

# 지능형 위협대응 자동화 및 디지털신뢰 확보 전략

윤영훈 상무

Apr. 24, 2019

# 기업의 정보보호 직면과제

## Cyber Threat Increased

**200**억개  
이상의 정보보호 대상

**50**억건  
개인정보 유출

향 후 2년간의 사이버 범죄를 통해

**6000**조원  
피해 예상

## Skill Shortage

2022년까지, CISO는  
**180만**  
사이버 보안 인력의  
부족사태에 직면

국내 기업의 60%가 매일  
**5000건 이상**  
위협 이벤트 탐지하고  
그 중 30%만 조치/대응

대응 건수의  
**84%**  
실제 위협이 아닌 것으로  
판명됨

기업 평균, 40개의 서로 다른  
벤더의  
**80종** 보안 솔루션 사용

국내 보안담당자의  
**92%**  
여러 협력업체 및 제품간  
협업/조율에 어려움을 겪음

## Advanced Threat

## Too Many Tools

# 보안 전문가들은 엄청난 양의 보안 지식을 생성하고 있으나 대부분의 지식은 활용되지 못하고 있음

## 전통적 보안 데이터

- 보안 이벤트와 경보
- 로그와 구성 데이터
- 사용자와 네트워크 활동
- 위협과 취약점 피드

## 사람이 생산한 지식



## 보안 지식의 세계 방어에는 활용되지 못하는 다크 데이터

전통적인 회사는 이 지식의 8%만을 활용함 \*

### 예시:

- 연구 논문
- 산업 발표
- 포렌식 정보
- 위협 인텔리전스 코멘트
- 컨퍼런스 프레젠테이션
- 분석가 보고서
- 웹페이지
- 위키
- 블로그
- 뉴스
- 뉴스레터
- 트위터

# 보안 관제 운영의 어려움

## 분석 데이터가 너무 많음

## 알려지지 않은 공격들

## 대응 능력 부족

Analysts are only able to keep up with about **8%** of the information needed to do their jobs

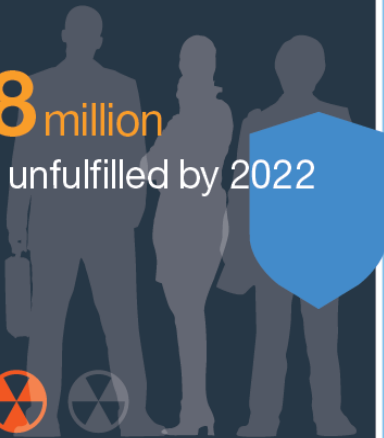


**93%** SOC managers are not able to triage all potential threats

**43%** of security professionals ignore a 'significant number of alerts'



**\$1.8 million** Jobs unfulfilled by 2022



“분석 대상 작업이 너무 많고 반복적임.”

“빠른 공격 대응을 위해 어디에 중점을 두어야할지 모르겠음.”

“분석 관련 정보가 너무 많고 유용한 정보를 찾기 힘들”



# CHANGE THE GAME WITH AI

AI를 활용한  
보안역량 강화

지능형  
위협 대응

Digital  
Identity Trust

# Journey to AI Security: Threat Management

인공지능의 SOC 적용: 인공지능이 자동으로 초동 분석을 수행하여 SOC팀이 더 효율적으로 관제업무를 수행하도록 도와 줍니다.



