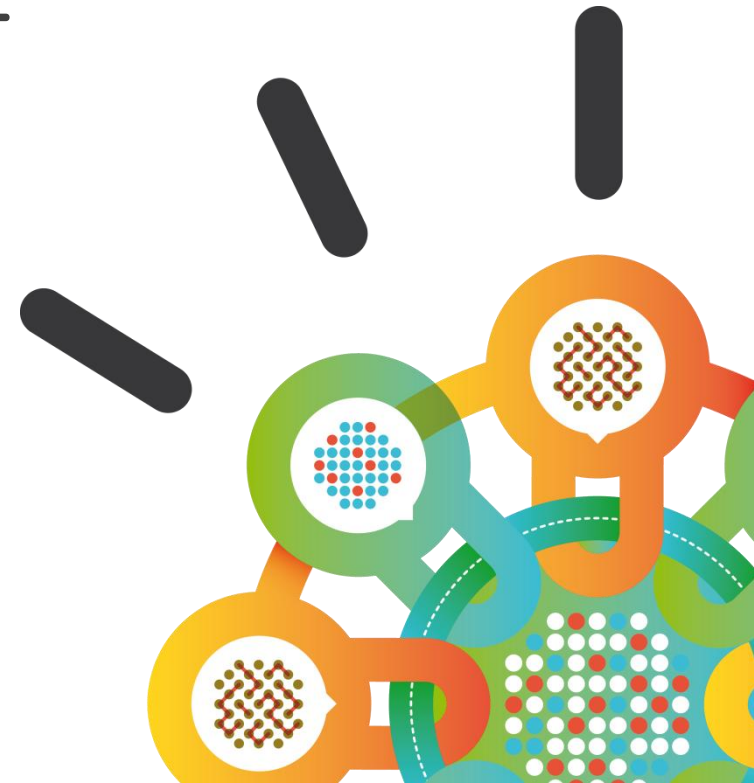


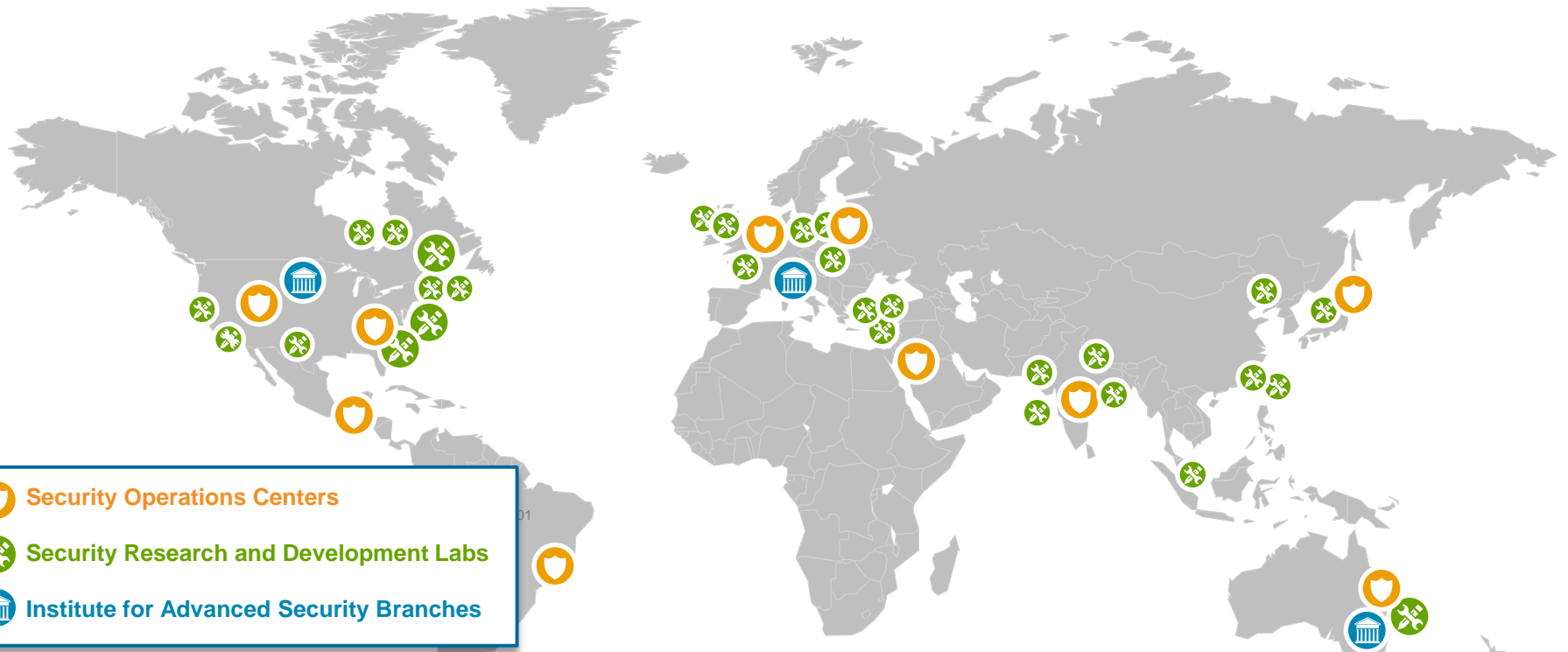
Security Intelligence.  
Think Integrated.

