보안, 침입을 막아라!
- 제로데이, APT 그리고 트랜잭션 보안

IBM 소프트웨어 보안 사업부 박형근 부장/전문위원

미디어를 통해 바라본 APT

APT공격, 99.999% 당한다 :: 보
www.boan.com › 뉴스 › 보안/융합 - Ca
2011년 10월 16일 – 3500만명 S 사
스턱스넷(Stuxnet)과 ... 공격 등

특정 기업 노린 표적 공격, 11월
www.csokorea.org/.../sub01-5_view.asp
2011년 12월 14일 – 이는 2백만개의 이메
적 공격을 ... 직원수가 250명 미만인 중

"APT 공격 급증세, C
2012년 05월 [redacted] 7:44:45 / 이민형 기자 kiku

'APT 공격 확산, 모바일 보안 위협
www.itdaily.kr › 뉴스 - Cached - Translat
2011년 11월 30일 – APT 공격도 이 같은
단 보안 ... 공격의 위협에 대한 무관심과

Computer networks crash at South Korean banks, media companies; North Korea attack suspected

By Associated Press, Published: March 20 | Updated: Thursday, March 21, 7:38 AM

SEOUL, South Korea — A cyberattack caused computer networks at major South Korean banks and top TV broadcasters to crash simultaneously Wednesday, paralyzing bank machines across the country and prompting speculation of North Korean involvement.

Advanced Persistent Threat이란?

특정 대상의 기밀정보나 정치적 목적을 위해 최신의 복합적인 공격 전략과 방식들을 통해 지속적으로 위협을 가하는 형태

Advanced

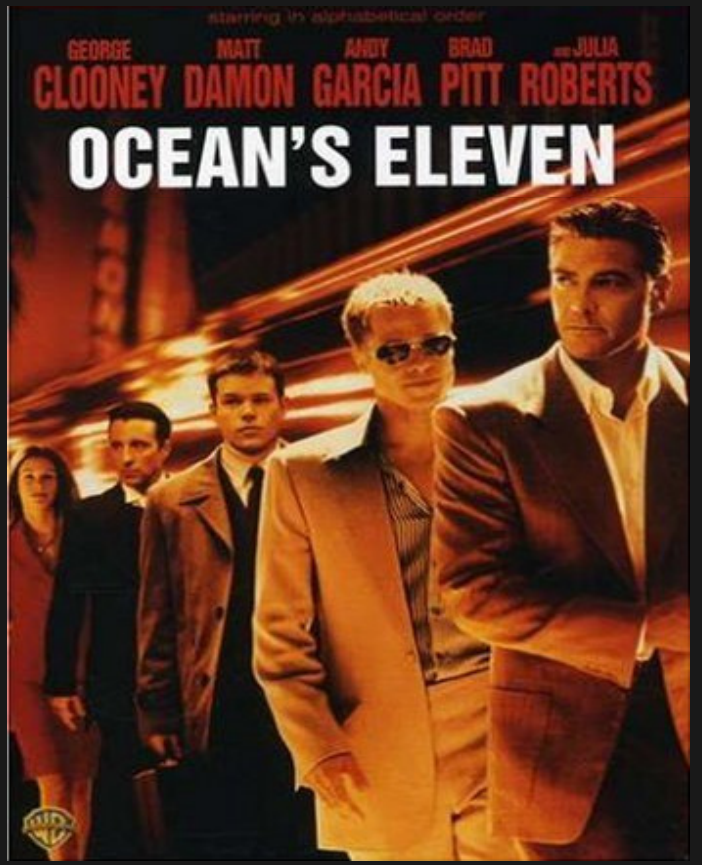
- 기존 보안 제품을 우회하도록 새로운 형태의 악성코드 제작
- 아직 보고되지 않은 취약점 악용 (제로데이)
- 협업과 연구 기반의 공격 수행

Persistent

- 수 개월에서 수년에 걸친 공격 수행
- 탐지에 대한 방해 및 조치 회피 시도 (내성)

Threat

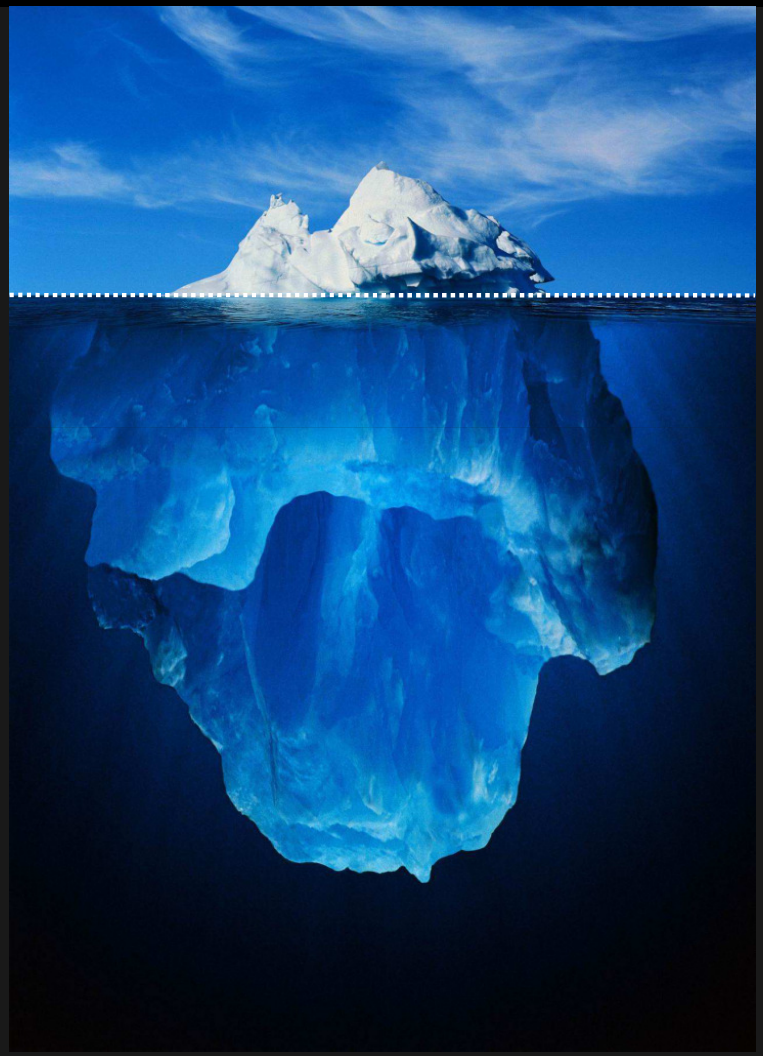
- 무작위 공격이 아님
- 기밀 정보 획득을 위해 조직내에 특정 개인 또는 그룹을 목표로 함
- 자동화된 툴/스캐닝에 의존하지 않고 사람이 개입됨



APT의 공격사례: Watering Hole (Drive-by-Download)

공격의 파급력

드러난 공격은 빙산의 일각이다



지속적 정보 노출

- 기밀정보
- 개인정보
- 금융정보(계좌번호..)

