

IBM의 AI기반 보안 솔루션

—

나병준 실장/CISSP
한국IBM

IBM Security

IBM

IBM Watson의 기초



What is WATSON ?

- 인간의 뇌를 닮은 컴퓨팅 기술에 기반
- IBM WATSON은 인간의 뇌와 같이 학습하고 이해하며, 인간과 상호작용을 통해 계속 진화하며, 추론과 학습까지 할 수 있는 컴퓨팅 기술이 적용되어 있음.



Understand : 인간의 언어로 상호작용

자연어 이해 와 음성인식, 이미지 인식, 시각화 기술 등 인간의 방식으로 오늘날 존재하는 데이터의 약 80 %를 차지하는 비정형 데이터로 부터 데이터간의 상호작용을 이해

Reason : 전문지식으로 의사결정 향상

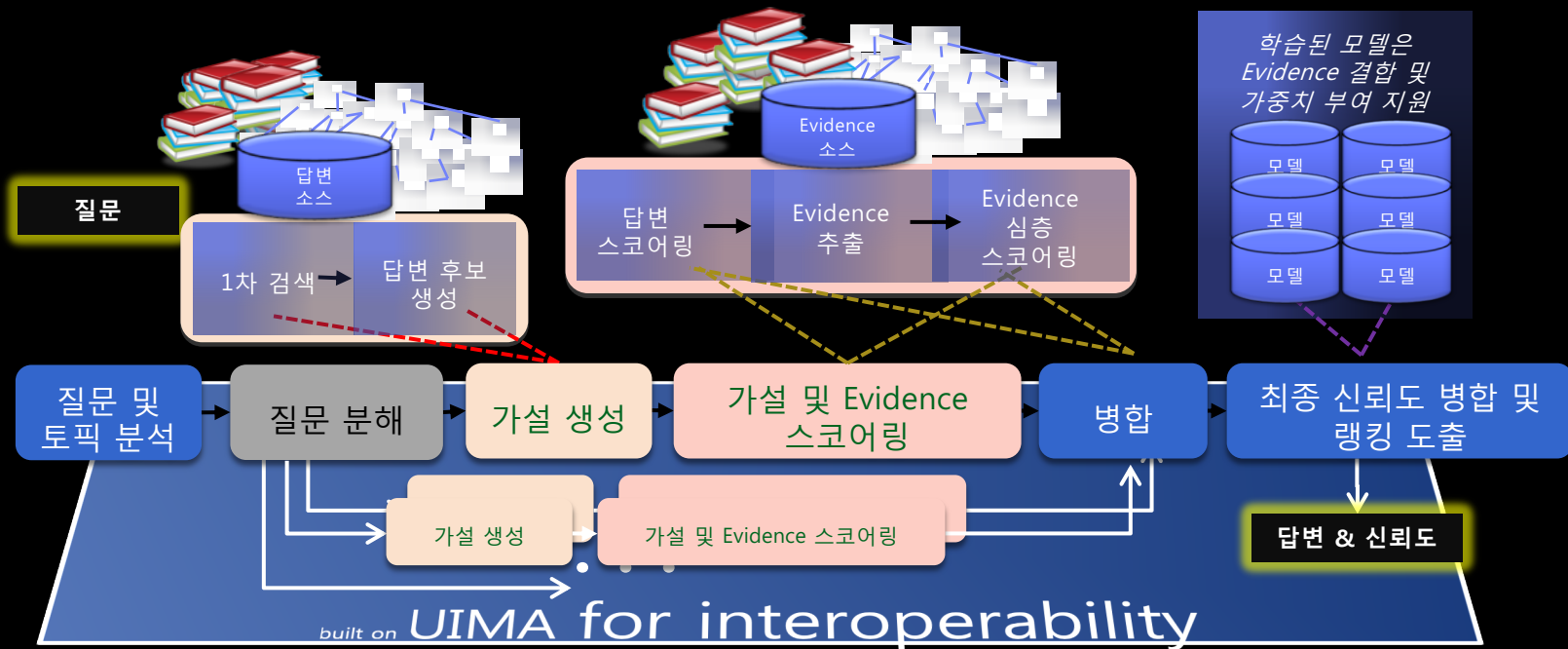
질문을하면, 가설의 생성하고 이를 기반으로 전문분야 데이터로 부터 평가 및 분석하여, 여러 해답 후보를 확실성과 함께 제공하여, 최적의 의사결정을 지원