# 2014년 최신 보안 동향 분석 및 보안 인텔리전스 대응 방안



성명/ 직급	박 형근 전문위원	소속	한국 IBM
수상	<ul style="list-style-type: none"> <li>1997 국군기무사령부 사령관 표창 수상(제111호) - 국군기무사령부 전산 보안 체계의 취약점 발굴 보고</li> </ul>	이메일	<a href="mailto:phk@kr.ibm.com">phk@kr.ibm.com</a>
주요 경력	<ul style="list-style-type: none"> <li>고려대학교 화학공학과 학사 졸업(93학번, 2000년 졸업)</li> <li>2000년 - 현재 한국IBM 재직</li> <li>現 한국IBM IBM Security 보안팀 기술 리더 및 한국 IBM X-Force 연구소 한국 대변인</li> </ul>	저서	<ul style="list-style-type: none"> <li>2010 OASIS 웹 서비스 품질 요소 표준 중 웹 서비스 보안 품질 분야 표준 저술 (OASIS)</li> <li>2010 ‘경영자, 보안 담당자, 개발자, 감사자가 반드시 알아야 하는 정보 보안 취약점과 지침’ 기획, 감수 및 출간 (시큐리티플러스)</li> <li>2011 개인정보보호 실천 가이드 (인포더, 공저)</li> <li>2012 퍼블릭 클라우드 컴퓨팅 사용 기업이 고려해야 할 보안 위험과 대응 방안에 대한 小考 (정보보호학회 2012.11 제22권 제7호)</li> </ul>
	<ul style="list-style-type: none"> <li>現 서울사이버대학교 정보통신학부 외래교수</li> <li>現 미래창조과학부 미래전략 IT 자문 위원</li> <li>現 국제 OWASP 한국챕터 고문</li> <li>現 정보보안 전문 커뮤니티 시큐리티플러스 대표 운영자</li> <li>CISSP, CISA, CGEIT 국제 자격증 보유</li> </ul>	강의	<ul style="list-style-type: none"> <li>국가정보보안교육원 정보보안 과정 출강               <ul style="list-style-type: none"> <li>- APT 사고 사례 및 대응 방안</li> </ul> </li> <li>CIOCISO매거진 2012 CISO 전략 과정 출강               <ul style="list-style-type: none"> <li>- 정보보호 프레임워크와 아키텍처</li> <li>- 정보보호 성과 관리</li> </ul> </li> <li>IBM교육센터 보안 과정 다수 출강               <ul style="list-style-type: none"> <li>- IBM 보안프레임워크와 아키텍처</li> </ul> </li> <li>서울사이버대학교 해킹과 보안 과정 출강</li> </ul>
	<ul style="list-style-type: none"> <li>現 ISC2, ISACA, 국제보안포럼, OpenGroup 정회원</li> </ul>	SNS	<ul style="list-style-type: none"> <li>트위터: <a href="http://twitter.com/#!/securityinsight">http://twitter.com/#!/securityinsight</a></li> <li>페이스북: <a href="http://www.facebook.com/hyungkeun.park">http://www.facebook.com/hyungkeun.park</a></li> <li>Linkedin: <a href="http://kr.linkedin.com/pub/hyung-keun-park/1/890/113">http://kr.linkedin.com/pub/hyung-keun-park/1/890/113</a></li> </ul>

# IBM 보안 역량



- Security Operations Centers
- Security Research and Development Labs
- Institute for Advanced Security Branches

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
<b>3</b>	<b>IBM</b>
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



- ✓ central strategic targets
- ✓ takeover social profiles
- zero day drive by download
- ✓ mobile malware

# 5억건 이상, 2013년도 개인정보 유출 사고!!!

**A historical look at security incidents by attack type, time and impact, 2011 to 2013**  
 conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

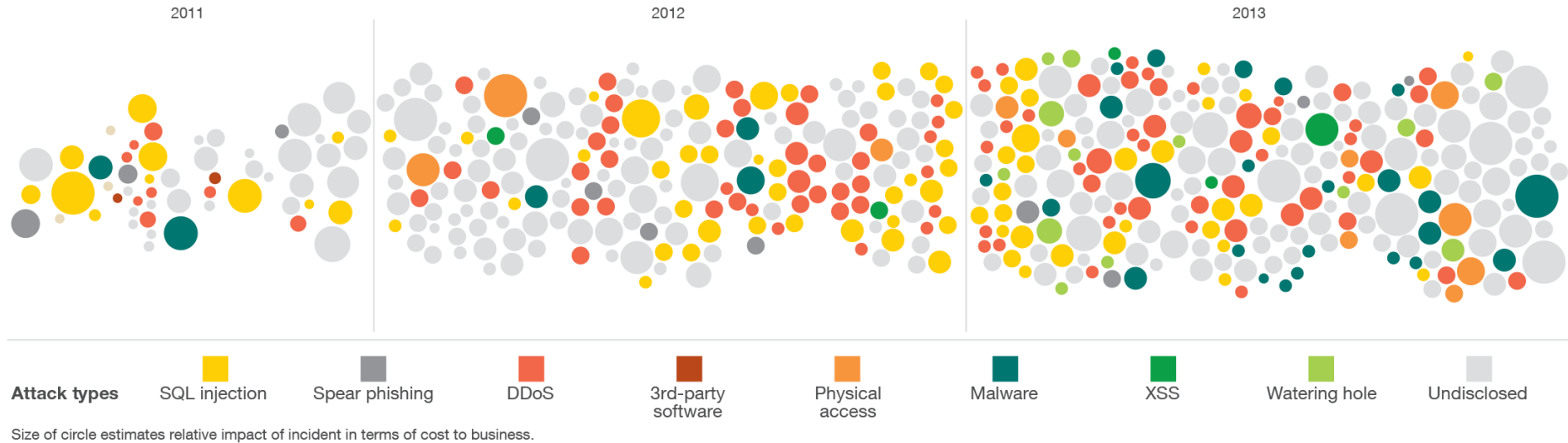
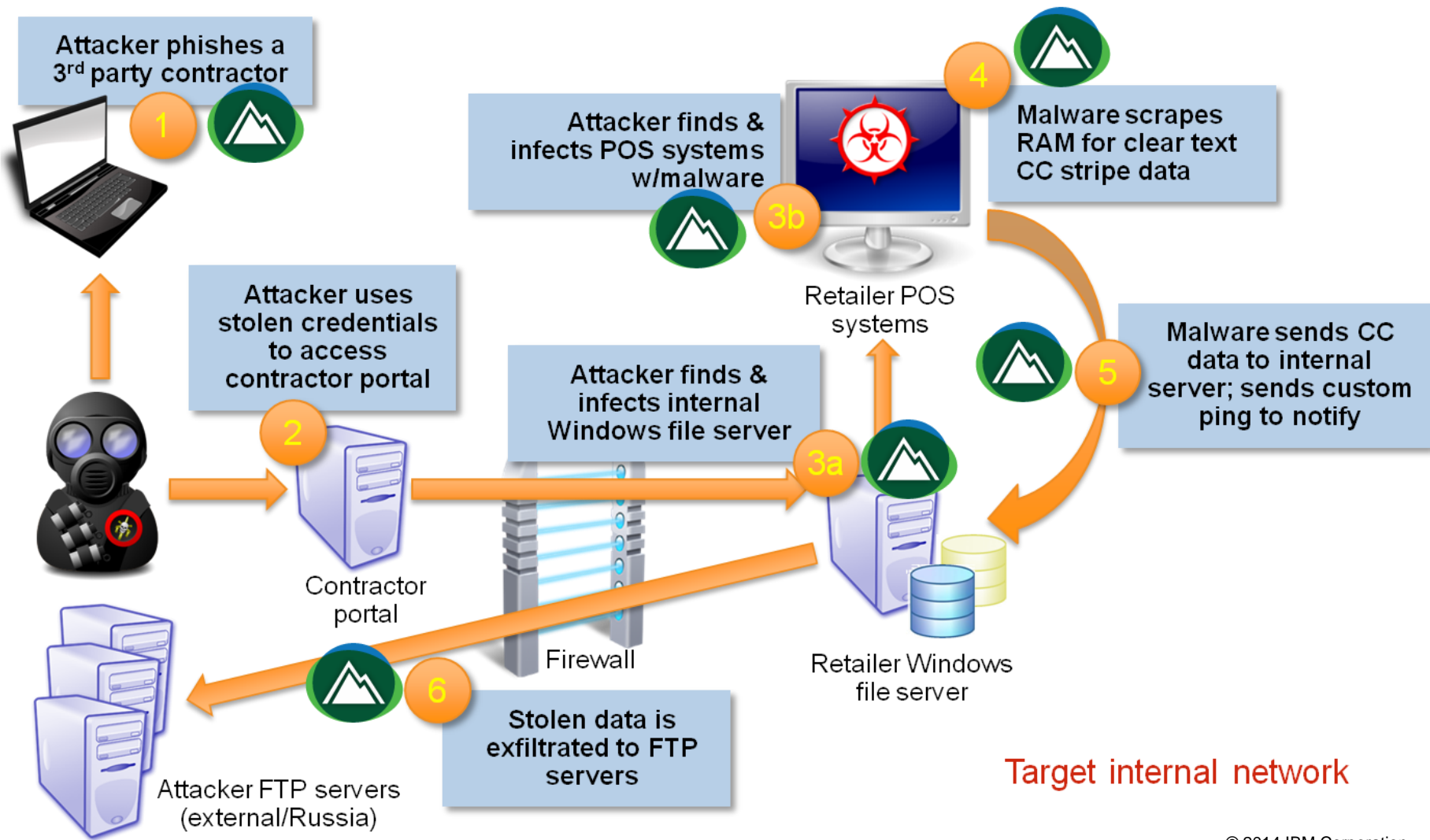