컴플라이언스와 법적문제

- 기관의 감사
- 법적 분쟁
- 소송

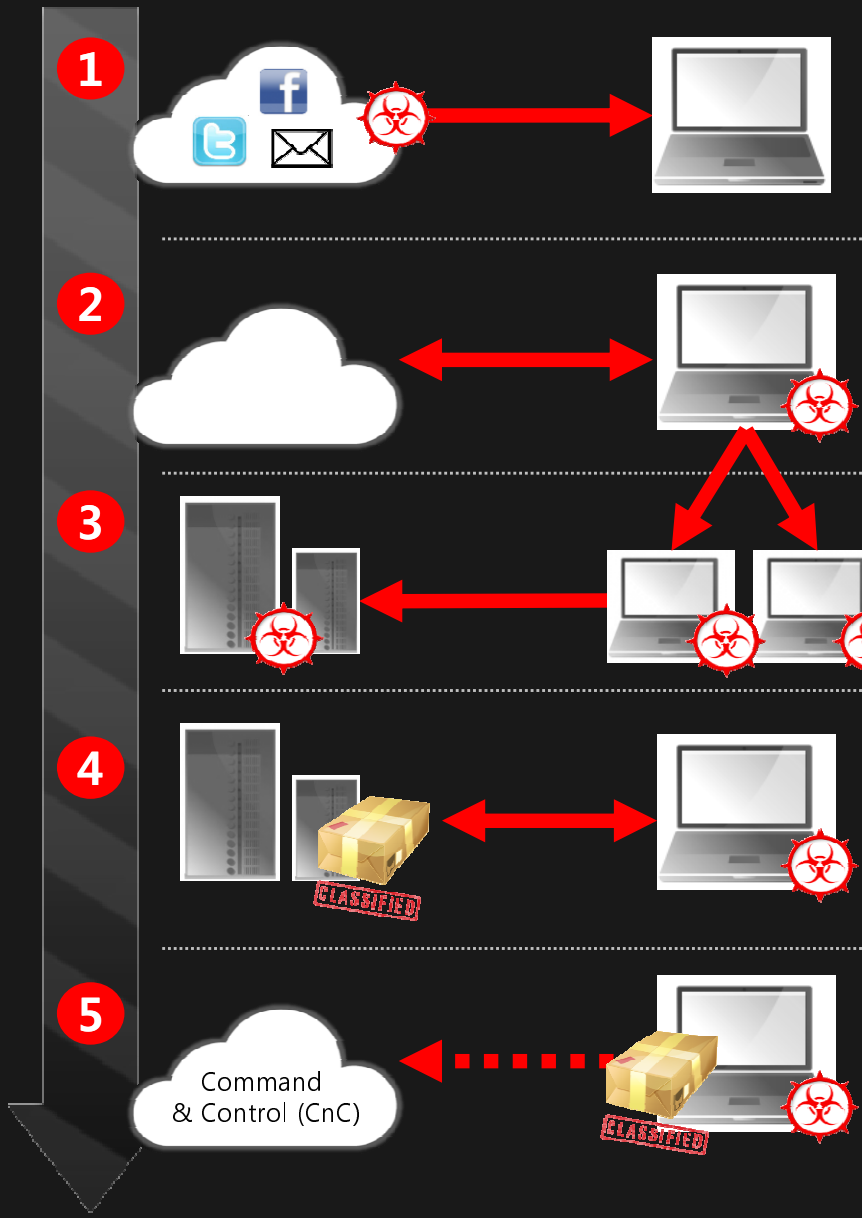
관리 비용의 증가

- 포렌식 관찰
- 트랜잭션 리뷰
- 지속적 기술투자

고객 영향

- 브랜드
- 고객의 경험
- 시장의 혼란

공격자의 5단계 공격



침투 — 스피어 피싱 또는 원격 취약점 공격을 통해 접근

교두보 — 거점 확보를 위한 멀웨어와 백도어 설치

확장 — 추가 접근 획득 및 상태 유지를 위한 정찰 및 이동

수집 — 기밀 데이터에 대한 수집

탈취 — 외부 네트워크로 데이터 빼내기

APT에 대한 대응 ? ATP (Advanced Threat Protection) !!

1. 침투
2. 교두보
3. 확장
4. 수집
5. 탈취

Network and Endpoint Security 행위기반 분석을 사용해 제로데이 공격 차단과 130억개의 URL 데이터 베이스를 사용해 피싱/악성 사이트 차단

Network Security SIEM의 확장 기능이 네트워크를 지속적으로 모니터링하며, 위치, 어플리케이션 접근 등에 관한 비정상 행위 탐지

Secure Users 의심 가는 행위에 대한 모니터링과 접근정책 강화를 위한 강력한 계정관리

Data Security 데이터 활동에 대한 모니터링을 제공하는 데이터 저장소에 대한 깊이 있는 보안 및 세세한 접근 통제

Network Security 일반적인 데이터 유출/탈취하는 네트워크 트래픽을 능동적으로 모니터링하며 실시간 차단

Security Analytics

전사적 엔터프라이즈를 포괄하는 로그, 네트워크 트래픽, 사용자 활동 분석을 통한 행위 분석 및 월드 클래스 보안 연구소의 인텔리전스를 통한 상관분석 및 트랜드 분석으로 보안 인텔리전스 구현

Security **Intelligence**. Think **Integrated**.