Learn : 인공지능과 기계학습의 결합

사용자의 피드백을 추적하고 성공 및 실패 모든 상황으로 부터 감지하고 예측하고, 생각할 수 있도록 인공지능과 기계학습을 통해 훈련되는 학습 시스템 으로 이용을 할 수록 똑똑해 짐

DeepQA 아키텍처

DeepQA는 NLP, 머신러닝 및 추론 알고리즘을 사용하여 수많은 가설을 생성하고 스코어링



왓슨과 보안

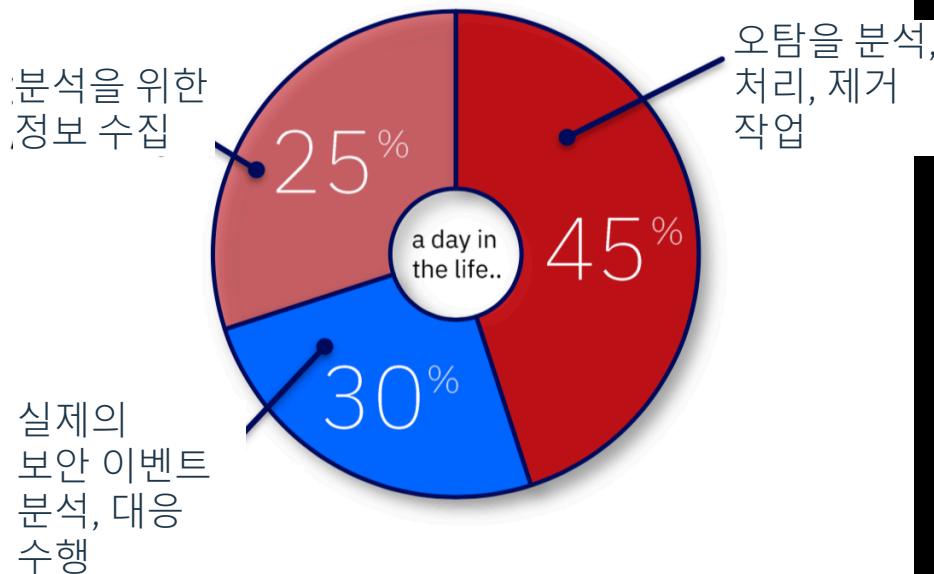


IBM Security

IBM

보안 관제 인력/분석가의 하루 작업 중 실제 비즈니스와 직접 관련이 없는 작업 비율

70%



Think 2018 / 8126 / March 22, 2018 / © 2018 IBM Corporation

Sources:

https://www.arbornetworks.com/images/documents/White%20Papers%20and%20Research/WP_SecurityAutomation_EN.pdf
<https://www.securitymagazine.com/articles/87601-duplicate-alerts-draining-security-analysts-time>
<https://www.novetta.com/2015/04/70-of-a-security-analysts-day-is-a-waste-of-time/>