Figure 1. A historical look at security incidents by attack type, time and impact, 2011 to 2013

Source: IBM X-Force® Research and Development

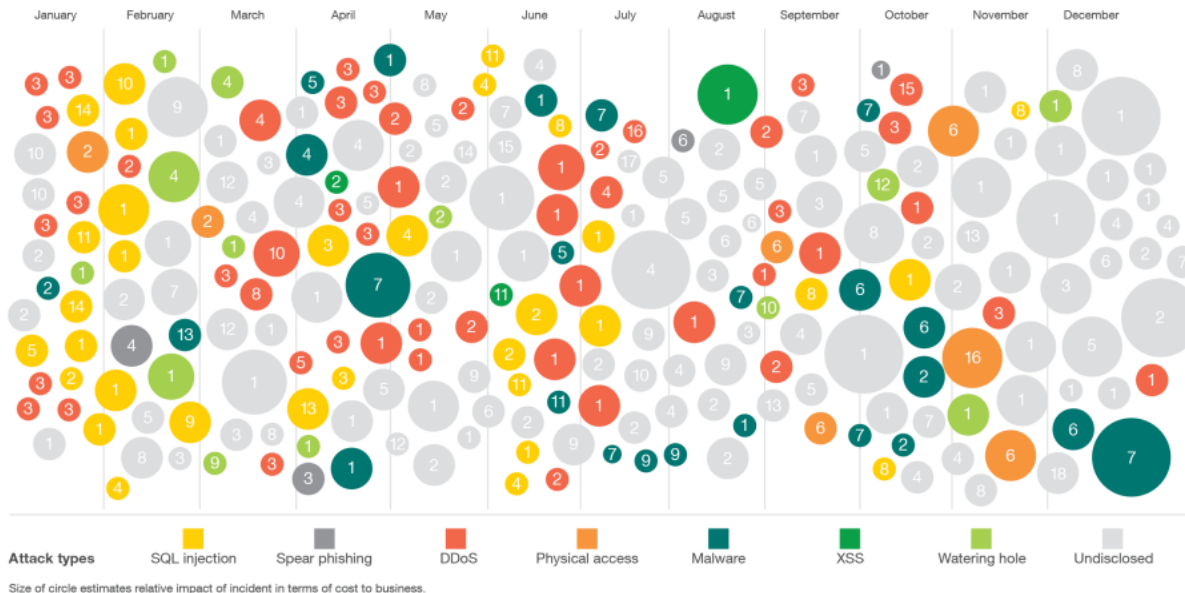
# Target Data Breach Case Study

## Anatomy of the Target Retailer Breach



## Sampling of 2013 security incidents by attack type, time and impact

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses



### Most-commonly attacked industries

- 28% Computer Services (1)
- 15% Government (2)
- 12% Financial Markets (3)
- 9% Media & Entertainment (4)
- 7% Education (5)
- 5% Healthcare (6), Retail (7), Telecommunications (8)
- 3% Consumer Products (9)
- 2% Non-Profit (10), Automotive (11), Energy & Utilities (12), Professional Services (13)
- 1% Industrial Products (14), Travel & Transportation (15), Wholesale Distribution & Services (16)
- <1% Aerospace & Defense (17), Insurance (18)