Stage1 : 침투

1 침투
2 교두보
3 확장
4 수집
5 탈취

도전 과제

- 임직원들이 피싱 시도에 항상 취약함
- 잘 패치되어 있는 시스템도 알려지지 않은 취약점을 악용한 "제로데이" 공격으로 해킹당할 수 있음
- 백신은 "제로데이" 악성코드에 대해 거의 효과적이지 못함이 증명됨

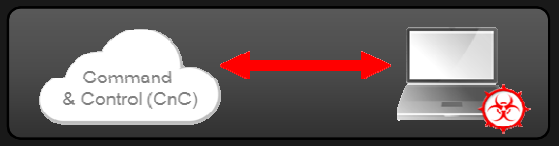
IBM 대응

- **IBM Security Network IPS와 IBM Security Network Protection**은 선진 행위기반 분석을 사용해 제로데이 공격 차단과 130억개의 URL 데이터 베이스를 사용해 피싱 및 악성 사이트를 차단을 도와 줌
- **IBM Endpoint Manager**은 패치 및 보안정책의 준수를 강화 및 공격 노출을 최소화 함
- **IBM Trusteer** Rapport는 브라우저의 신뢰성을 확보함을 통하여 Watering Hole 공격을 방어

다른 고려 사항들

- 사용하는 백신 업체에게 문의 – 제로데이 악성코드 탐지를 위해 어떤 기능을 제공하는지, 어떻게 해킹 여부를 탐지할 수 있는지.
- 제로데이 악성코드를 탐지하는 솔루션 사용을 고려
- 임직원 교육 프로그램 수립 및 수행

Stage2: 교두보



1 침투

2 **교두보**

3 확장

4 수집

5 탈취

도전 과제

- 일단 공격자가 여러분의 경계 네트워크를 무력화하여 공격에 성공하면 감염 호스트는 외부의 C&C 서버와 통신 채널을 수립하며, 언제든지 여러분의 네트워크에 접속할 수 있는 이중화를 위한 백업채널 수립

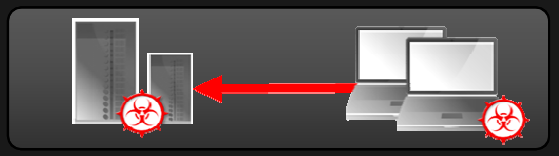
IBM 대응

- **IBM Security QRadar**는 위치, 어플리케이션 접근 등에 의한 비정상 행위를 식별하고 지속적인 모니터링 수행; 네트워크 활동의 상세 정보를 통해 해킹 여부를 판단하기 위한 포렌직 데이터 제공
- **IBM Security Network IPS**는 악의적인 목적지로의 감지하기 어려운 통신을 탐지하기 위해 행위 기반 분석을 사용
- **IBM Trusteer Apex**은 메모리상에서 비정상적인 어플리케이션의 행위 (예: C&C서버와의 통신 시도)를 감지하고 무력화시킴

다른 고려 사항들

- 사용하는 백신 업체에게 문의 – 제로데이 악성코드 탐지를 위해 어떤 기능을 제공하는지, 어떻게 해킹 여부를 탐지할 수 있는지 확인

Stage3: 확장



1 침투

2 교두보

3 **확장**

4 수집

5 탈취

도전 과제

- APT는 통상 목표 데이터를 포함하고 있는 호스트는 감염시키지 않음; 공격자는 목표 데이터를 찾아 접근하기 위한 권한 획득
- 내부 네트워크를 이해하고 핵심 자산을 확인하기 위한 정찰 활동을 수행

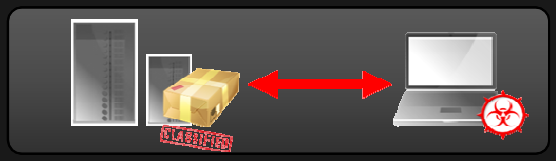
IBM 대응

- **IBM Security Privileged Identity Manager**는 핵심 시스템 및 데이터의 접근 권한을 관리하고 레코드함
- **IBM Security QRadar**는 빅데이터 규모에 활동들을 상관 분석하여 의심되는 네트워크 활동을 찾음
- **IBM Security Host Protection**는 암호화된 웹 어플리케이션으로의 통신을 포함해 의심되는 시스템 활동을 탐지하고, 악의적인 통신을 분석, 차단함
- **IBM Security AppScan**은 어플리케이션 취약점을 찾아내고 우선화 함으로써 엔터프라이즈 어플리케이션의 공격 노출을 최소화함

다른 고려 사항들

- 여러분의 접근 정책, 최소 요구되는 권한 부여, 주기적인 사용자 접근 권한 리뷰 등 능동적인 관리가 요구됨

Stage4: 수집



1. 침투
2. 교두보
3. 확장
4. **수집**
5. 탈취

도전 과제

- 공격자가 여러분의 사용자를 해킹하고 기밀 데이터 저장소에 접근 권한을 획득한다면, 목표 데이터를 획득

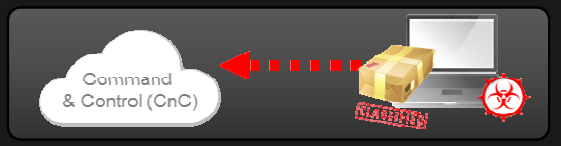
IBM 대응

- **IBM InfoSphere Guardium**는 의심적인 접근을 파악하고, 기밀 데이터를 보호하기 위해 데이터베이스와 데이터 웨어하우스를 지속적으로 모니터함
- **IBM Security Network IPS**는 네트워크내에 악의적인 행위를 차단
- **IBM Security Network Protection**는 어플리케이션에 대한 세세한 접근 통제 제공
- **IBM Security Privileged Identity Manager** 는 접근 정책을 강화
- **IBM InfoSphere Guardium EE**는 중요정보의 암호화 제공