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 *

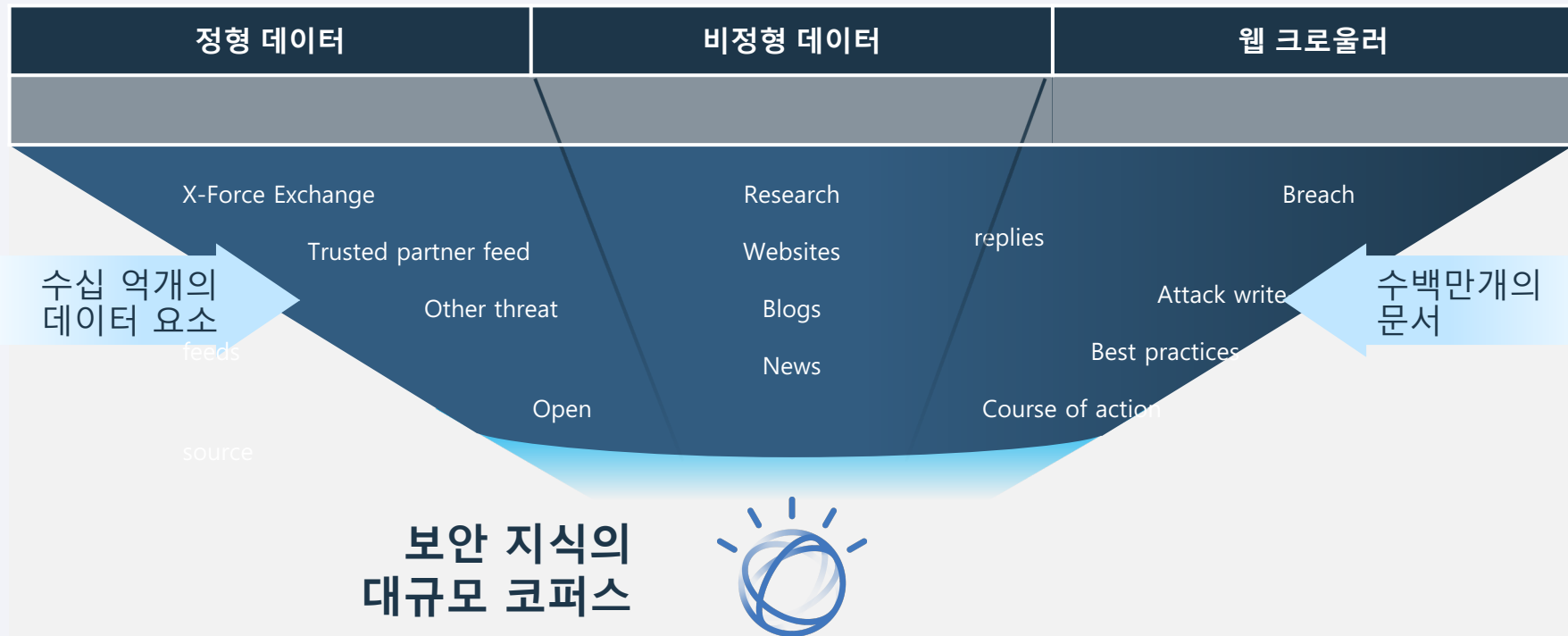
예시:

- 연구 논문
- 산업 발표
- 포렌식 정보
- 위협 인텔리전스 코멘트

- 컨퍼런스 프레젠테이션
- 분석가 보고서
- 웹페이지
- 위키
- 블로그

- 뉴스
- 뉴스레터
- 트위터

Watson for Cyber Security의 운영 형태



100+ customers
140K+ web visits in 5 weeks
200+ trial requests

SEE THE BIG PICTURE

"QRadar Advisor enables us to truly understand our risk and the needed actions to mitigate a threat."



ACT WITH SPEED & CONFIDENCE

"The QRadar Advisor results in the enhanced context graph is a BIG savings in time versus manual research."



IBM Cognitive SOC

보안장비/엔드포인트

네트워크 행위

데이터

사용자 및 인증 정보

위협 정보

설정 내역

취약점 및 위협

어플리케이션 내용

클라우드 사용 정보

○ 내부자 위협

○ 외부 위협

○ 클라우드 위협

○ 취약점

○ 중요 데이터

이벤트 인지

새로운 분석 대상
간편한 추가

위협 탐지

머신 러닝 & 실시간
상관분석

고객환경을
고려한 분석을
통한 새로운 위협
확인

전문가 분석

AI를 활용한
위협 분석 및
추론

SME에 의한
심층 분석/
위협 헌팅

행동

자동화된 조치 및
협업

SOC에 대한 인공지능 적용



인공지능이 자동으로 초동 분석을 수행하여 SOC팀이 루틴작업에서 해방되도록 합니다.