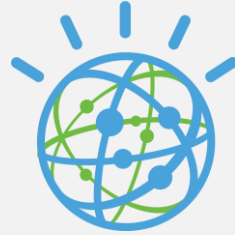
## QRadar 보안 인텔리전스 플랫폼

자동으로 Advisor에 오픈스(보안경보)를 전송



## QRadar Advisor

관련된 로컬 문맥을 수집하여 관찰 대상을 추출



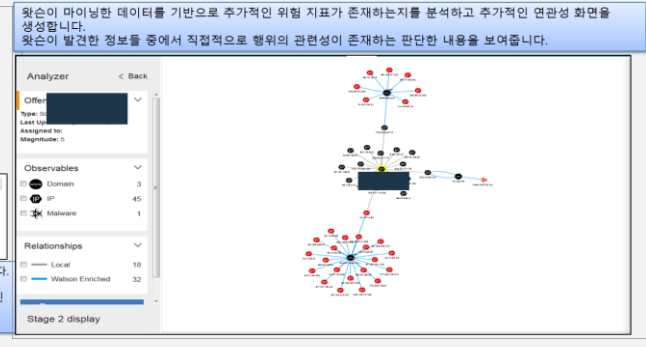
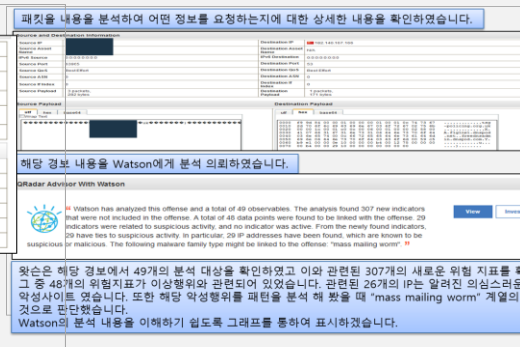
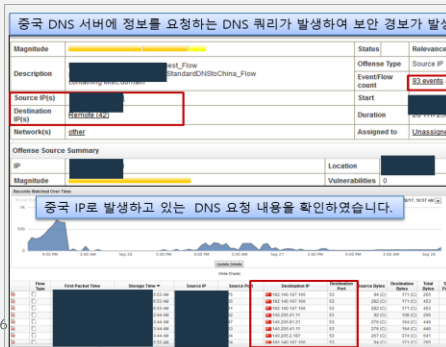
## Watson for Cyber Security

인공지능 분석을 사용하여 관련 외부 지식의 통찰력을 보안경보와 연결



## QRadar Advisor

신속한 판단/결정을 위한 피드백 및 상황정보를 제공



# Journey to AI Security: Threat Management

위협 분석 결과에 대한  
신뢰 수준

공격이 어떻게 발생하고  
진행되고 있는지 시각화

어떤 공격활동이 추가로  
발생 할 수 있는지 확인

1

Watson Investigations / ID: Offense 126

Key findings for  
**Source IP 192.168.0.119**  
Default | Investigated

Reinvestigate | Graph Relationships  
Last investigation 4 days ago, on October 4, 2018, 8:50 PM

**Key Insights**

Threat Actors	Malware Families	High Value Assets	Risky Users	Watched Users	Related Investigations	Duplicate Investigations
0	5	2	0	1	0	0

**Key Observables**

Total	Suspicious	Critical	New Local Context
65	44	35	4

Type	Description	Found Locally
	ee18e36bf1ct32fac9ee006931a7a912	Yes
	donni.smith	Yes
	3f118d0b888430ab9f58fc2589207988	Yes
	kyle.langford	Yes
	http://sandbox.bottiestore.com/765f46vb.exe	Yes
	NGM3450264505.js	Yes
	*_Locky_recover_instructions.bmp	Yes
	0beb1124cb82e4e1d37f43b5d711e5f	Yes
	_Locky_recover_instructions.bmp	Yes

**MITRE ATT&CK Tactics**

Credential Access  
31 observables

**Insights**

From this offense, Watson has analyzed 24 observables. The analysis found 73 new indicators that were not included in the offense. A total of 35 data points were found to be linked with the offense. 31 indicators were related to suspicious activity, and six indicators were active. From the newly found indicators, 25 have ties to suspicious activity. In particular, four files, 24 URLs, one domain name and two IP addresses have been found, which are known to be suspicious or malicious. The following malware family types might be linked to the offense: "icepack", "locky", "dridex", "spam zero-day", "emotet". The evidence is provided by "three anti-virus signatures". One user on a watch list is associated with the offense: kyle.langford. Advisor has identified one high value asset associated with the offense: 192.168.0.119.

Analysis of the indicators found by Watson revealed four additional observables related to the offense in the local context. Advisor has identified one additional high value asset related to the offense in the expanded local context: 192.168.0.122.