다른 고려 사항들

- 중요 자산과 데이터에 포커스하고 추가적인 통제 구현
- 효과적인 DLP 전략 구현

Stage4: 탈취



1 침투

2 교두보

3 확장

4 수집

5 **탈취**

도전 과제

- 탈취한 데이터를 외부로 보내는 방법은 무궁무진함

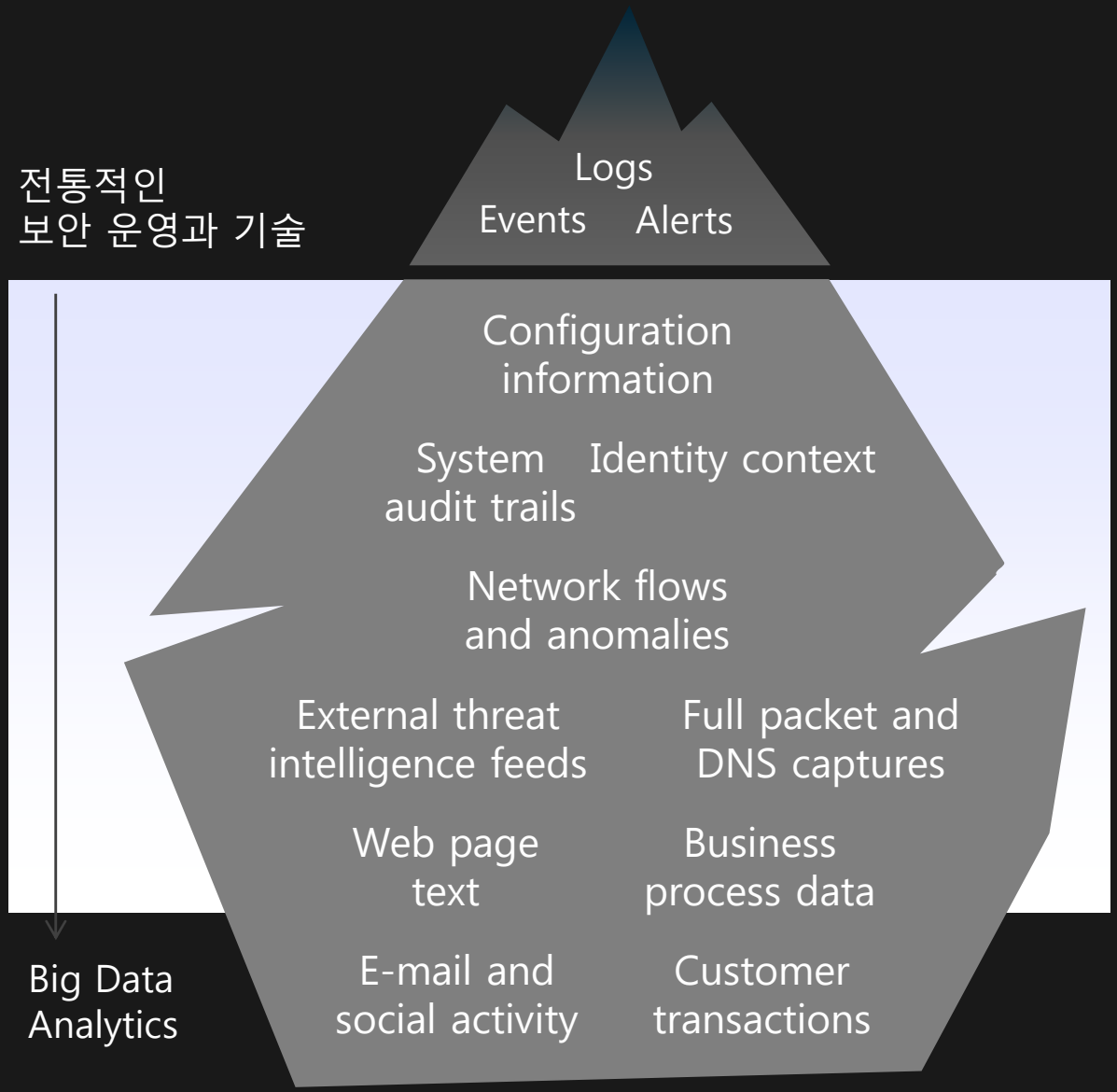
IBM 대응

- **IBM X-Force Threat Intelligence**는 악의적인 통신 차단을 돕는 악의적인 사이트를 인지합니다.
- **IBM Security QRadar**는 악의적인 사이트 접근을 탐지하기 위해 X-Force 데이터를 사용함. 또한, 전송 데이터양, 위치, 활동 타입에 기반으로한 비정상적인 사용자 행위를 탐지하는 학습 수행
- **IBM Security Network IPS**는 의심스러운 암호화 트래픽을 차단하며, 카드 데이터와 같은 민감한 데이터 전송을 차단함
- **IBM Security Network Protection**는 어플리케이션 통제를 통해 정책 강화 및 데이터 유출을 방지함

다른 고려 사항들

- 의심스러운 데이터 전송을 탐지하는 기능향상을 위해 Endpoint Protection, Network DLP 그리고 네트워크 보안 벤더와 협업

보안 인텔리전스 + Big Data



더 폭넓은 데이터로부터 깊은 통찰을 얻어 새로운 위협을 인지하고 보호하려는 욕구 증가

IBM의 보안 인텔리전스와 Big Data가 만남

1. 보안성 향상을 위해 다양한 데이터와 비정형화된 데이터를 분석
2. 보안 분석 추이와 포렌직을 위한 데이터 저장 양의 급격한 증가
3. 새로운 방식으로 데이터를 쿼리하고 표시함
4. 기존 보안 운영에 Big Data 분석을 통합