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
데이터의 인사이트를
오픈스에 추가



QRadar Advisor

인공지능 분석을
사용하여 관련 외부
데이터의 통찰력을
오픈스에 추가

QRAW 데이터 해석 stage

Analyzer < Back

Assigned to:
Magnitude: 3

Observables

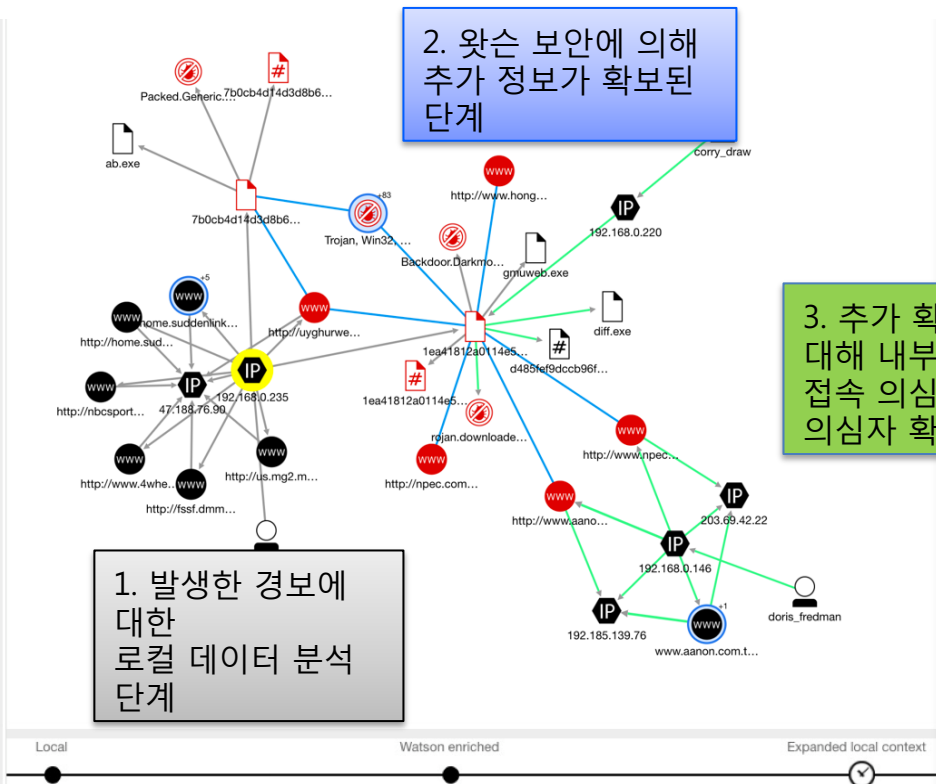
- ☐ AV Signature 3
- ☐ Domain 3
- ☐ File 3
- ☐ Hash 1
- ☐ IP 25
- ☐ Malware 3
- ☐ URL 3

Relationships

- ☐ Local 7
- ☐ Watson enriched 52
- ☐ Expanded local context 5

Export view to STIX

Key insights only ☒



3. 추가 확보된 정보에 대해 내부 추가 감염, 접속 의심, 이상 행위 의심자 확보 단계

QRadar Advisor 주요 기능



인시던트를 ATT&CK 프레임워크에 맞춤

위협을 확인하는 개별
진행에 대한 확신
레벨을 제공

1

공격이 어떻게
발생하여 진행되고
있는지 시각화

2

어떤 공격 전술이
추가로 발생할
가능성이 있는지 확인

3

Watson Investigations / ID: Offense 126

Source IP 192.168.0.119

Default | Investigated

Reinvestigate Graph Relationships

Last investigation 4 days ago, on October 4, 2018, 8:59 PM

Current Medium

Key Findings for

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

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.

