IBM의 AI기반 보안 솔루션

나병준 실장/CISSP
한국IBM

IBM **Security**

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

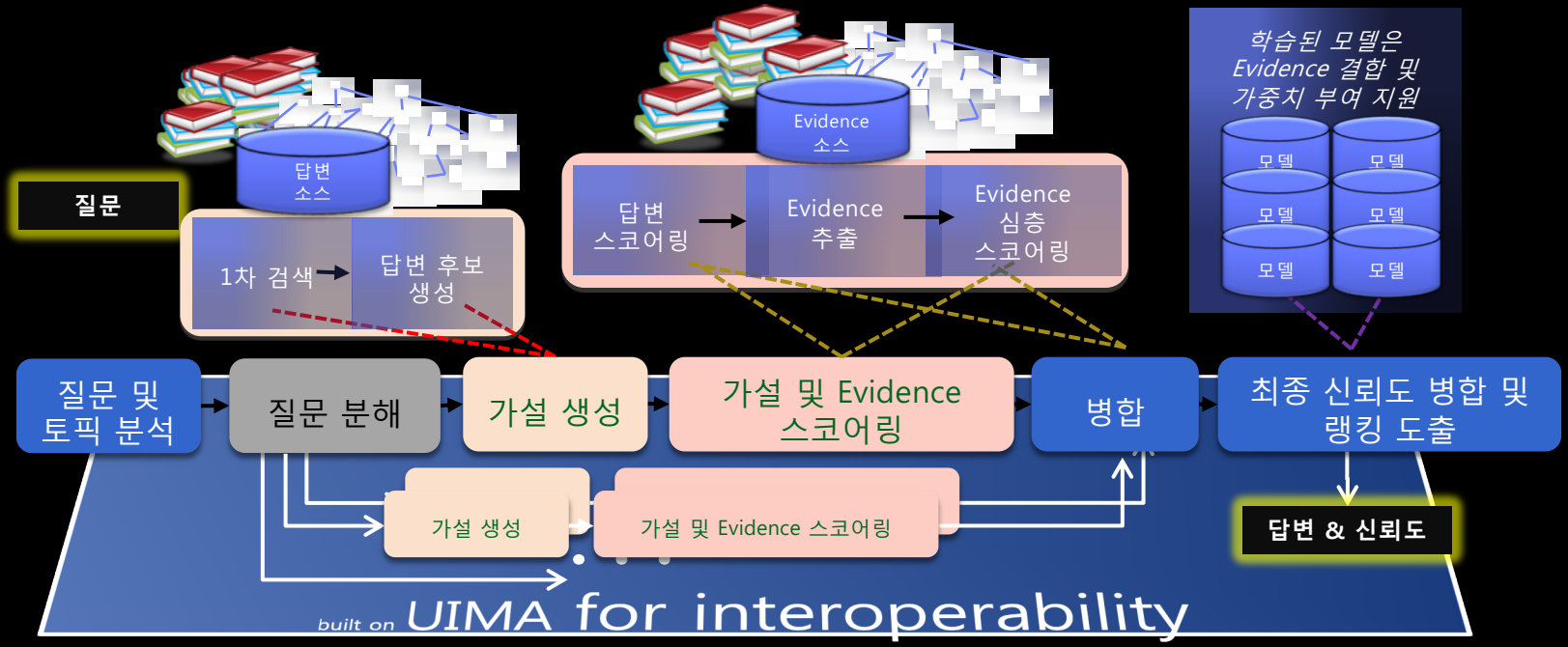
질문을하면, 가설의 생성하고 이를 기반으로 전문분야 데이터로 부터 평가 및 분석하여, 여러 해답 후보를 확실성과 함께 제공하여, 최적의 의사결정을 지원

