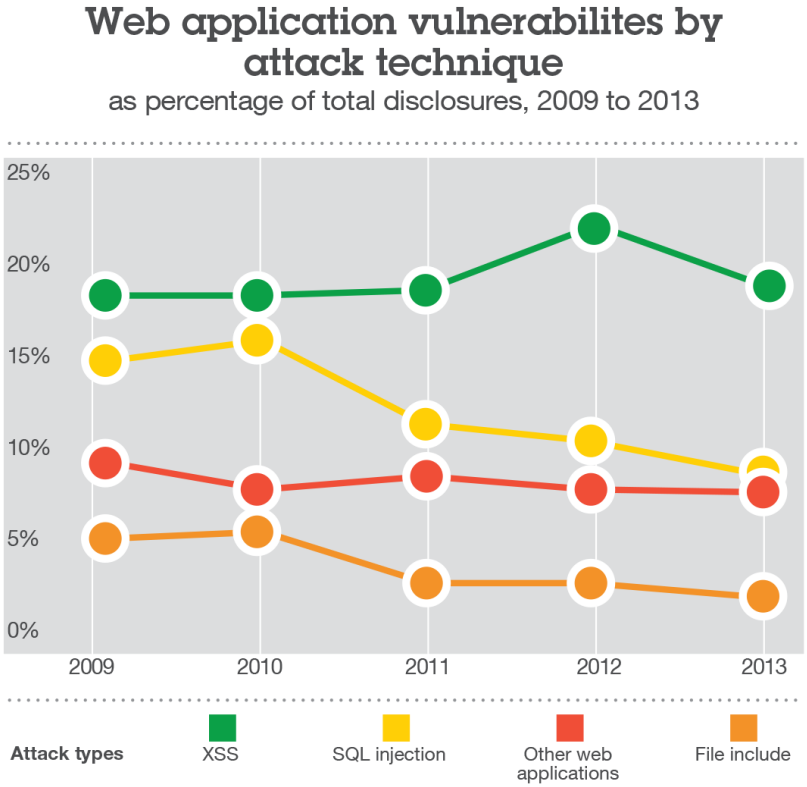


Figure 11. Web application vulnerabilities by attack technique, 2009 to 2013

Source: IBM X-Force® Research and Development

주요 소프트웨어 공급사의 패치 주기 향상

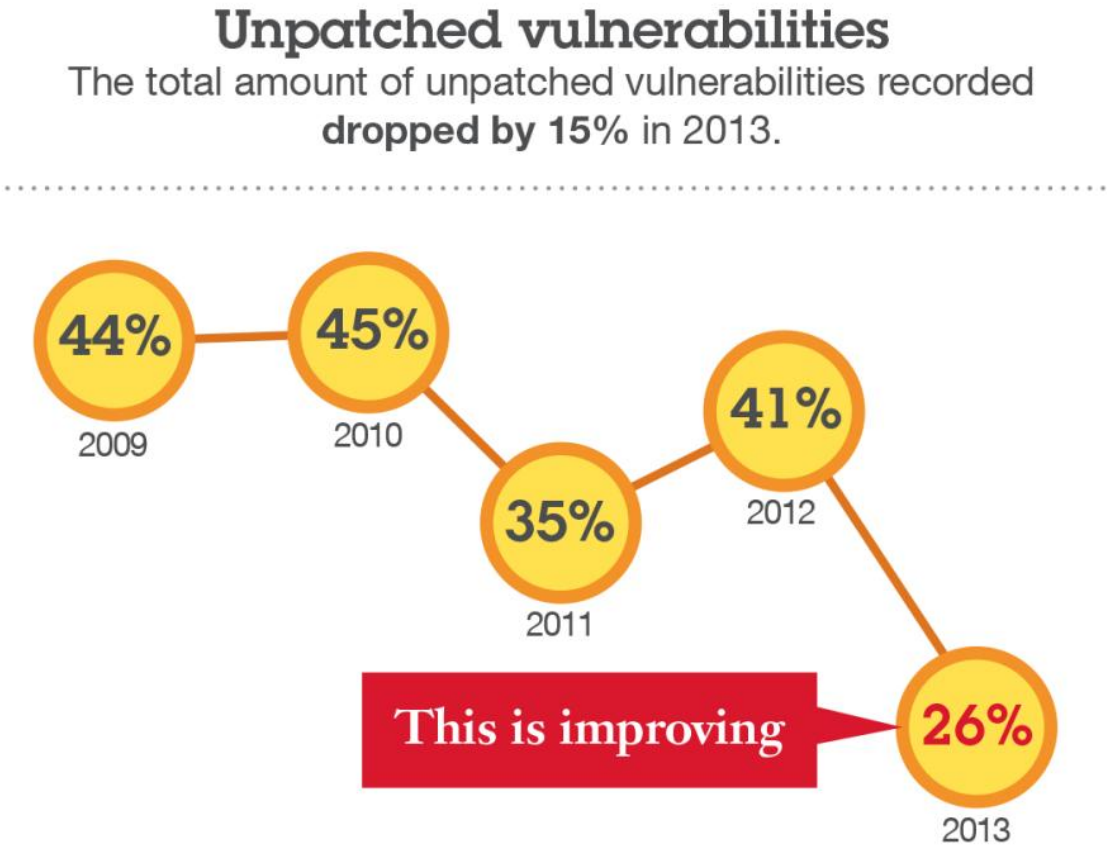