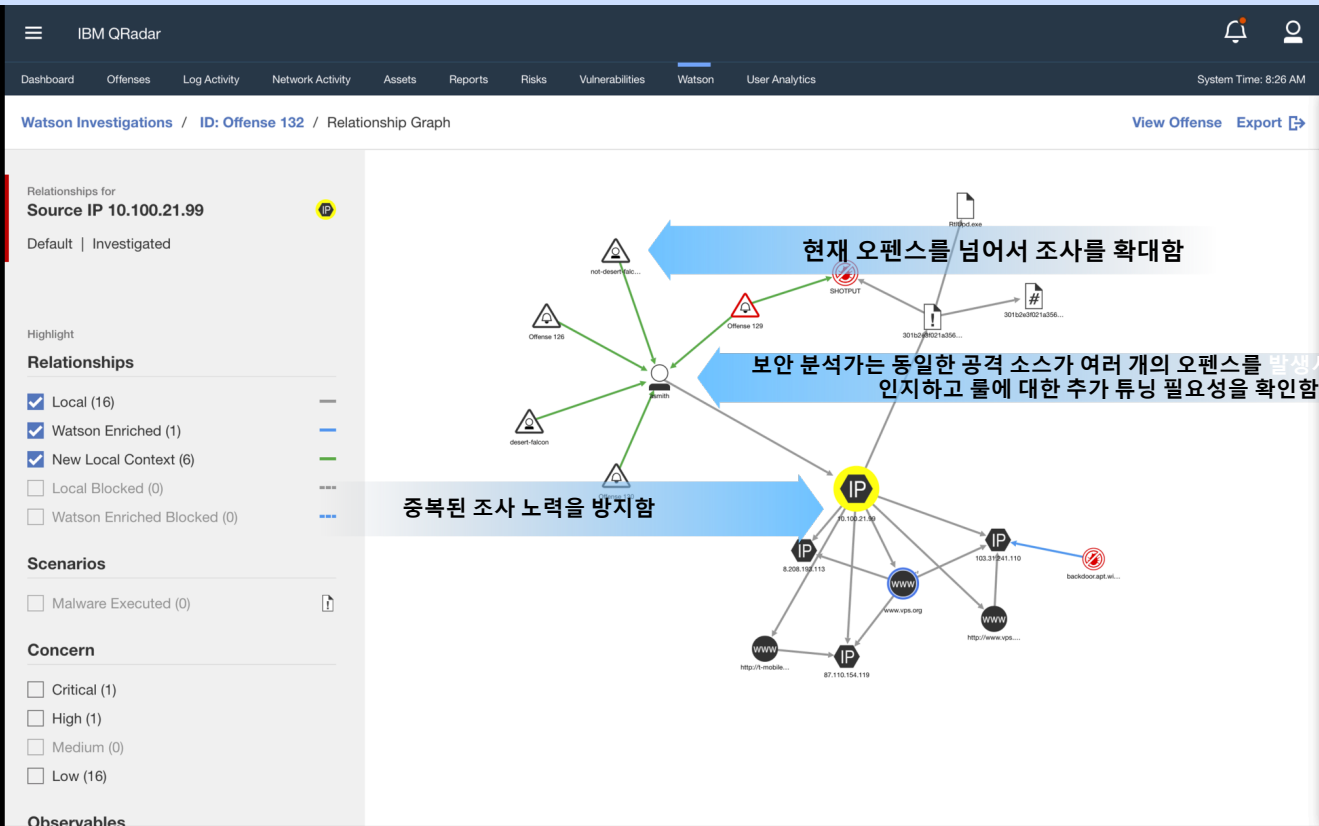
Analysis of the indicators found by Watson revealed four additional observables related to the offense in the local context. Advisor has identified one additional high value asset related to the offense in the expanded local context: 192.168.0.122.

Offense Summary View details

Type	Description	Found Locally
File	ee18e36bf1cf32fac9ee006931a7a912	Yes
User	donni.smith	Yes
File	3f118d0b888430ab9f58fc2589207988	Yes
User	kyle.langford	Yes
URL	http://sandbox.bottlestore.com/765f46vb.exe	Yes
File	NGM3450264505.js	Yes
File	._Locky_recover_instructions.bmp	Yes
File	0beb1124cbe82e4e1d3f743b5d711e5f	Yes
File	._Locky_recover_instructions.bmp	Yes

작동방식 - 교차-조사 분석

QRadar Advisor는 연결된 관찰 항목을 통해 조사를 자동으로 연결함



현재 오픈스를 넘어서 조사를 확대함

보안 분석가는 동일한 공격 소스가 여러 개의 오픈스를 발생시켰다는 것을 인지하고 룰에 대한 추가 튜닝 필요성을 확인함

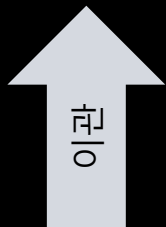
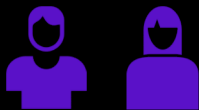
중복된 조사 노력을 방지함

작동방식- 오펜스 처리 분석

학습

Tier 2 분석가

심층 조사; 사고 대응



Tier 1 분석가

첫번째 선별 ; 정보 수집 및 Tier 2로 이관



적용

오펜스
#152

Advisor 권고:
이 조사는 우선 순위에서
해제되었음.

Offense # 152는 Offense # 29,
53 및 # 112와 유사함.이
모든 것은 과거에 오탐으로
처리되었음.

오펜스
#221

Advisor 권고:
이 조사는 이관되었음.

Offense # 221은 과거에
이관된 Offense # 42 및 #
68과 유사함.