### Most-common attack types

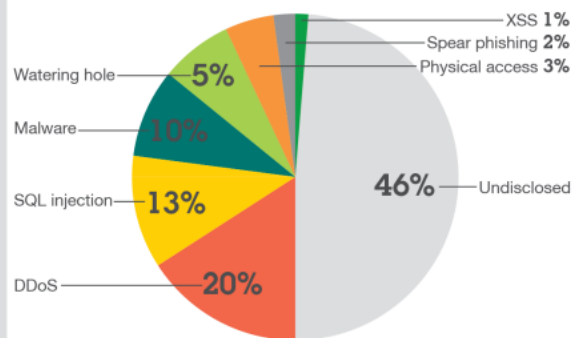


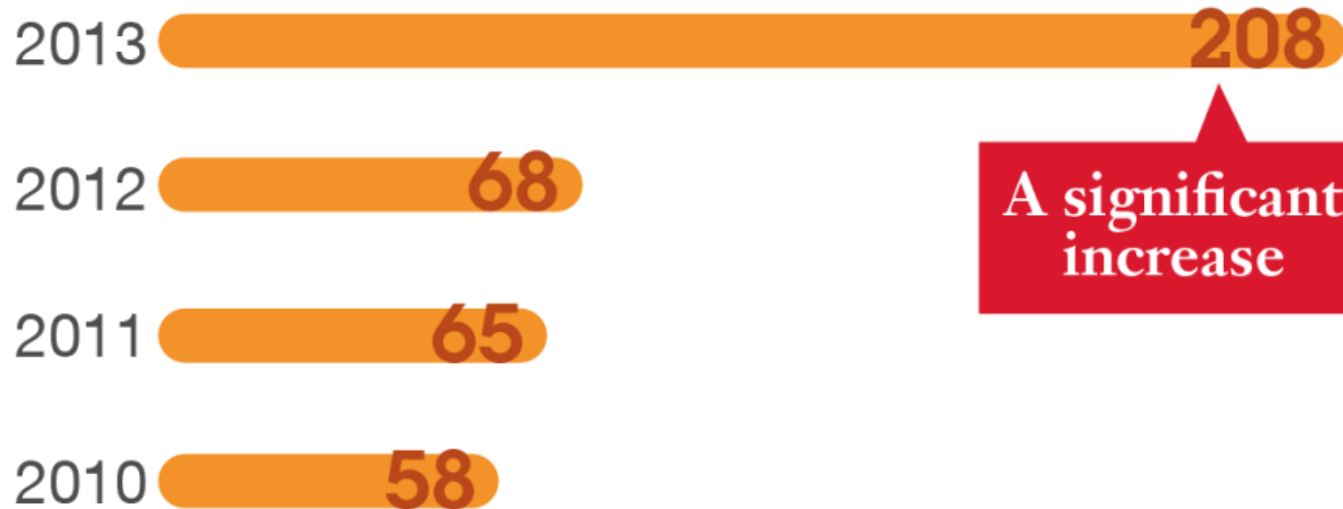
Figure 2a. Sampling of 2013 security incidents by attack type, time and impact



# 자바 취약점 증가

## Java vulnerability disclosures growth by year, 2010 to 2013

originating in either the core Oracle Java or in IBM Java SDKs



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

Source: IBM X-Force® Research and Development

# 공격에 활용되는 대표적인 사용자 어플리케이션

## Exploitation of application vulnerabilities

from survey of 1 million Trusteer customers, December 2013

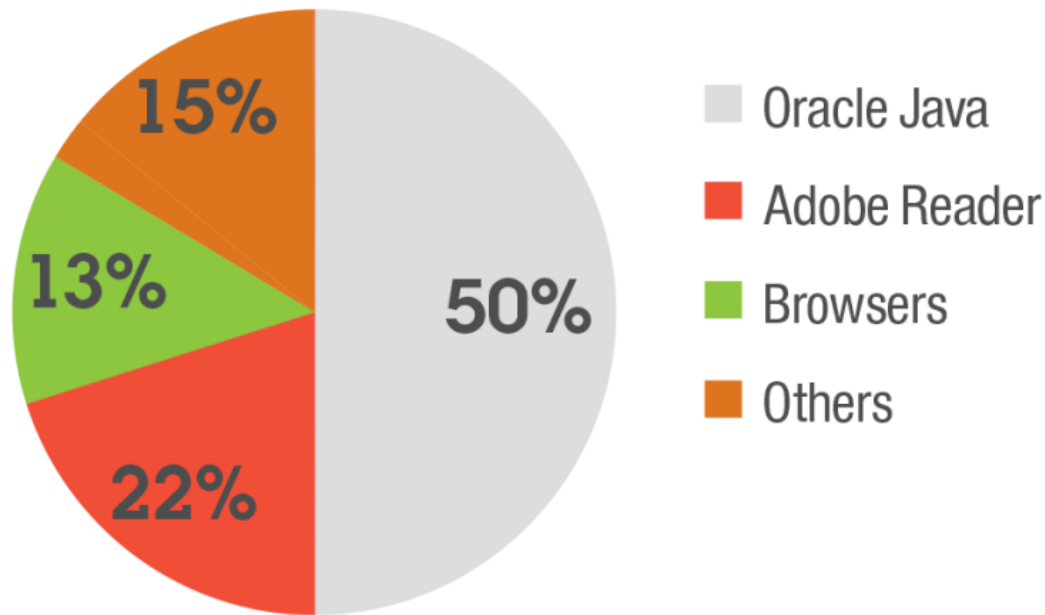
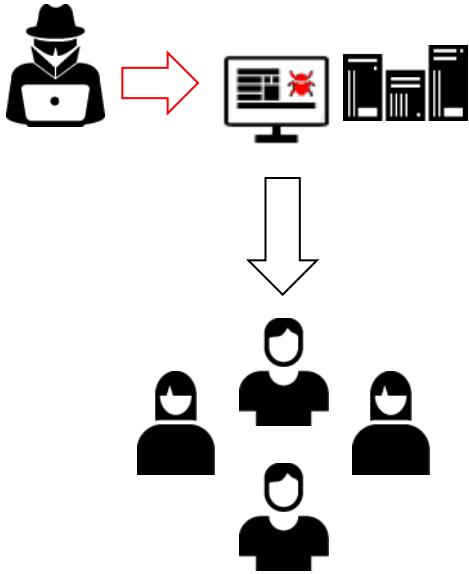


Figure 4. Exploitation of application vulnerabilities

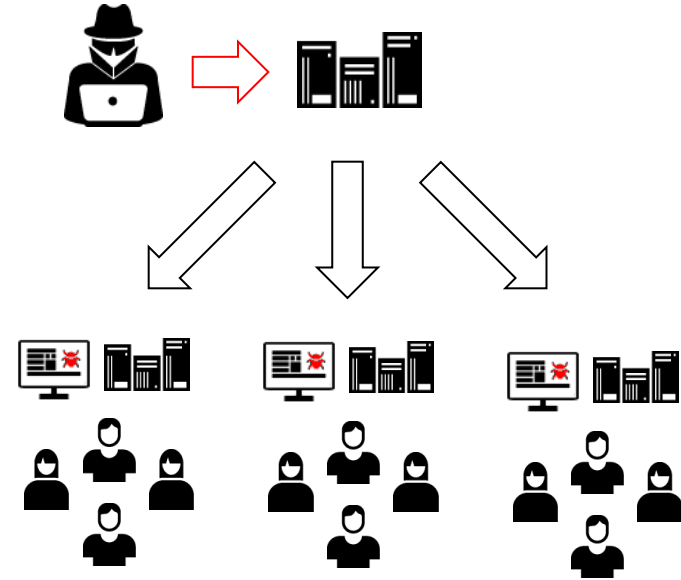
Source: IBM X-Force® Research and Development