보안 인텔리전스 + Big Data

보안 인텔리전스 플랫폼

IBM Security QRadar

- 데이터 수집 및 농축
- 이벤트 상관분석
- 실시간 분석 및 아노말
- 오펜스 우선순위화

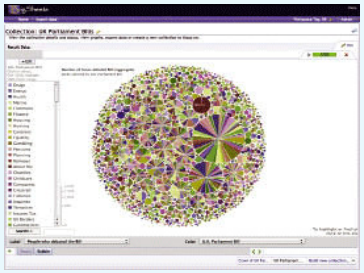
Radar

향상된 위협 감지

Data ingest

인사이트

Big Data 플랫폼



IBM InfoSphere BigInsights

- 하둡 기반
- 엔터프라이즈 등급
- 무제한 데이터/볼륨
- 데이터 마이닝
- Ad hoc 분석

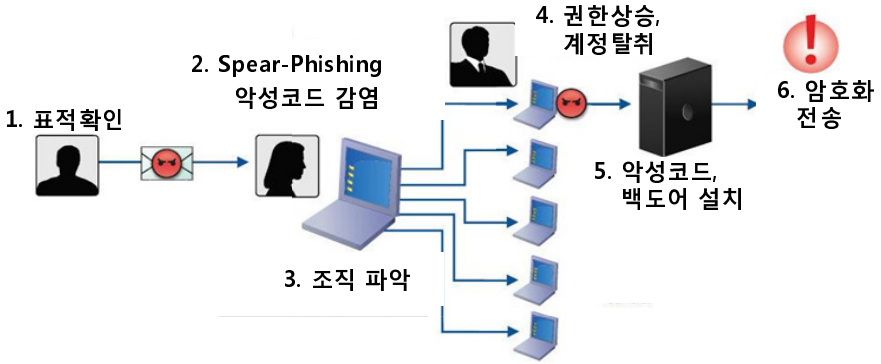
커스텀 분석

전통적인 데이터 소스

새로운 데이터 소스

포괄적 상관분석 - 시나리오 기반의 공격 탐지

▪ APT 공격 시나리오

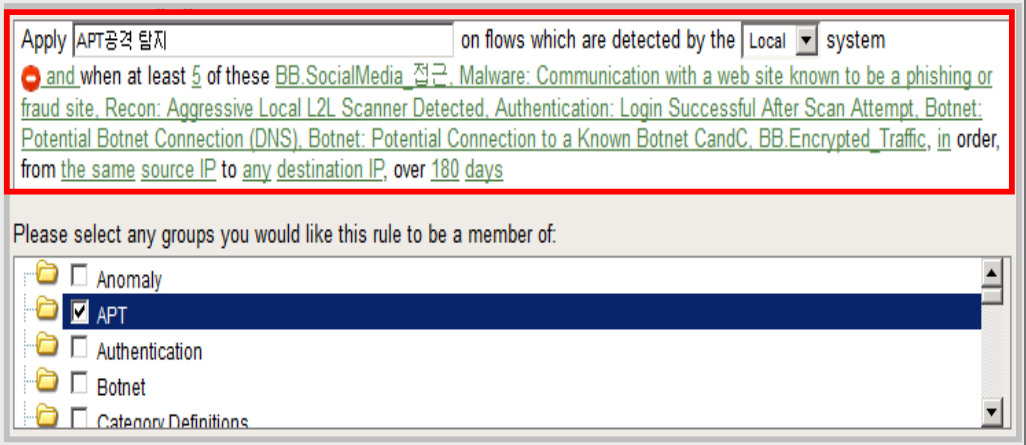


아래의 Activity들이 3개월에 걸쳐 수행됨

1. Social media를 통한 개인정보 유출
2. 악성코드 감염(피싱 사이트접속)
3. L2R로 SSH, IRC 접속 탐지 (non-standard port)
4. C&C Destination 탐지 및 위협 국가 접속 탐지
5. 로컬 호스트에 대한 스캐닝시도
6.. 접근 시도 (Brute Force Attack시도) 및 인증 성공
7. 수개월간 접속되지 않은 IP에서 접속 탐지
8. 백도어 설치 (Bot C&C 통신)
9. 암호화 전송 (Non-standard 포트 이용)

▪ APT 탐지 정책 (Event + Flow)

"When at least **this number** of these **rules**, **in|in any order**, from **the same|any source IP** to **the same|any destination IP**, over **this many seconds**"



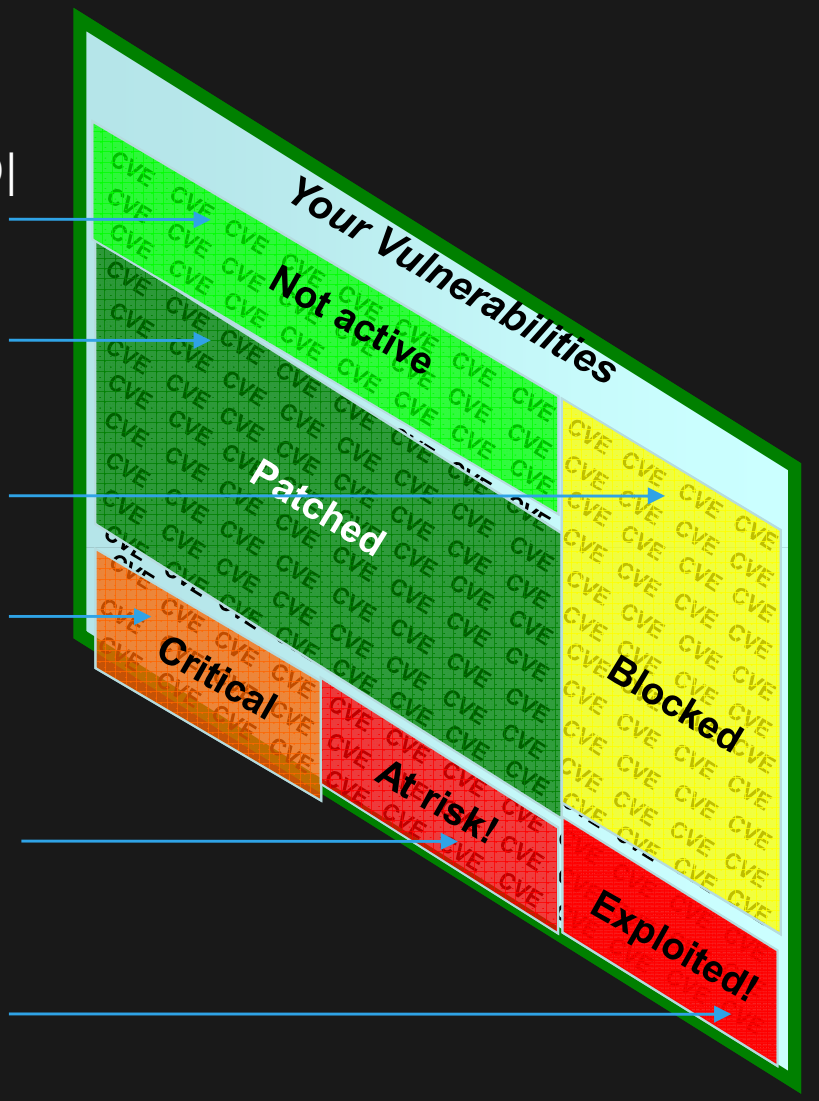
탐지조건:

Same IP에서 **Multi IP**로 **90일** 동안 **다음 활동 중 순서대로** 최소 **7개**가 만족할 때 탐지

- 소셜 사이트 접속, 피싱사이트 탐지, L2L Scan, 인증 3회 이상 실패 후 성공, IPS/IDS 탐지, Anomaly탐지, 알려진 BOT 서버 접속, 암호화 통신

QRadar Vulnerability Manager (QVM) - 보안 인텔리전스 기반의 취약점 관리체계

- **비활성**: Qflow와 협력하여, QVM은 취약한 어플리케이션이 기동되면 취약점 활성에 대해 알려줌.
- **패치 완료**: IBM Endpoint Manager와 협력하여, QVM은 어떤 취약점이 패치될 것인지 이해
- **차단**: QVM은 어떤 취약점이 방화벽과 침입방지솔루션에 의해 차단될 것인지 이해할 수 있음.
- **심각**: 취약점 지식 기반, 수정 flow와 QRM 정책과 협력하여, QVM은 비즈니스 핵심 취약점을 식별할 수 있다.
- **위험**: Qflow 네트워크 트래픽 가시성과 함께 X-Force 위협과 SIEM 보안 사고 데이터를 활용하여, QVM은 취약한 자산이 잠재적인 위협에 직면해 있는지를 파악할 수 있다.
- **공격**: SIEM 상관 분석과 침입방지솔루션 데이터를 활용하여, QVM은 어떤 취약점이 공격받고 있는지를 밝힐 수 있다.