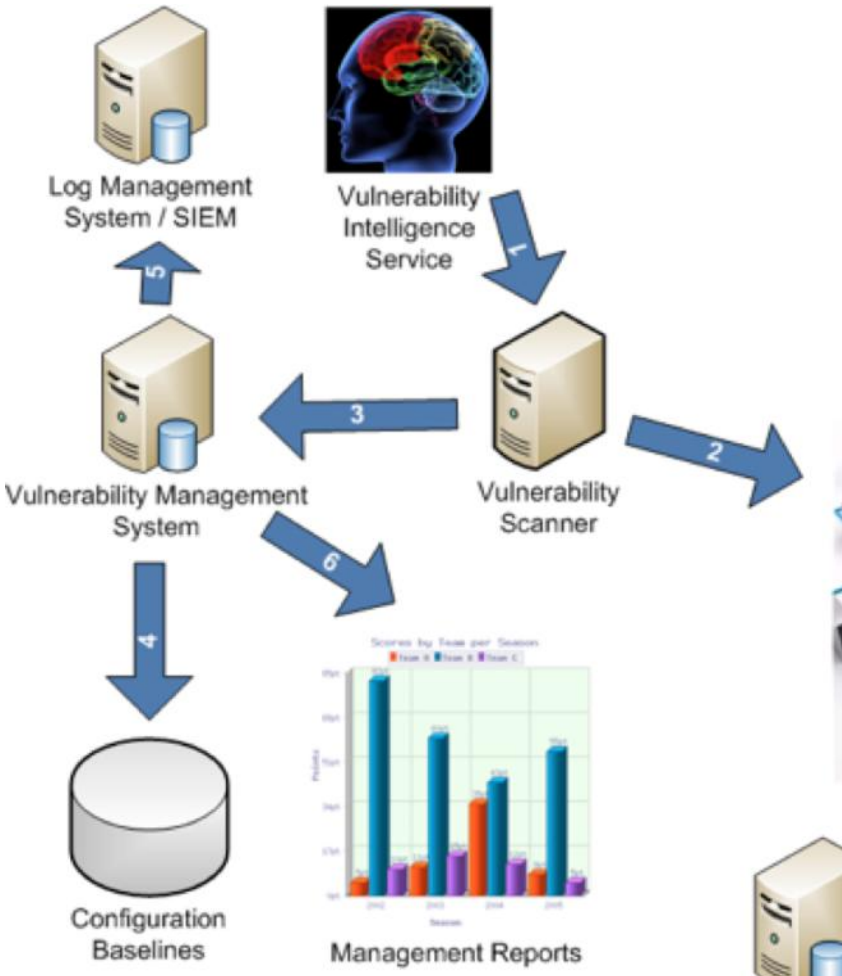


Figure 10. Vendor patch rates of publicly disclosed vulnerabilities, 2009 to 2013

Source: IBM X-Force® Research and Development

OpenSSL HeartBleed Vulnerability?!!!!!