Offense Summary | View details

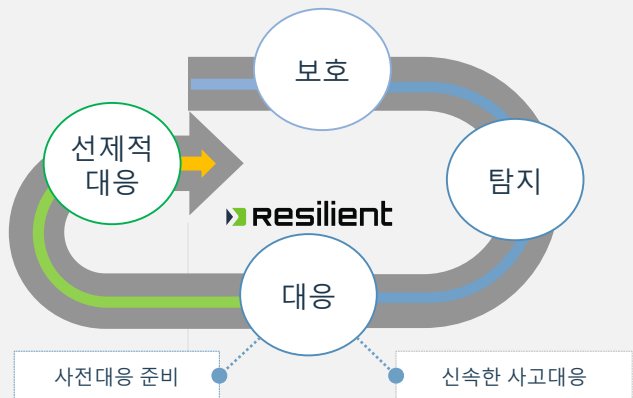
2

3

# Journey to AI Security: Threat Management

인공지능 분석 결과에 대한 대응: 프로세스 자동화 및 오케스트레이션

보안 사고 오케스트레이션과 대응 자동화 플랫폼을 통한  
빠른 대응으로 보안 사고의 피해를 최소화



- 사고 대응시간 단축
- 보안팀 유연한 권한 확보
- 자동화된 사고대응 프로세스

- 보안 사고대응 수준향상**
  - 산업규정 항목 정보제공
  - 정보유출 데이터 타입유형 정의
  - 글로벌 표준 정보보호 규정
- 자동화 프로세스 최적화**
  - 사고대응 업무단계 및 업무 기본 제공
  - 사고대응 유형별 변동사항 자동 업데이트
  - 시뮬레이션을 통해 최적 대응 프로세스 구축
- 보안 위협정보 자동분석**
  - 사고처리 대응가이드, 조건별 대응 항목표기
  - 정보유출 관련항목 정의
  - 포렌식, 사고 관련 근거정보 수집
- 중앙관리 환경 통합관리**
  - 보안사고 유형별 체크리스트 자동정의 및 할당
  - 처리담당 지정, 진척사항 점검, 대응 이력조회
  - 자동화 액션정의 (API연동 및 스크립트 적용 등)



## Before An Attack



- **Resilient** SOC가 사람, 프로세스 및 기술에 걸쳐 강력하고 자동화된 인시던트 대응 워크 플로우를 준비

- **QRadar** 사이버공격의 초기단계에서 위협과 이상행위를 식별

- **X-Force IRIS** 보안팀이 IR 플레이 북을 개발, 준비 및 훈련을 지원

## During An Attack



- 신속하고 종합적인 대응을 통해 보안 분석가를 안내하고 사건 조사 및 조치의 자동화

- QRadar Advisor w/Watson은 위협을 신속하게 조사하기 위해 인공 지능을 적용

- IR 전문가의 지원을 통한 팀 역량 강화

## After An Attack



- SOC가 IR 프로세스를 지속적으로 평가하고 개선

- 학습을 통하여 지속적으로 탐지 메커니즘을 조정/보완

- SOC가 사후 분석을 수행하고 IR 프로세스를 향상을 위한 지원

# Journey to AI Security: Digital Identity Trust

## 티몬페이 계정 도용 피해 '또' 발생, 피해 사례 속출

"친화번호 일게 변경 가능" vs 해킹 아닌 도용, 시스템 결함 아니다

주한선 기자 | oms@newsprime.co.kr | 2018.12.14 16:42:23

[프라임경제] 국내 대표 이커머스 업체인 티몬페이에서 발생한 것으로 알려진 "내 페이스북 계정유출 확인해보세요"...한국 3만여개 유출

간편결제 시스템인 '티몬페이'를 내세우고 있지만, 별다른 보안 대책이 없다는 지적이다.

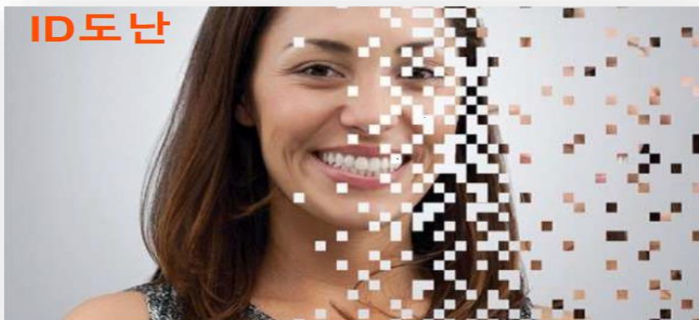
14일 한 온라인 커뮤니티에 "내 페이스북, 14일 당혹스러웠다"는 글이 올라왔다.