# 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

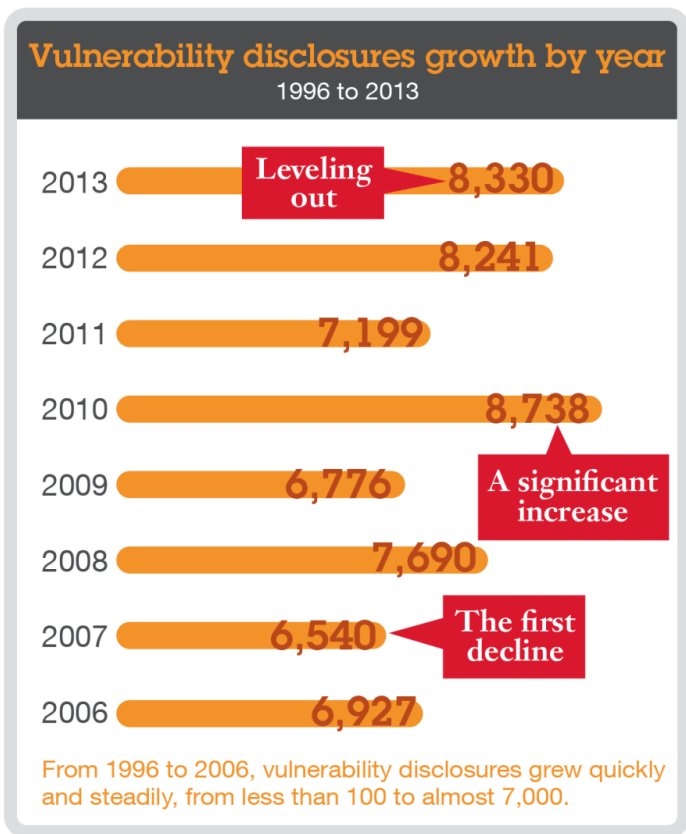


Figure 8. Vulnerability disclosures growth by year, 1996 to 2013

Source: IBM X-Force® Research and Development

## Web application vulnerabilities by attack technique

as percentage of total disclosures, 2009 to 2013

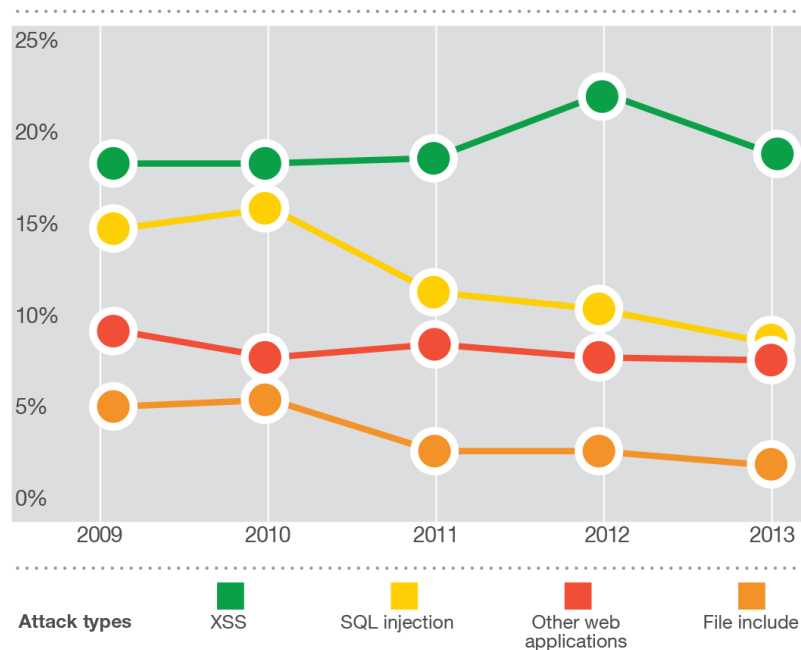


Figure 11. Web application vulnerabilities by attack technique, 2009 to 2013

Source: IBM X-Force® Research and Development

# 주요 소프트웨어 공급사의 패치 주기 향상

## Unpatched vulnerabilities

The total amount of unpatched vulnerabilities recorded **dropped by 15%** in 2013.

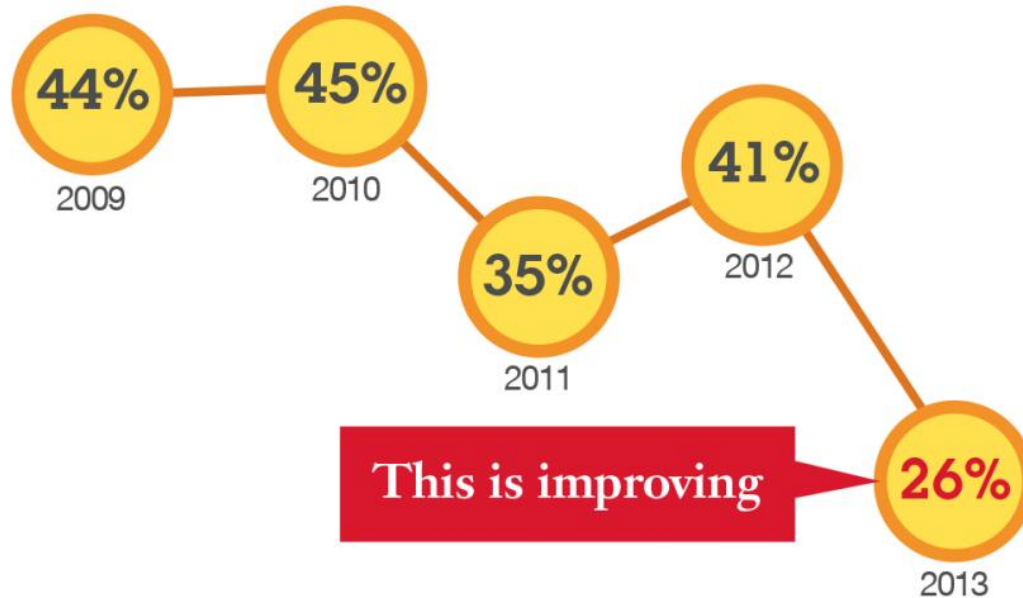
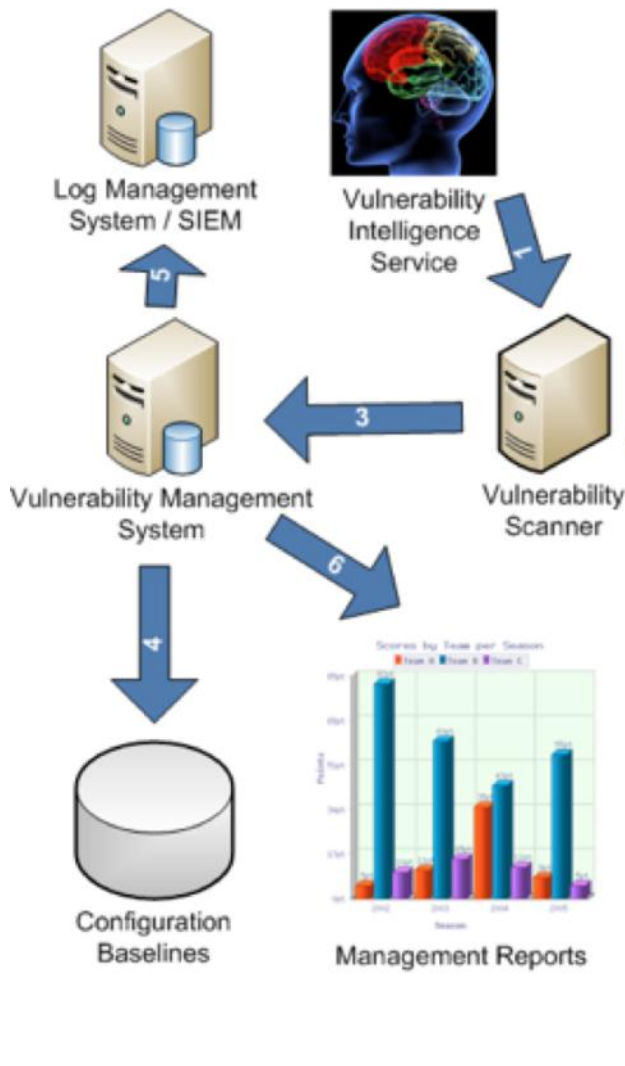