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

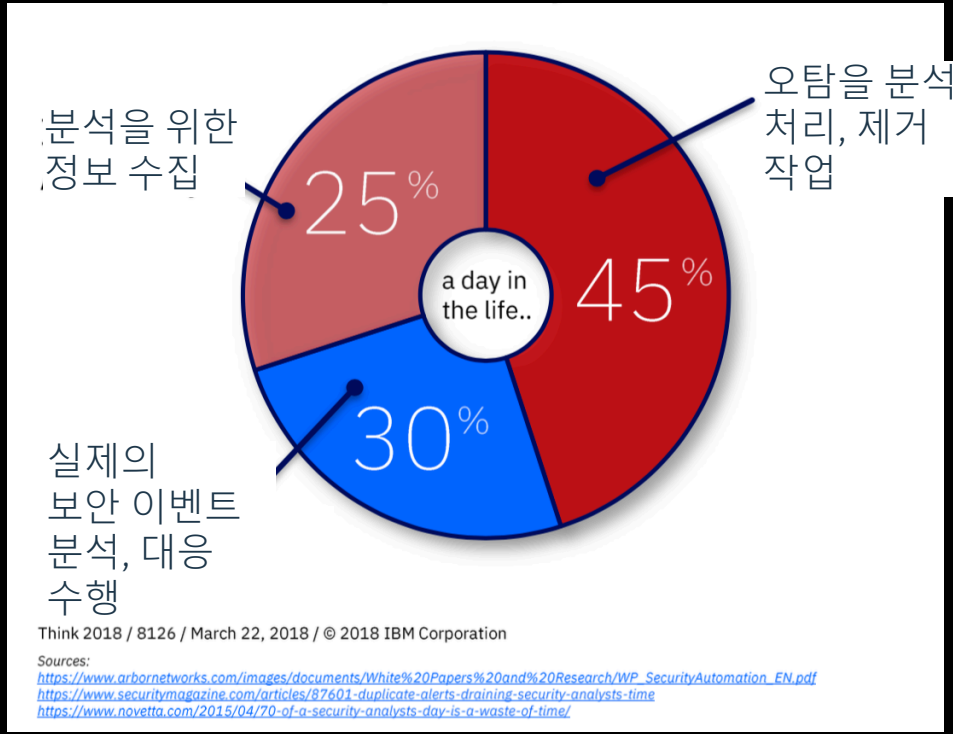
DeepQA는 NLP, 머신러닝 및 추론 알고리즘을 사용하여 수많은 가설을 생성하고 스코어링