작성자가 A씨는 "처음 전세 상품권을 구입한 내역을 되짚어볼 때 불가능하다는 메시지가 떴다"고 밝혔다.

A씨의 글은 현재 삭제된 후 올라오고 있는 상황.

티몬, 계정 해킹, 개인정보 유출, 금융 기관, 사용자 정보, 해킹, 계정 도용, 금융 기관, 사용자 정보, 해킹, 계정 도용, 금융 기관, 사용자 정보

최근 A 한국인 사용자 정보 관리



- 도난된 실제 사용자 정보
- 계정이 탈취된 개인 및 금융 기관

Impact

41%

신규 계정 생성 사기가 탈취된 실제 사용자 정보 사용

## 세련·경교해진 피싱 공격, 기업 계정 타겟 '집중포화'

11월 1: 2018-09-07 15:25

#피싱 #인텔 #ASEC #계정정보

## 조작된 ID



- 조작된 가상의 사용자 정보
- 계정이 사용되는 금융 기관

27%

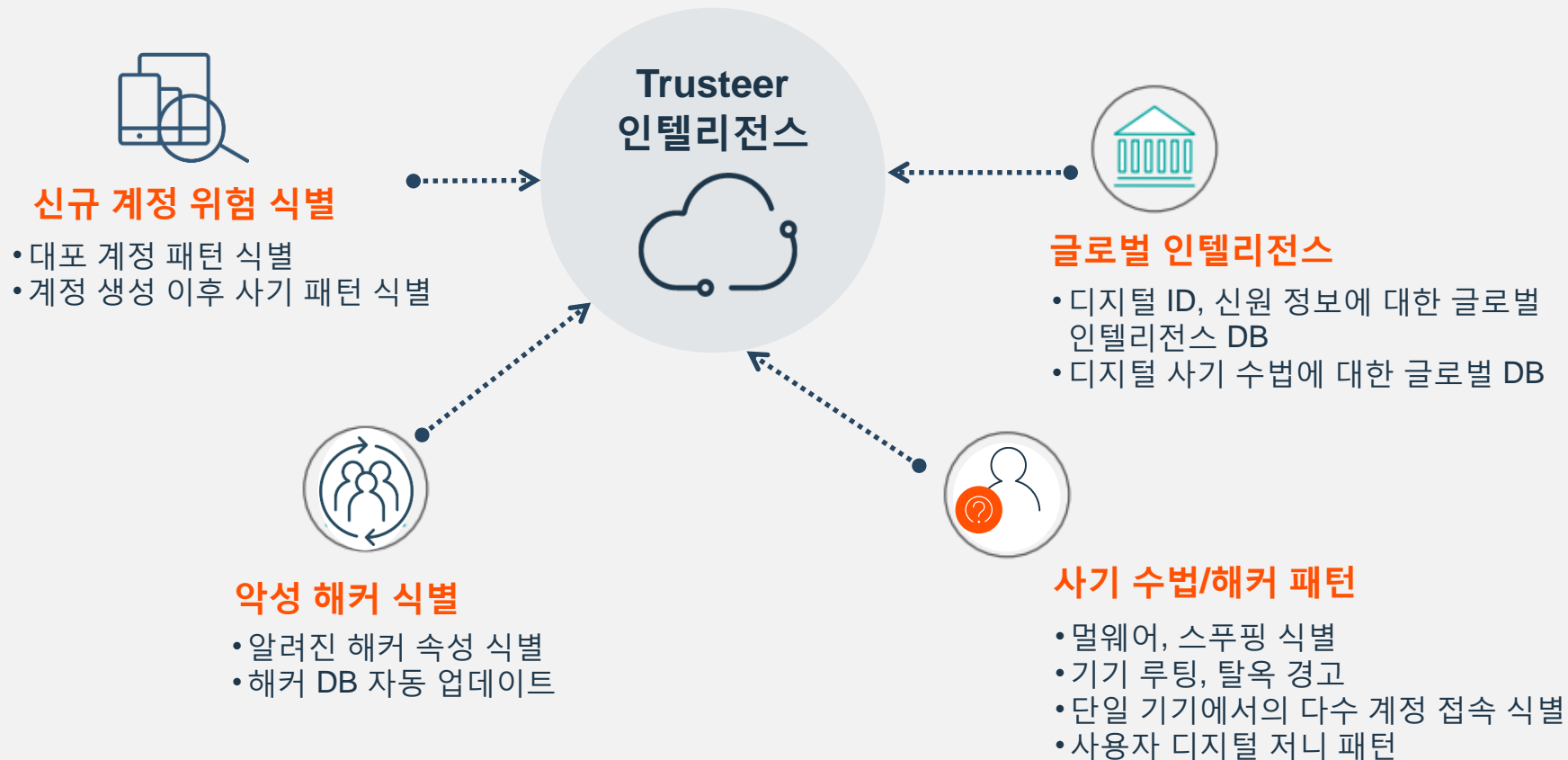
신규 계정 생성 사기가 탈취된 일부 사용자 정보 기반 조작

# 디지털 신뢰성 (Digital Identity Trust)

*the key to customer relationships in the digital age*



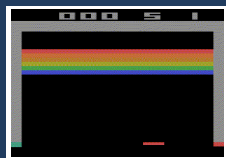
# 다양한 인텔리전스 기반 통합 분석



# AI 기술의 적대적 활용

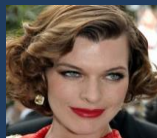
## AI 활용 공격

- **Generate:** SQL injection을 학습한 DeepHack tool [DEFCON'17]
- **Automate:** 트위터에서 표적공격의 생성 [Zerofox Blackhat'16]
- **Refine:** 신경망으로 무장한 비밀번호 크래커



## AI 자체를 공격

- **Poison:** 트위터를 통해 Microsoft Tay chatbot 이 중독됨 [Po]
- **Evade:** 안면 생체 인식을 위한 컴퓨터 비전에 대한 직접 공격 [CCS'16] [Ev]
- **Harden:** 맬웨어 탐지기를 피하는 유전 알고리즘 및 강화 학습 (OpenAI Gym) [Blackhat/DEFCON'17] [Ev]



## Theft of AI

- **Theft:** 공개 API를 통해 기계 학습 모델 탈취 [USENIX'16] [DE]
- **Transferability:** 실용적인 블랙박스 공격은 전송 공격에 대한 대리 모델을 학습 [ASIACCS'17] [ME, Ev]
- **Privacy:** 모델 역 공격은 학습 데이터를 탈취 [CCS'15] [DE]