Figure 10. Vendor patch rates of publicly disclosed vulnerabilities, 2009 to 2013

Source: IBM X-Force® Research and Development

# OpenSSL HeartBleed Vulnerability?!!!!



Manage Vulnerabilities > By Asset > By Vulnerability Instances

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 - OpenSSL - 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

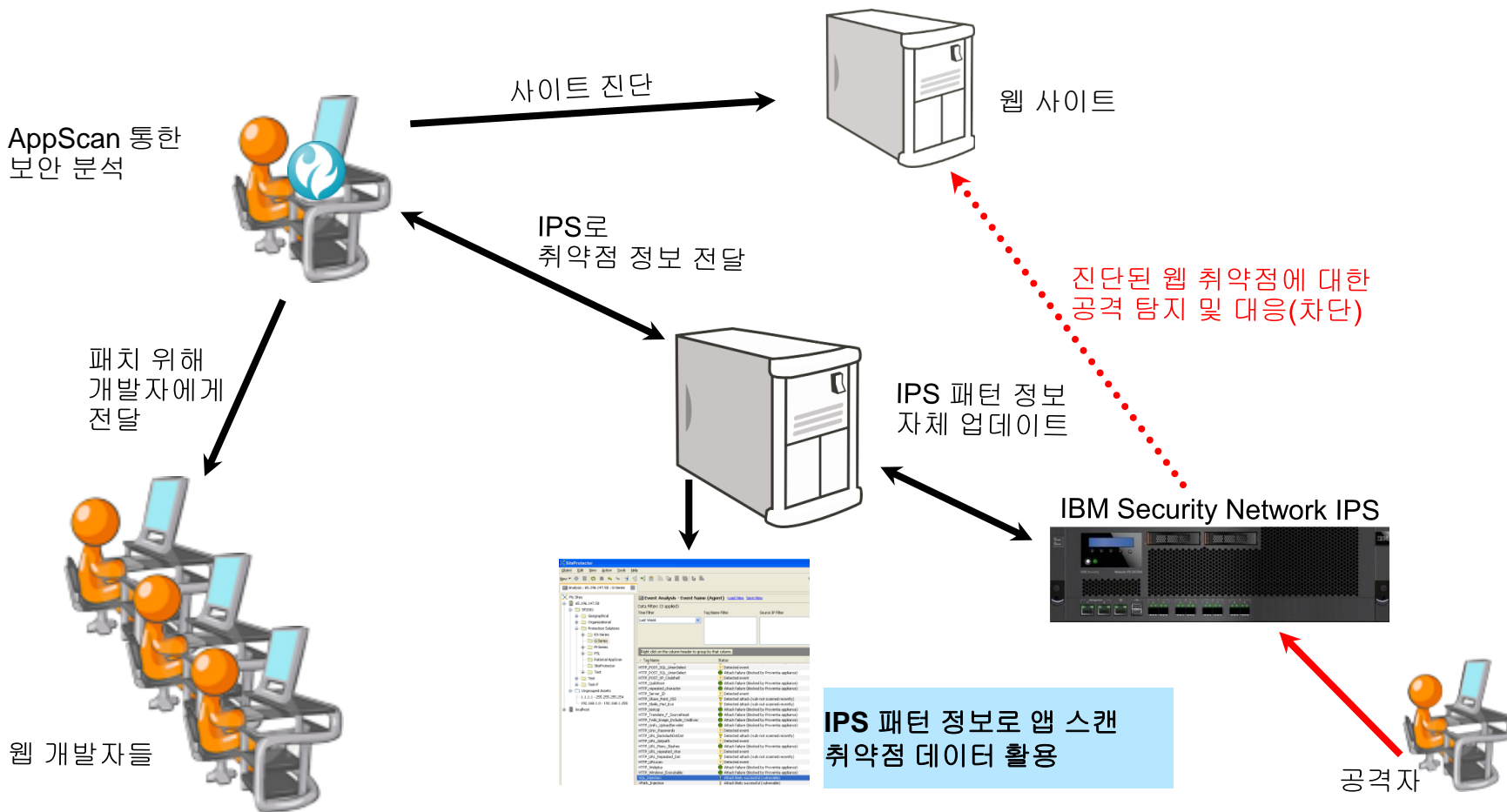


OpenSSL HeartBleed  
취약점에 대한 공격 탐지 및  
대응(차단)