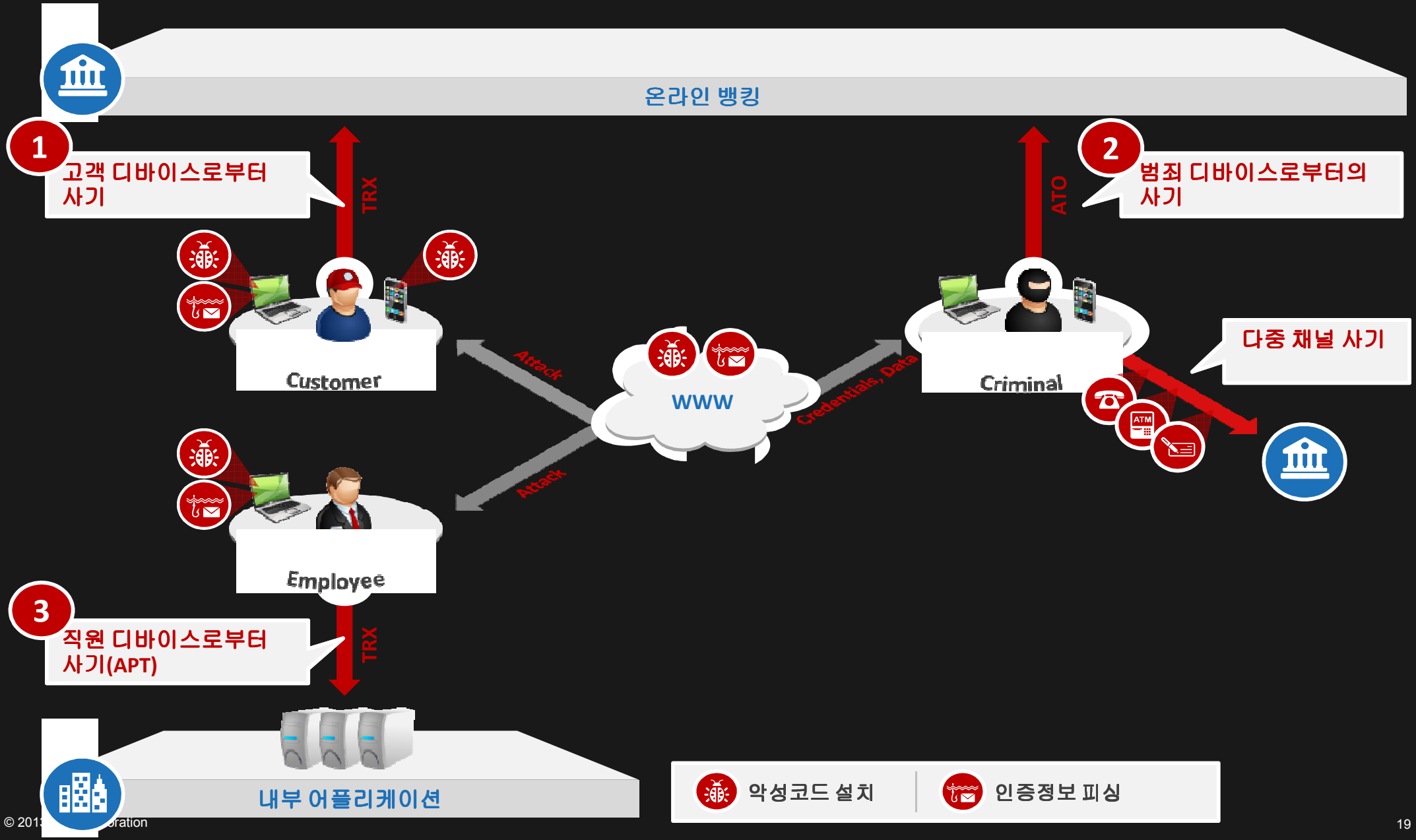


애플리케이션 가시성을 확보한 차세대 네트워크 통제

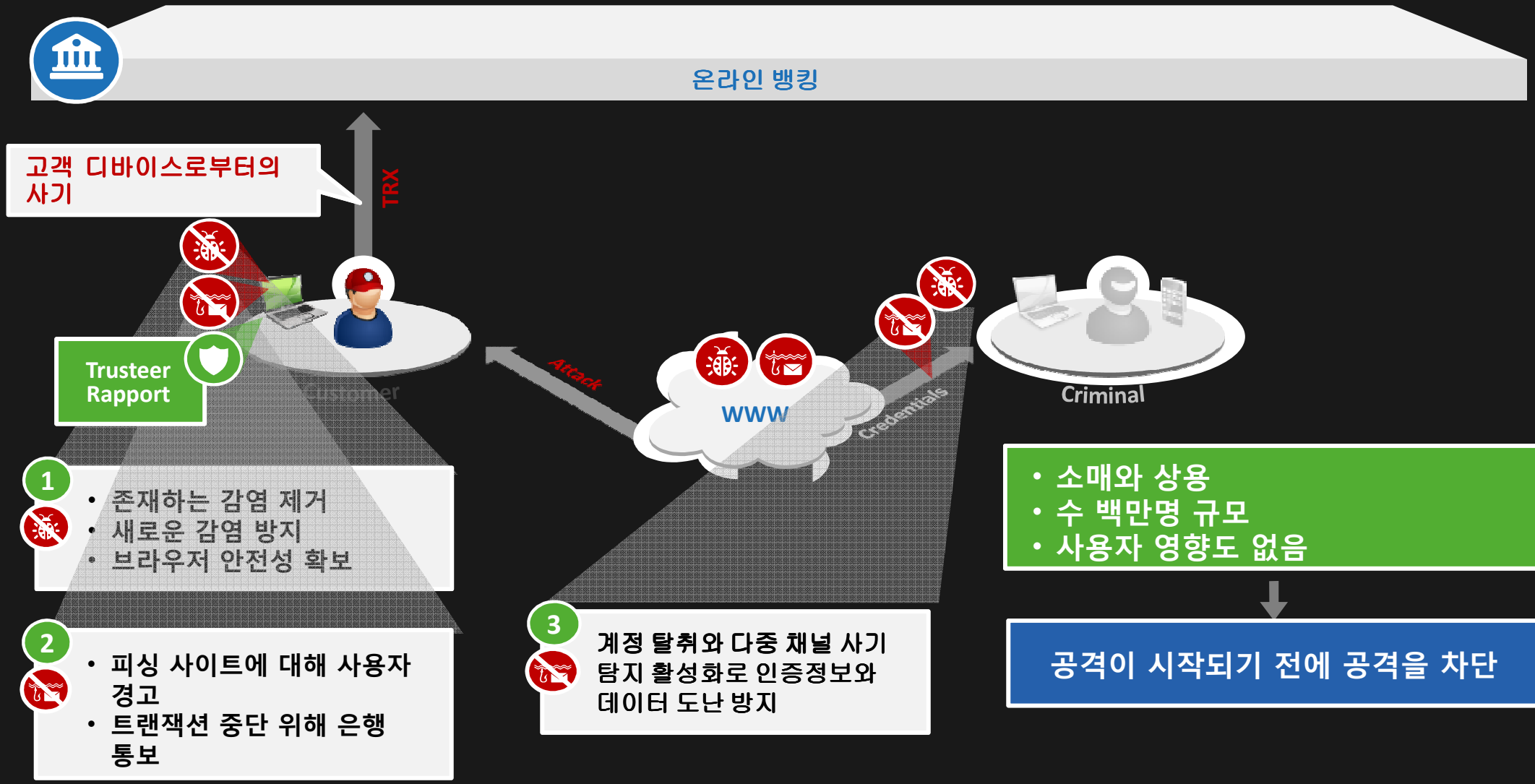
증명된 보안	XGS 궁극적인 가시성	XGS 완전한 통제
X-Force에 의해 공급된 확장된 제로데이 공격 방어	암호화 채널을 포함한 모든 네트워크 Activity에 대해 누가, 언제, 무엇을 했느냐에 대한 이해	어플리케이션과 네트워크 사용의 적절성을 판단

IBM Security Network Protection XGS Series