**ME:** Model Extraction  
**DE:** Data Extraction

**Ev:** Model Evasion  
**Po:** Model Poisoning

# Cyber Security에서 AI의 활용 영역

## 예측 분석

- **접근방법:** 행동특성 모델링 및 새로운 또는 과거의 위협과 위험을 식별
- **Applications:** 네트워크 정보, 사용자 정보, endpoint, 어플리케이션 데이터 및 클라우드 데이터



## 분석 능력 강화

- **접근 방법:** 위협정보를 분류하여 전달하고 상황에 따른 판단
- **Applications:** Structured and unstructured (NLP) 데이터



## 협업 및 대응

- **접근 방법:** 보안 이벤트가 발생한 원인 및 대응 방안 제공
- **Applications:** Cognitive SOC 분석가, Orchestration, 자동화



# 결론: AI를 어떻게 이해/활용할 것인가?

대학생2명 + 노트북3대



체스전용 슈퍼컴, 하이드라









체스 챔피언  
게리 카스파로프



딥블루

# THANK YOU

## FOLLOW US ON:

-  [ibm.com/security](https://ibm.com/security)
-  [securityintelligence.com](https://securityintelligence.com)
-  [ibm.com/security/community](https://ibm.com/security/community)
-  [xforce.ibmcloud.com](https://xforce.ibmcloud.com)
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  [youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2019. 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. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. 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.

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, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, 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 any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.