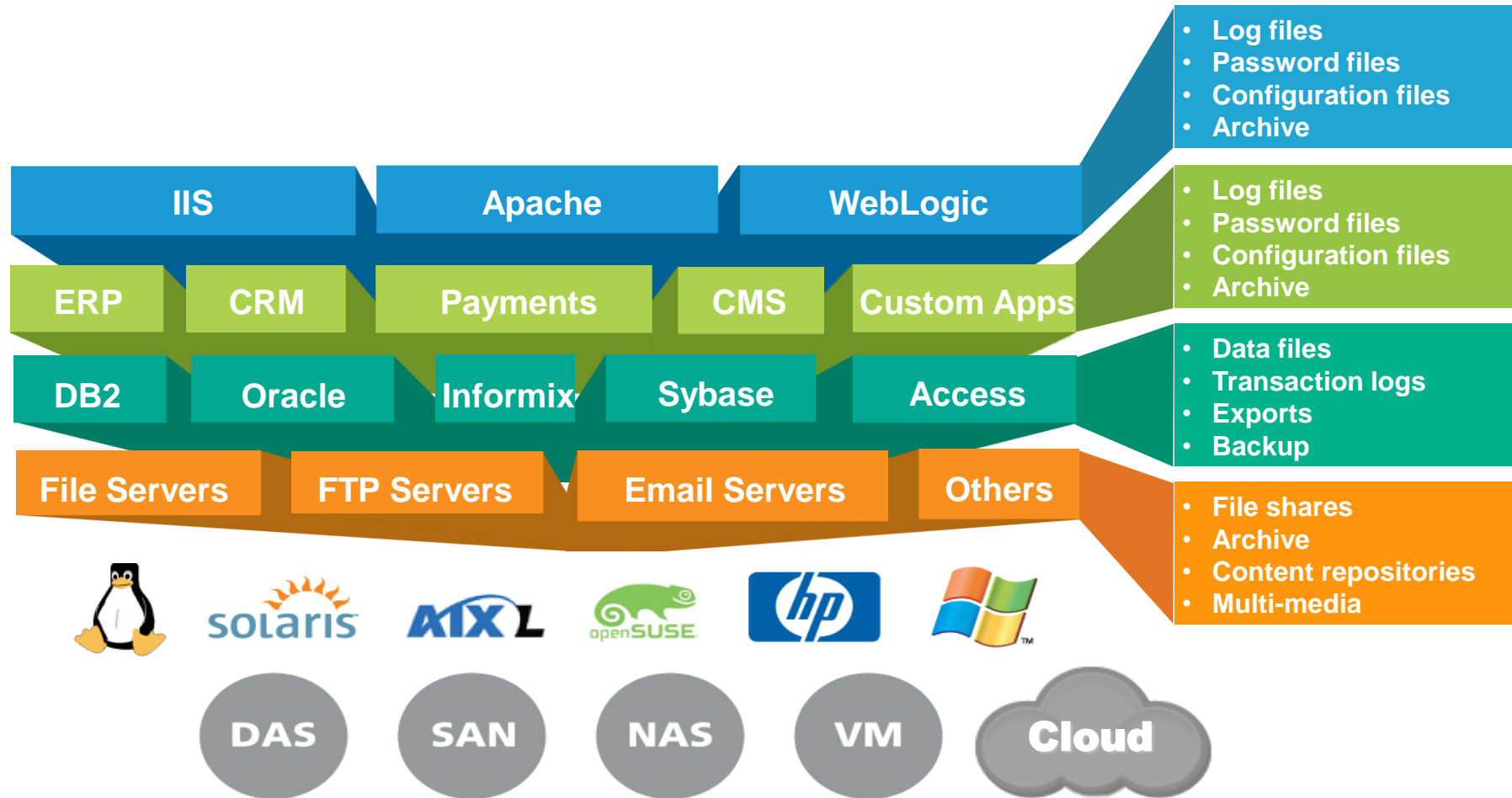


총 1,151,673건

# 웹 보안, 또다른 생각!!!

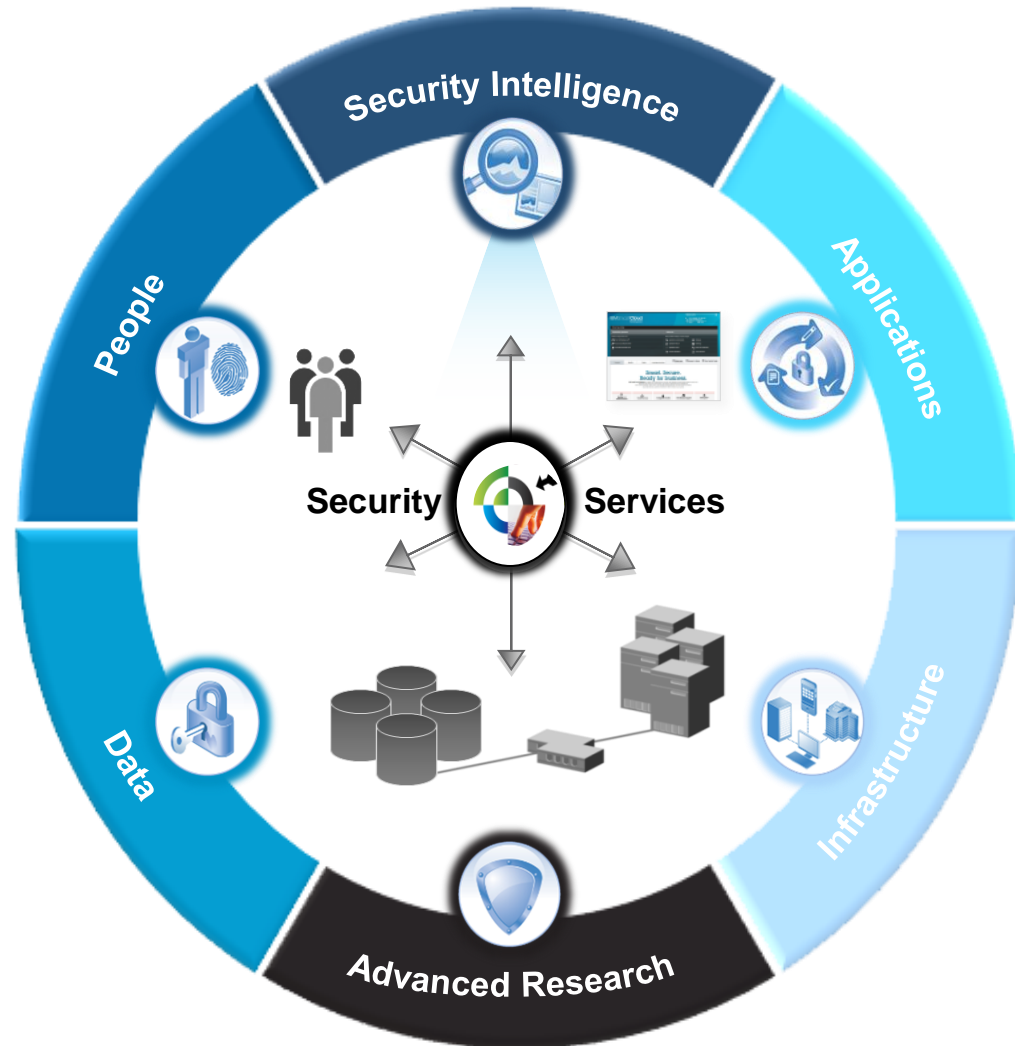


# DB 암호화, 또다른 생각!!!





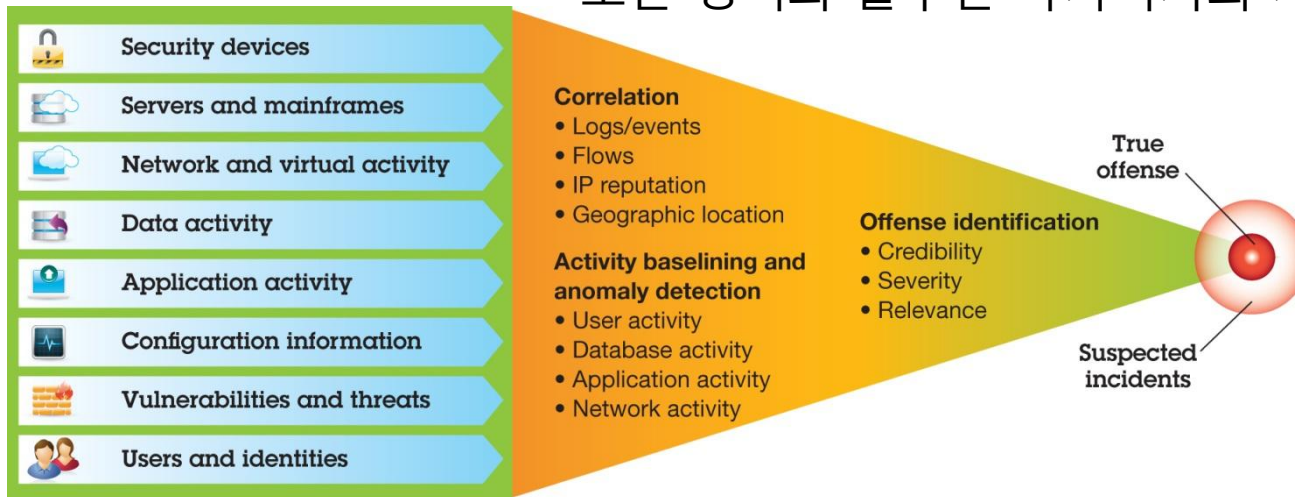
# IBM 보안 프레임워크



# 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.

Offense 3	Summary	Display	Events	Flow	Actions	Print					
<b>Magnitude</b>	4	Reference	4	Severity	4	Credibility	3				
<b>Description</b>	성공한지(공백 로그인 및 다중) recorded by 성공한지 (Role Force Abuse 탐지 및 대응)로그인 실패						Status Offense Type: Username EventFlow count: 17 events and 2 flows in 4 categories				
<b>Source IP(s)</b>	Multiple (2)	<b>Start</b>	2014. 3. 18. 오후 4:02:38								
<b>Destination IP(s)</b>	100.100.100.101 (100.100.100.101)	<b>Duration</b>	11m								
<b>Network(s)</b>	Samsung Samsung_Electronic	<b>Assigned to</b>	Unassigned								
<b>Offense Source Summary</b>											
<b>Username</b>	user2	<b>Host Name</b>	user2								
<b>Mac Address</b>	Unknown NIC	<b>Last Known Host</b>	null								
<b>Last Known MAC</b>	Unknown NIC	<b>Last Known IP</b>	100.100.100.100								
<b>Last Observed</b>	2014. 3. 18. 오후 12:00:00		<b>Last Known Group</b>								
<b>Offenses</b>	2	<b>Events/Flows</b>	24								
<b>Last 5 Notes</b>											
No results were returned.											
<b>Top 5 Source IPs</b>											
Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last EventFlow	Events/Flows	
100.100.100.101	4	Samsung Samsung_Elec...	No	user2	Unknown NIC	0	2	1	4b 37m 45s	24	
100.100.100.101	4	Samsung Samsung_Elec...	No	user2	Unknown NIC	0	3	1	4b 23m 44s	4	
100.100.100.101	4	Samsung Samsung_Elec...	No	user2	Unknown NIC	0	3	1	3h 43m 44s	96	
<b>Top 5 Destination IPs</b>											
Destination IP	Magnitude	Location	Vulnerability	Chained	User	MAC	Weight	Offenses	Source(s)	Last EventFlow	Events/Flows
100.100.100.101	4	Samsung Samsung_Electronic	No	No	sec_master	Unknown NIC	0	8	7	1h 25m 45s	176

계정, Password 바꾸가면서 지속적으로 POP3에 접속 시도

Source Payload	Destination Payload	Type	First Packet Time	Tim	IP	Port	IP	Port	Byt	Byt	Byt