보안과 비즈니스 요구사항의 균형을 맞추기 위해 지금까지 증명된 방어 기능에 차세대 가시성과 통제 기능을 추가한 IBM의 차세대 침입방지 솔루션

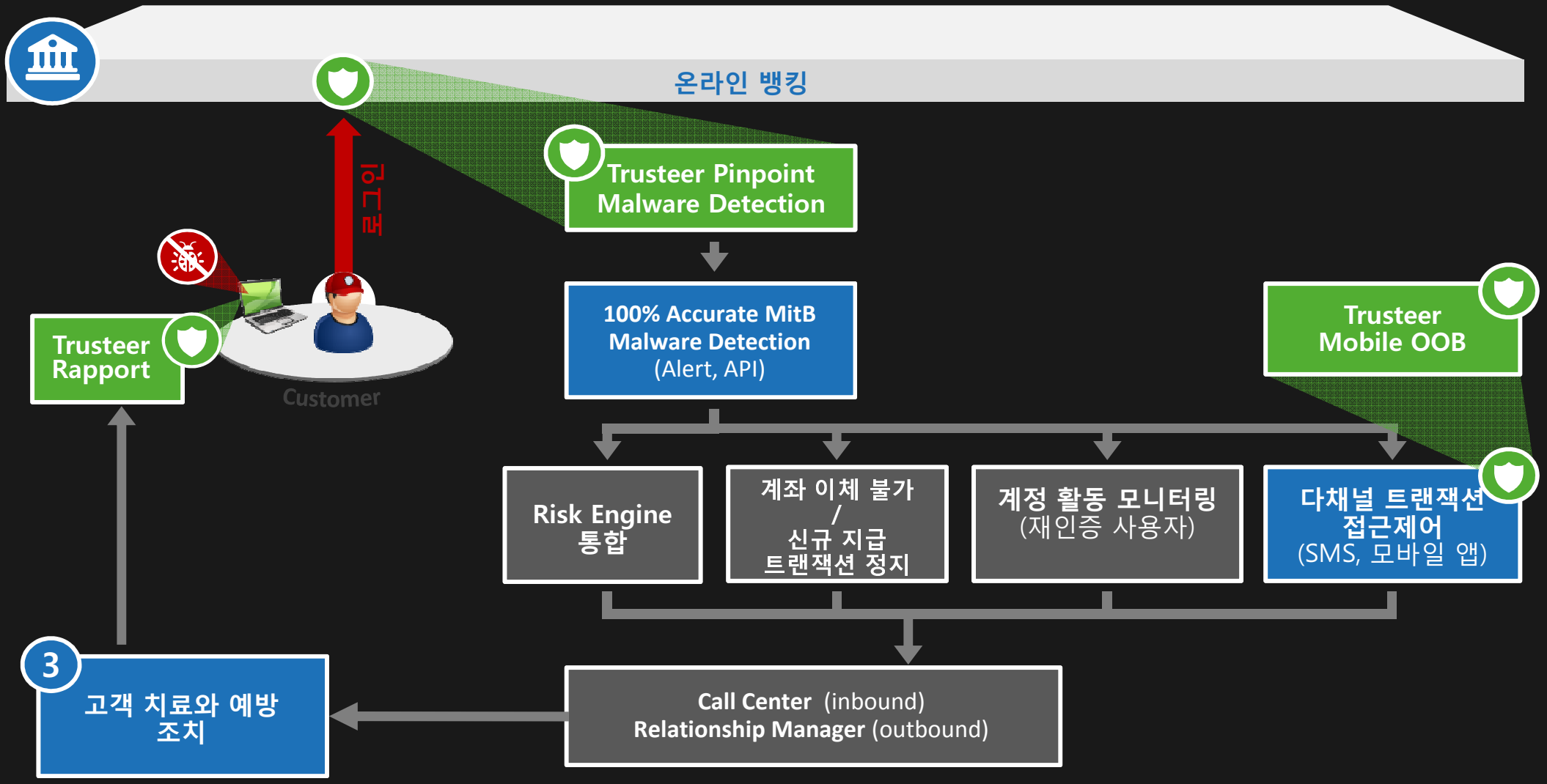
웹 / 금융 사기 문제


온라인 뱅킹
1
고객 디바이스로부터 사기
TRX
2
범죄 디바이스로부터의 사기
ATO
Customer
Attack
WWW
Credentials, Data
Criminal
다중 채널 사기
ATM
Attack
Employee
3
직원 디바이스로부터 사기(APT)
TRX
내부 어플리케이션
악성코드 설치
인증정보 피싱