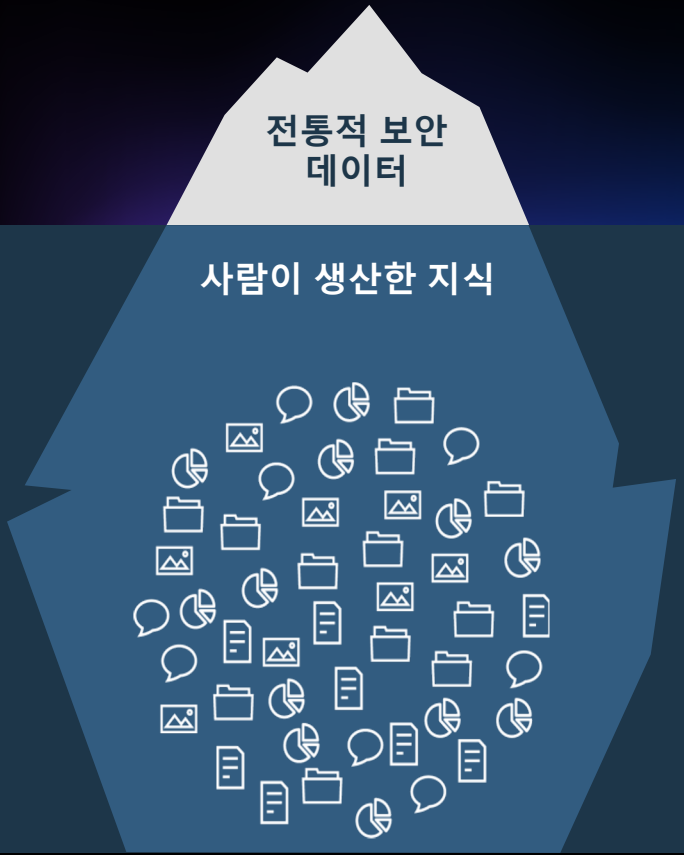
왓슨과 보안

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

70%



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



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

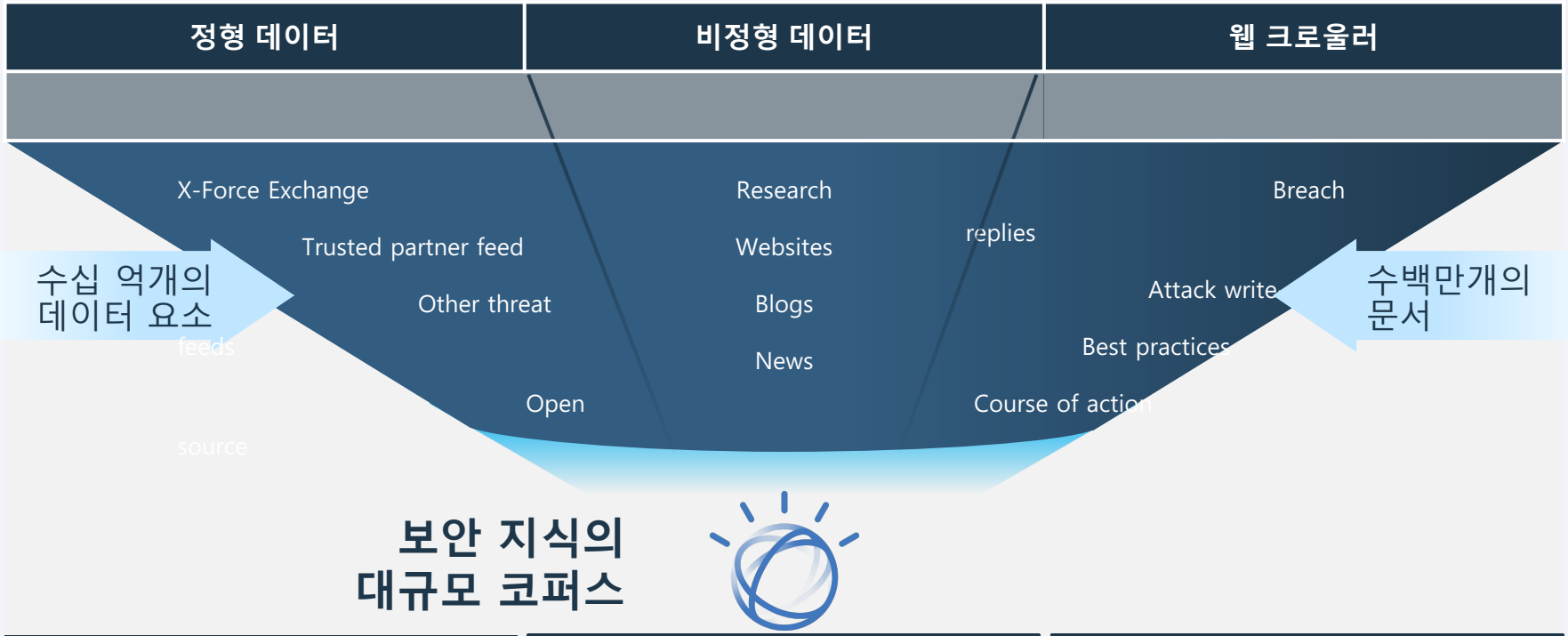
보안 지식의 세계
방어에는 활용되지 못하는 다크 데이터

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
- 트위트

Watson for Cyber Security의 운영 형태



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

SEE THE BIG PICTURE

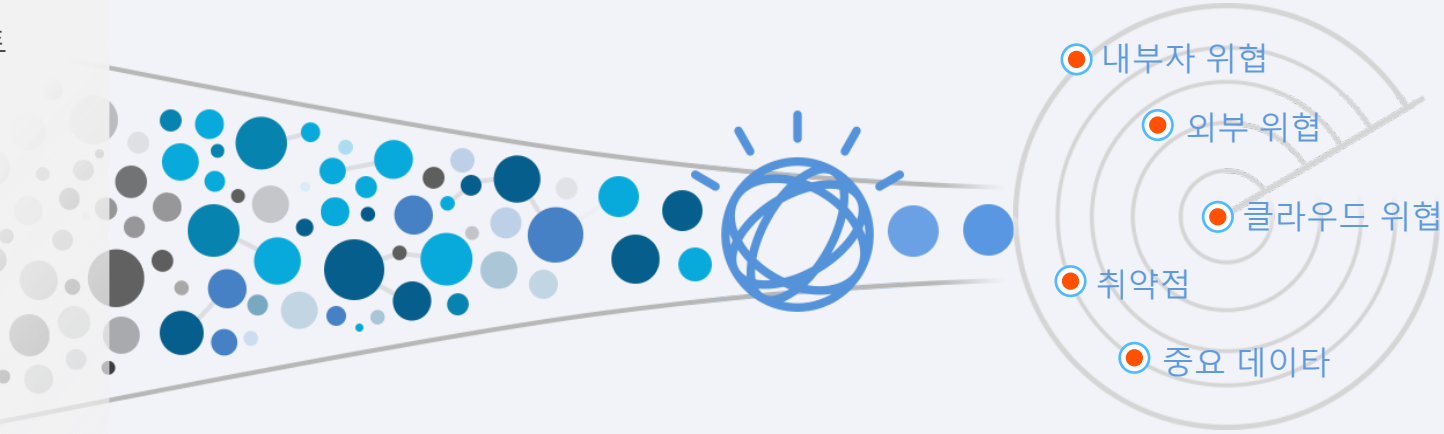
"QRadar Advisor enables us to truly understand our risk and the needed actions to mitigate a threat." UNB UNIVERSITY OF NEW BRUNSWICK