Manage Vulnerabilities > **By Asset** > By Vulnerability Instances

Display: Instar

Search Parameter(s)
Asset With AssetId Equals (Clear Filter)

IP Address	Asset Name	Vulnerability
.	q1hurvm...	Portmapper - Potential Problem Typically Unused Service
.	q1hurvm...	2010-4478 - OpenSSH - Security-bypass Issue
.	q1hurvm...	2014-1692 - OpenSSH - Memory Corruption Issue
.	q1hurvm...	SSL - Self-Signed Certificate
.	q1hurvm...	2014-0160 - OpenSSL - Private Key Theft - Heartbleed Overrun
.	q1hurvm...	SSL- Anonymous Ciphers Supported Issue
.	q1hurvm...	2010-5107 - OpenBSD - OpenSSH - Denial of Service Issue
.	q1hurvm...	2012-0814 - OpenSSH - Information Disclosure Issue
.	q1hurvm...	2011-5000 - OpenSSH - Denial-Of-Service Issue
.	q1hurvm...	2011-4327 - OpenSSH - Information Disclosure Issue
.	q1hurvm...	Trace Route Information
.	q1hurvm...	Web Service is Running

IBM Security Network IPS

OpenSSL HeartBleed
취약점에 대한 공격 탐지 및 대응(차단)

공격자

총 1,151,673건

웹 보안, 또다른 생각!!!

AppScan 통한
보안 분석

사이트 진단

웹 사이트

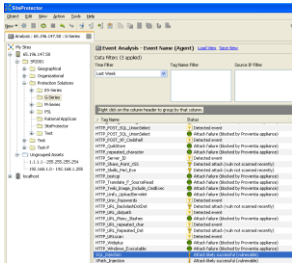
IPS로
취약점 정보 전달

진단된 웹 취약점에 대한
공격 탐지 및 대응(차단)