고객 디바이스로부터의 사기 트랜잭션 방어(1)



고객 디바이스로부터의 사기 트랜잭션 방어(2)



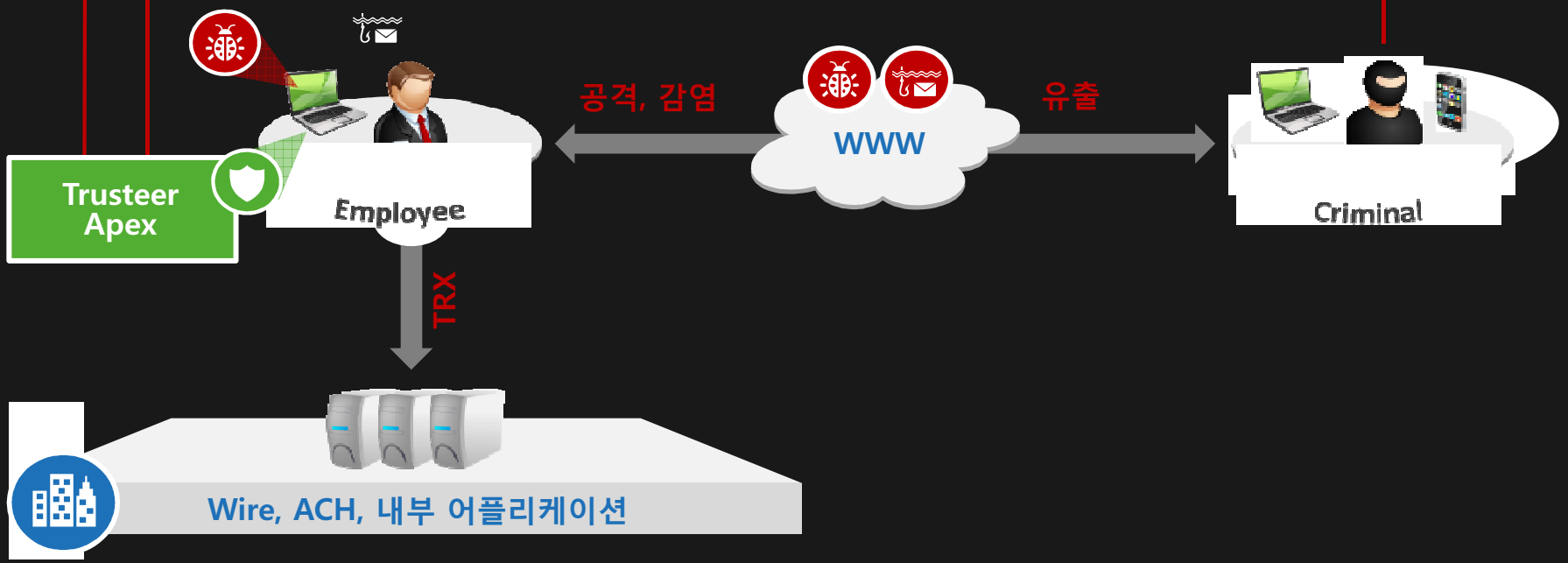
범죄 디바이스로부터의 사기 트랜잭션 방어

직원 엔드포인트 보호 – 엔드포인트 감염, 데이터 도난 방지

1 **어플리케이션 공격 방어**
취약점을 공격하는 악의적인 웹 사이트나 이메일 첨부파일에 의한 감염 중지

2 **데이터 유출 방지**
- 데이터 유출 기술을 사용하는 통신 프로세스 중지
- 키로깅에 의한 인증 정보에 대한 보호

3 **공격 중지:**
감염 없음
데이터 유출 없음.



www-01.ibm.com/software/kr/security/index.html

애플리케이션 | 무료 Hotmail | 연결 사용자 정의 | 웹 조각 갤러리 | 추천 사이트 | IE에서 가져온 북마크 | Firefox에서 가져온 ...

Korea | Na By

IBM 솔루션 서비스 제품 고객지원 & 다운로드 My IBM

IBM 소프트웨어 > Tivoli > 제품 >

IBM Security

→ IBM Security Virtual Conference 참여하기

보다 똑똑한 보안 | 최고 보안 경영자 | 솔루션 | 성공 사례 | 정보 및 자료 | 보안 관련 법 규제

보안 사고는 안전할 것이라는 믿음에서 시작됩니다. 지금 이 순간에도.

보안 사고가 발생하는 가장 큰 이유는 **'보안이 잘되고 있을 것'이라는 과신**에서 시작됩니다. 기업의 보안은 세계화가 가속화되고, 비즈니스와 커뮤니케이션이 확장되면서 더 큰 위협에 노출되고 있습니다.지켜야 할 기밀은 늘어나고, 막아야 할 위협은 늘어나기 때문입니다. 이제 **전통적인 방식의 보안은 안전성, 효율성, 경제성 측면에서 기업의 미래를 밝혀줄 수 없습니다.** 보다 스마트한 보안의 시작,**IBM Security와 함께 보안에 대한 새로운 접근법을 만나보세요.**

보이는 곳도, 보이지 않는 곳도 보안하는 스마트한 방법.

IBM 보안 프레임워크

IBM Security Framework의 목표는 보안 상태를 보다 효과적으로 평가할 수 있게 해주는 모범 사례와 공개 표준은 기반으로 보안 모델을 제공하고 성장을 지원하는 전사적인 보안 아키텍처를 효율적으로 구현할 수 있게 하는 것입니다.
IBM Security Framework를 사용하면 보안에 대한 구체적인 IT 구성 요소 및 IT서비스 이외의 포괄적인 비즈니스 솔루션을 개발할 수 있고, 모든 필요한 IT 보안 영역의 문제를 해결할 수 있습니다.

무엇을 도와드릴까요?

IBM 연락처

→ 견적서 요청

✉ 메일 보내기

또는 02-3781-7500
으로 전화하세요
Priority code:
109HH03W

똑똑한 세상의 바탕은 완벽한 보


IBM