ACT WITH SPEED & CONFIDENCE

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

IBM Cognitive SOC

보안장비/엔드포인트
네트워크 행위
데이터
사용자 및 인증 정보
위협 정보
설정 내역
취약점 및 위협
어플리케이션 내용
클라우드 사용 정보



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

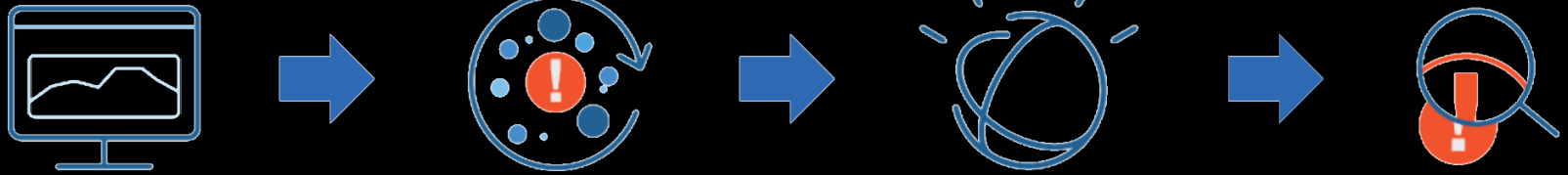
SME에 의한
심층 분석/
위협 헌팅

행동

자동화된 조치 및
협업

SOC에 대한 인공 지능 적용

인공지능이 자동으로 초동 분석을 수행하여 **SOC팀이 루틴작업에서 해방되도록 합니다.**