CAPA AUTH DIGEST-MD5 dXNlcmlzbnVURmludWVib... USER ge... PASS AaM... STAT... QUIT	+CK POP3 server ready (7.3.005) <P3168921D3CB5030... +CK Capability list follows TOP RESP-CODES USER SASL CRAM-MD5 DIGEST-MD5 PLAIN PIPELINING UIDL IMPLEMENTATION CPMS-7.3.006 AUTH-RESP-CODE + cmVhbG09ImNwblWFpbC5iYVVsZmZlZS5yZS51by5icm... -ERR [AUTH] invalid user or password +CK Password required +CK 0 messages +CK 0 OK +CK POP3 server closing connection		14. 3. 31. 오후 6:51:42	1...	100.100.100.101	110	103	1,371	2,41		
CAPA AUTH DIGEST-MD5 dXNlcmlzbnVURmludWVib... USER ge... PASS AaM... STAT... QUIT	+CK POP3 server ready (7.3.005) <A7ADB2C9E6E1FA47... +CK Capability list follows TOP RESP-CODES USER SASL CRAM-MD5 DIGEST-MD5 PLAIN PIPELINING UIDL IMPLEMENTATION CPMS-7.3.006 AUTH-RESP-CODE + cmVhbG09ImNwblWFpbC5iYVVsZmZlZS5yZS51by5icm... -ERR [AUTH] invalid user or password +CK Password required +CK 0 messages +CK 0 OK +CK POP3 server closing connection		14. 3. 31. 오후 5:30:09	1...	100.100.100.101	110	103	1,371	2,41		
	+CK POP3 server ready (7.3.005) <BD31B418C48C5093...										

Brute-Force Attack 이벤트 탐지

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

# IBM 보안 솔루션 포트폴리오

## IBM Security Systems Portfolio

### Security Intelligence and Analytics

QRadar  
SIEM

QRadar  
Log Manager

QRadar  
Risk Manager

QRadar  
Vulnerability Manager

### Advanced Fraud Protection

Trusteer Rapport

Trusteer Pinpoint  
Malware Detection

Trusteer Pinpoint  
ATO Detection

Trusteer Mobile  
Risk Engine

People	Data	Applications	Network	Infrastructure	Endpoint
Identity Management	Guardium Database Security	AppScan Source	Network Intrusion Prevention	<b>Trusteer Apex</b>	
Access Management	Guardium Vulnerability Assessment	AppScan Dynamic	Next Generation Network Protection	Mobile & Endpoint Management	
Privileged Identity Manager	Guardium / Optim Data Masking	DataPower Web Security Gateway	SiteProtector Threat Management	Virtualization and Server Security	
Federated Access and SSO	Key Lifecycle Manager	Security Policy Manager	Network Anomaly Detection	Mainframe Security	

### IBM X-Force Research

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](http://www.ibm.com/security)



© Copyright IBM Corporation 2014. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.