패치 위해
개발자에게
전달

IPS 패턴 정보
자체 업데이트

IBM Security Network IPS

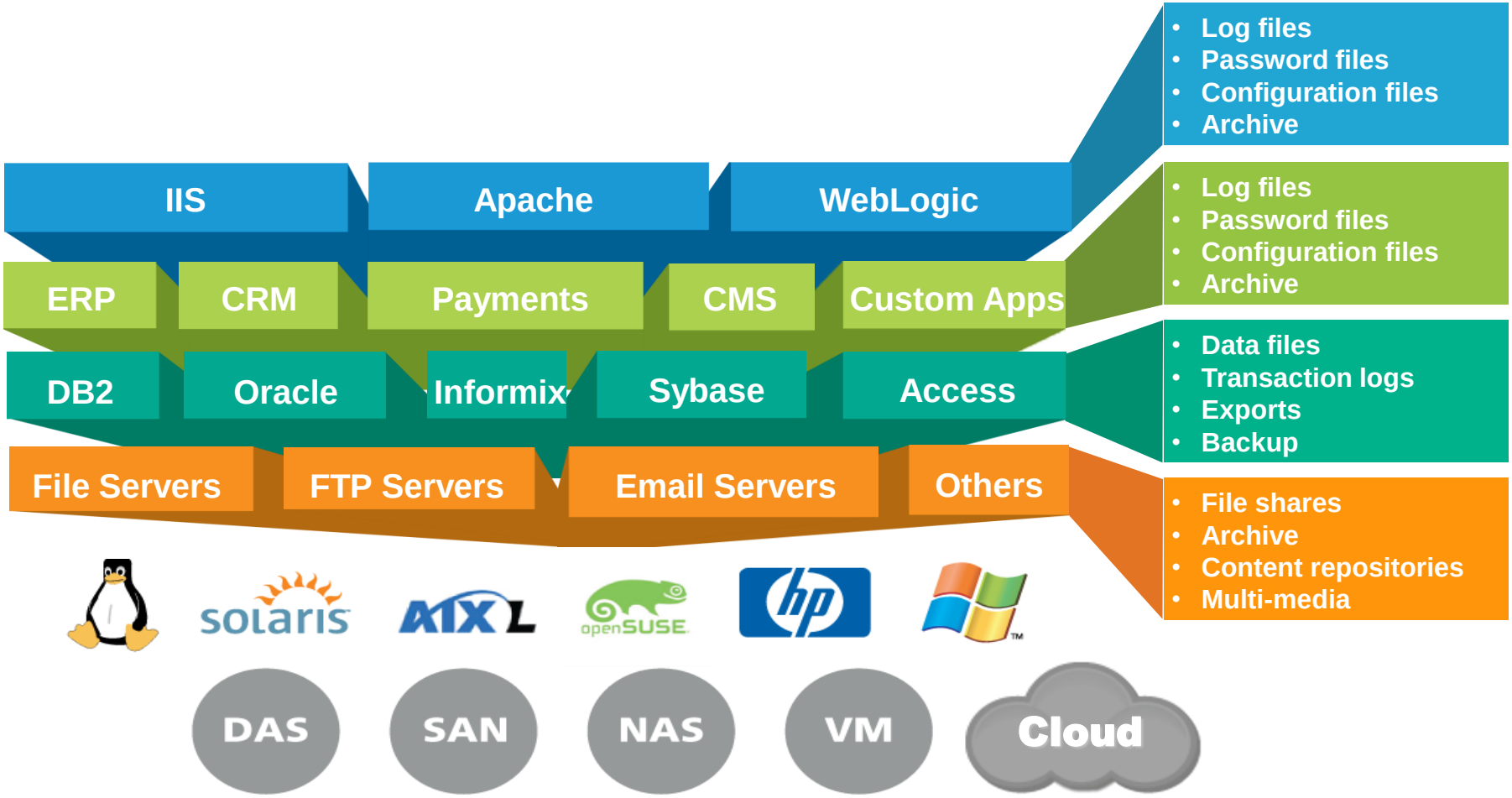


**IPS 패턴 정보로 앱 스캔
취약점 데이터 활용**

웹 개발자들

공격자

DB 암호화, 또다른 생각!!!