QRadar 보안 인텔리전스 플랫폼

자동으로 Advisor에 오펜스(보안경보)를 전송

QRadar Advisor

관련된 로컬 문맥을 수집하여 관찰 대상을 추출

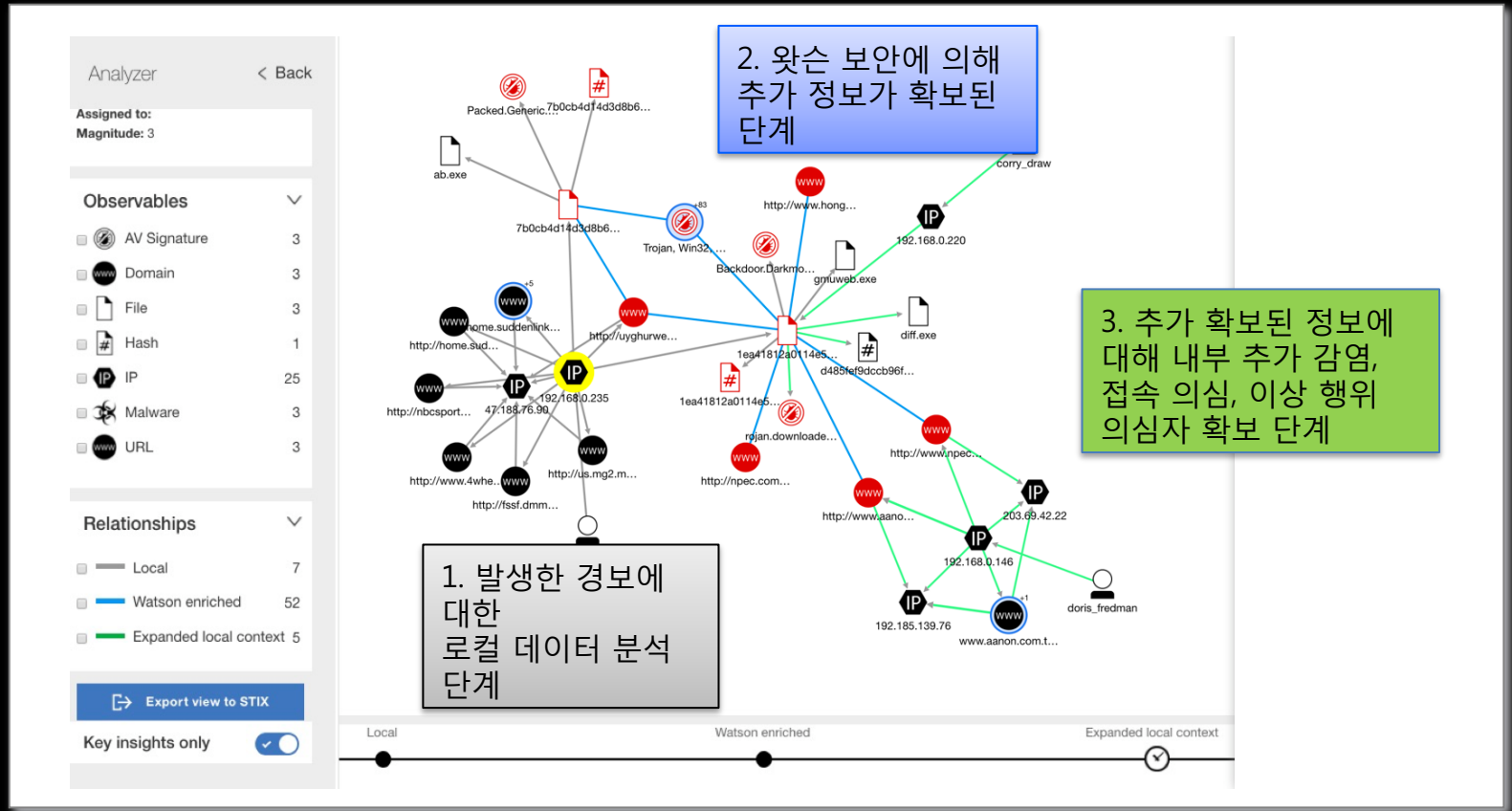
Watson for Cyber Security

인공지능 분석을 사용하여 관련 외부 데이터의 인사이트를 오펜스에 추가

QRadar Advisor

인공지능 분석을 사용하여 관련 외부 데이터의 통찰력을 오펜스에 추가

QRAW 데이터 해석 stage



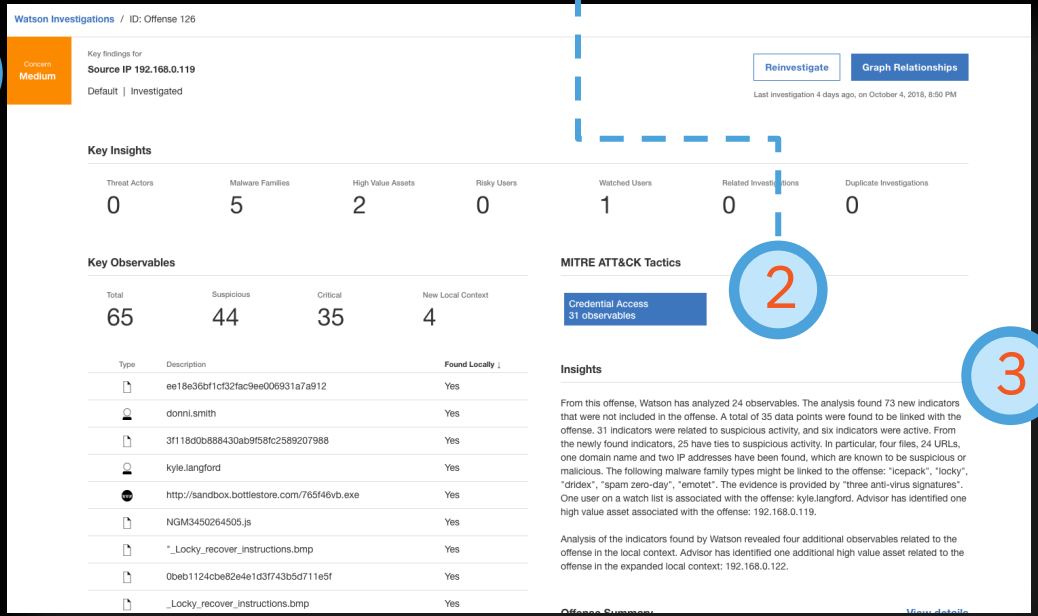
QRadar Advisor 주요 기능

인시던트를 ATT&CK 프레임워크에 맞춤

위협을 확인하는 개별 진행에 대한 확신 레벨을 제공