오픈스 우선 순위 AI 모델 - 예시

Watson Investigations Last updated a few seconds ago ↻

Investigated offenses		High priority		Low priority		Evaluations needed		Investigated searches	
7		3		3		3		0	
<input type="checkbox"/>	Evaluation ⓘ ↓	ID	Source	Suspicious Observables ⓘ		Domain	Last Investigation	Status	
<input type="checkbox"/>	High priority ⓘ	Offense 1416	frank_sanchez Username	83 of 97		Domain 1 USA Event Collector	5 hours ago	Investigated	
<input type="checkbox"/>	High priority ⓘ	Offense 1419	kyle.langford Username	5 of 8		Domain 1 USA Event Collector	5 hours ago	Investigated	
<input type="checkbox"/>	High priority ⓘ	Offense 1406	Celino_Espinoza Username	12 of 19		Domain 1 USA Event Collector	4 days ago	Investigated	
<input type="checkbox"/>	Low priority	Offense 1403	Dan_Goldman Username	5 of 9		Domain 1 USA Event Collector	5 hours ago	Investigated	
<input type="checkbox"/>	Low priority	Offense 1410	lance.springwell Username	1 of 8		Domain 1 USA Event Collector	4 days ago	Investigated	
<input type="checkbox"/>	Low priority	Offense 1407	192.168.107.107 Source IP	0 of 11		Domain 1 USA Event Collector	a month ago	Investigated	

SOC에 대한 인공지능 도입 가치



AI 적용에 따른 TEI(Total Economic Impact) 예시

정량적 이익



SOC 분석가의 업무 비용을 1.8M\$(약 20억원) 절약함

- 수동으로 진행한 위협 분석을 자동화 : 평균 4시간 걸리던 작업을 20분으로 단축
- 기존 SOC 분석의 시간을 50% 이상 절약하여 proactive 업무에 사용
- SOC Level1 업무를 NOC로 이관할 수 있어서 SOC 추가 고용 안함



분석을 아웃소싱하던 것을 인하우스로 변경하여 126,829\$(약 1억3천만원) 절약함

- QRAW이전에는 업무 과중으로 L2/L3 분석 업무를 아웃소싱하였음
- SOC 효율성 증대로 시니어 SOC분석가가 해당 업무를 인하우스로 처리 가능해짐



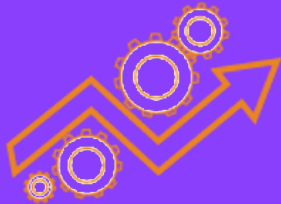
조직 보안성 증가로 651,936\$(약 7억원) 효과 얻음

- 평균 분석 시간 감소와 NOC인력을 L1조사로 활용하여, 조사대상 기업이 연간 분석하는 개수가 1,800개에서 7,000개로 증가함 (기존에는 분석이 안되거나 대응이 안되고 있었음)
- 증가한 분석수로 인해 심각한 보안 사고가 8% 감소

AI 기반 위협 탐지 및 분석의 이익&효과

보안 운영 팀의 노력이
배가 됨

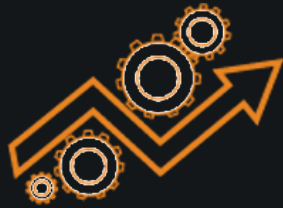
- 반복적인 SOC작업의
자동화



AI 기반 위협 탐지 및 분석의 이익&효과

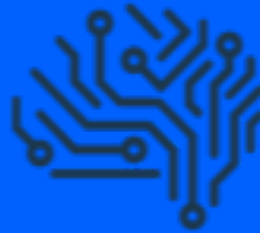
보안 운영 팀의 노력이
배가 됨

- 반복적인 SOC작업의
자동화



일관되고 더 자세한 조
사 및 분석을 수행함

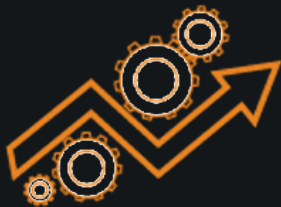
- 중요한 보안 사건에
대해 실행 가능한 통
찰력을 확보



AI 기반 위협 탐지 및 분석의 이익&효과

보안 운영 팀의 노력이
배가 됨

- 반복적인 SOC작업의
자동화



일관되고 더 자세한 조
사 및 분석을 수행함

- 중요한 보안 사건에
대해 실행 가능한 통
찰력을 확보



휴지 시간을 단축시킴

- 보다 신속하고 결정
적인 에스컬레이션
프로세스 채택



Thank you

—

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

[@ibmsecurity](https://twitter.com/ibmsecurity)

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.