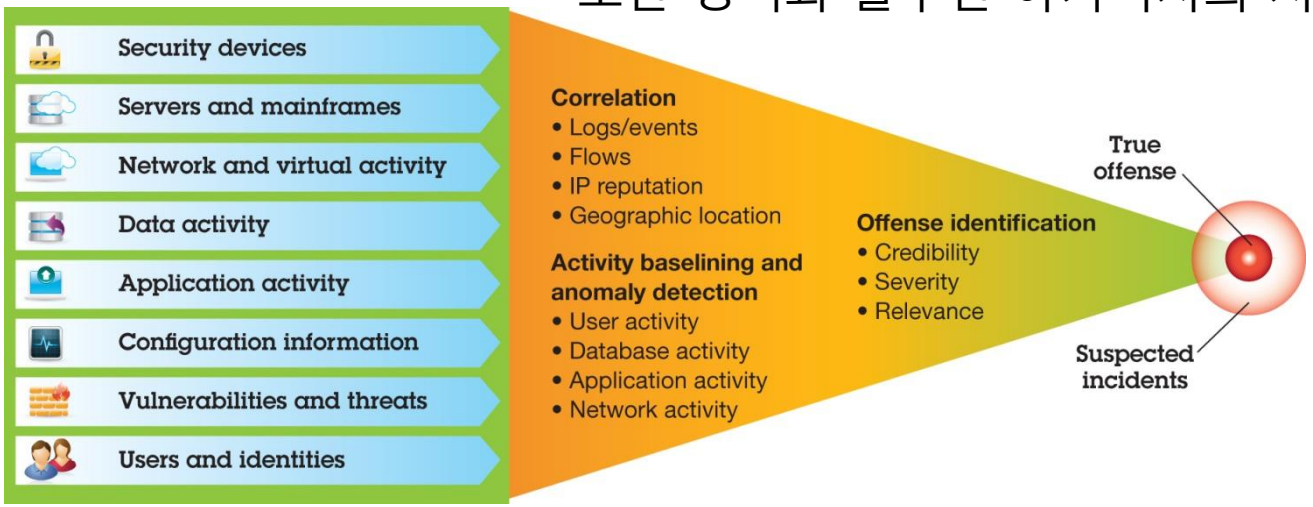


IBM 보안 프레임워크

IBM 보안 프레임워크 사용법

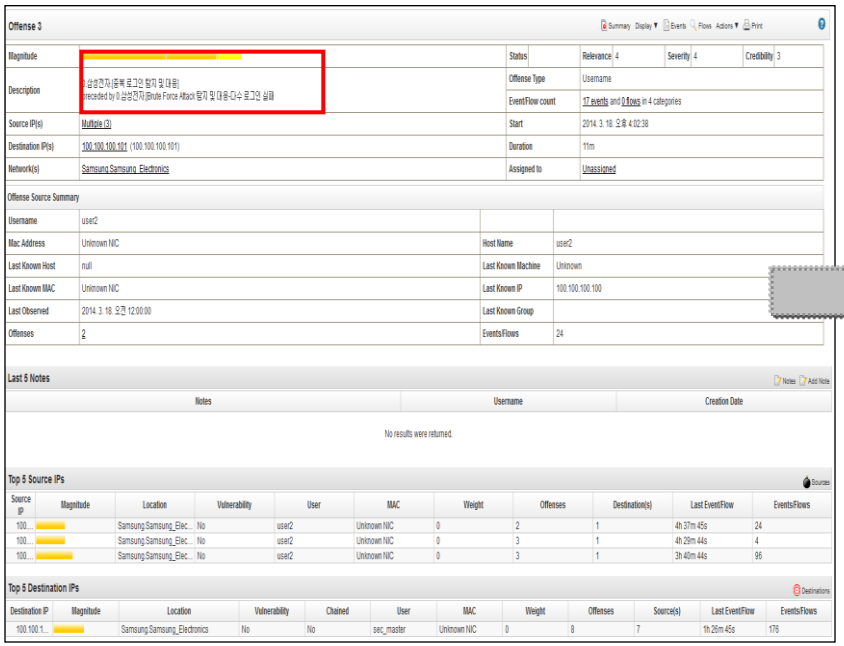
카테고리	Identity and Access Management	Data Information Protection	Assurance	Threat & Vulnerability
People	분류 & 관리	인증 보호	행위	교육 & 문화
Data	접근통제	분류 & 암호	무결성	암호키 관리
Application	권한	처리	테스트	보안코딩
Infra	접근통제	저장/전송	모니터링	패치 관리

보안 정책과 솔루션 아키텍처의 시작

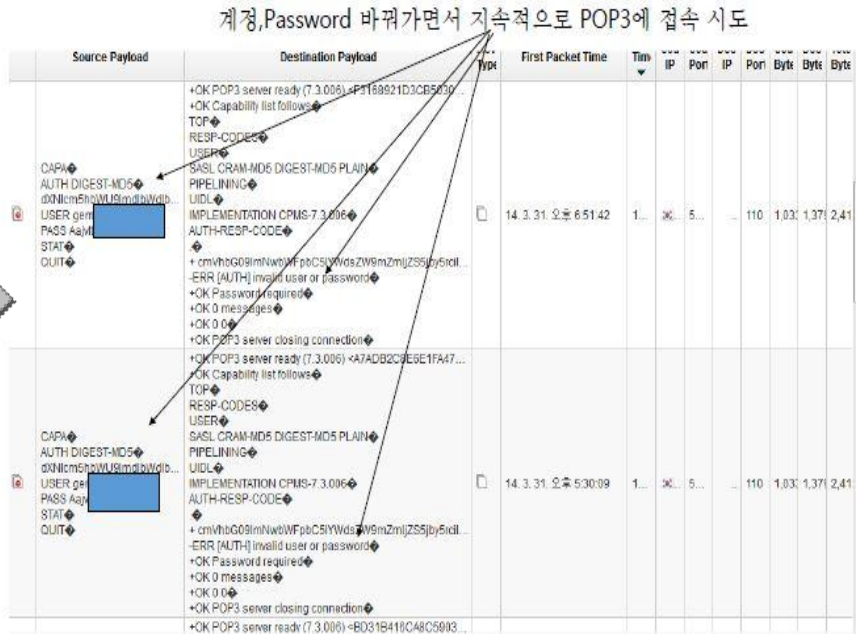


Identity Intelligence

사용자의 계정 정보를 알아내기 위해 로그인에 성공할 때까지 모든 가능한 값들을 가지고 무차별 대입시도하는 행위에 대해서 탐지합니다. 이를 QRadar가 감지하며 세션이 성공하면 발견된 세션을 삭제 또는 계정을 잠그는 등 실시간 권한을 차단하며, 보안 담당자에게 통보됩니다.

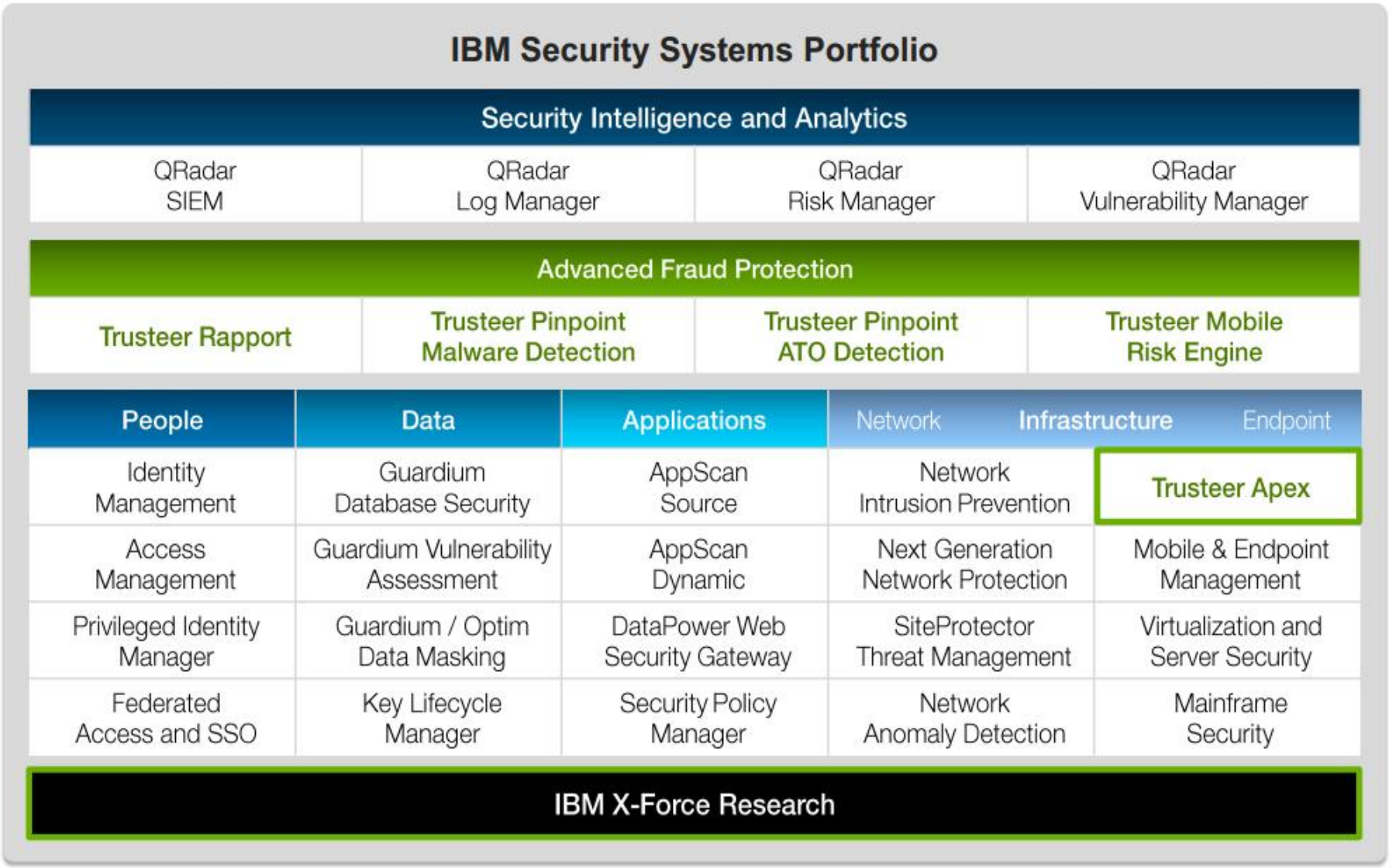


Brute-Force Attack 이벤트 탐지



동일 계정에서 1분마다 암호를 바꿔가면서 PoP3 메일 서버에 접속시도(Brute-Force Attack) 탐지 사례

IBM 보안 솔루션 포트폴리오



Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security