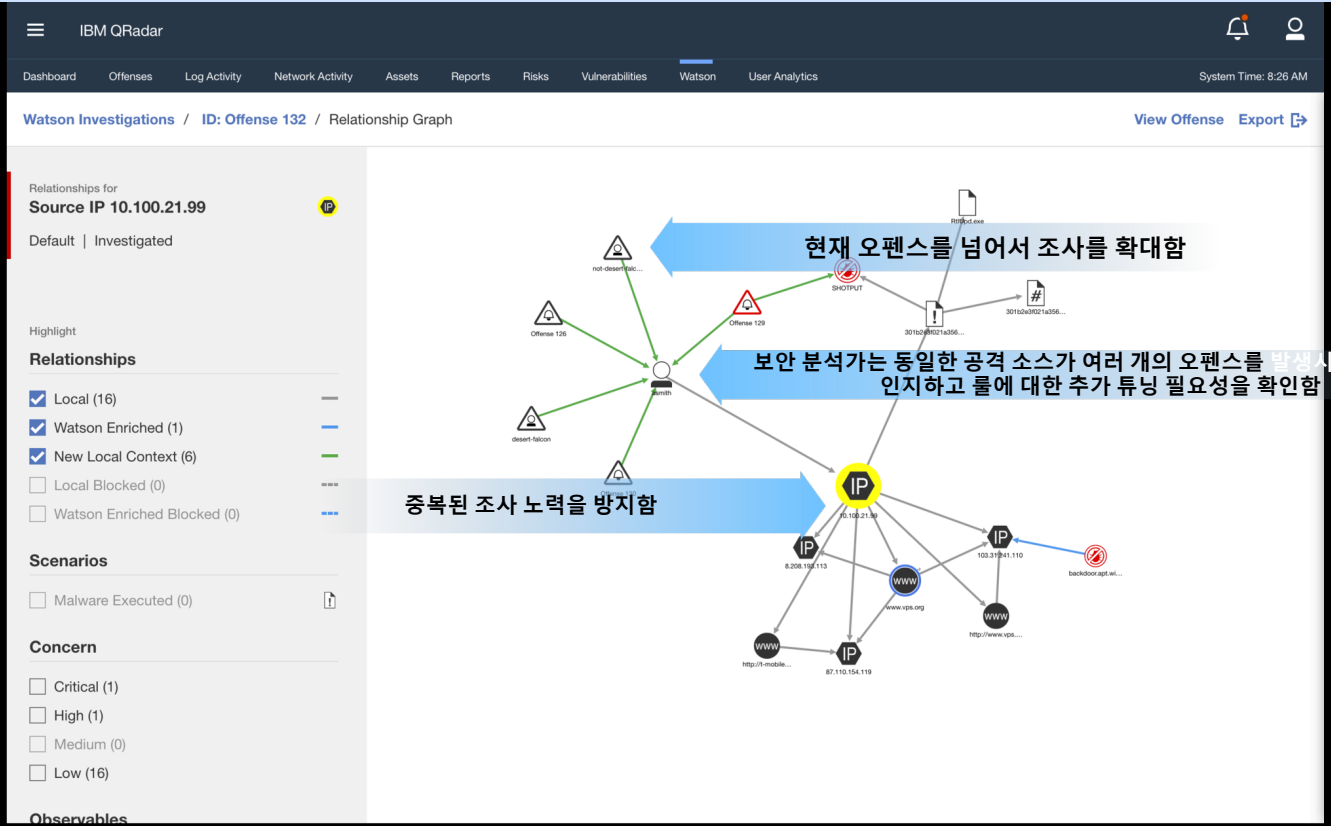
공격이 어떻게 발생하여 진행되고 있는지 시각화

어떤 공격 전술이 추가로 발생할 가능성이 있는지 확인



작동방식 – 교차-조사 분석

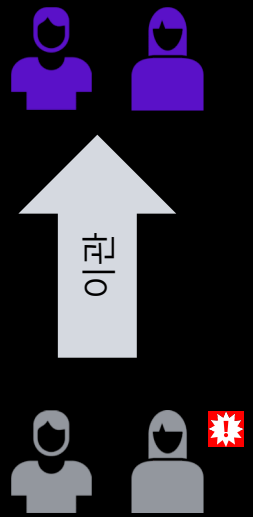
QRadar Advisor는 연결된 관찰 항목을 통해 조사를 자동으로 연결함



작동방식– 오펜스 처리 분석

학습

Tier 2 분석가
심층 조사; 사고 대응



Tier 1 분석가
첫번째 선별 ; 정보 수집 및 Tier 2로 이관

QRadar Advisor는 어떤 조사가 이관되거나 그렇지 않은지를 학습함

적용

오펜스 #152

Advisor 권고:
이 조사는 우선 순위에서 해제되었음.

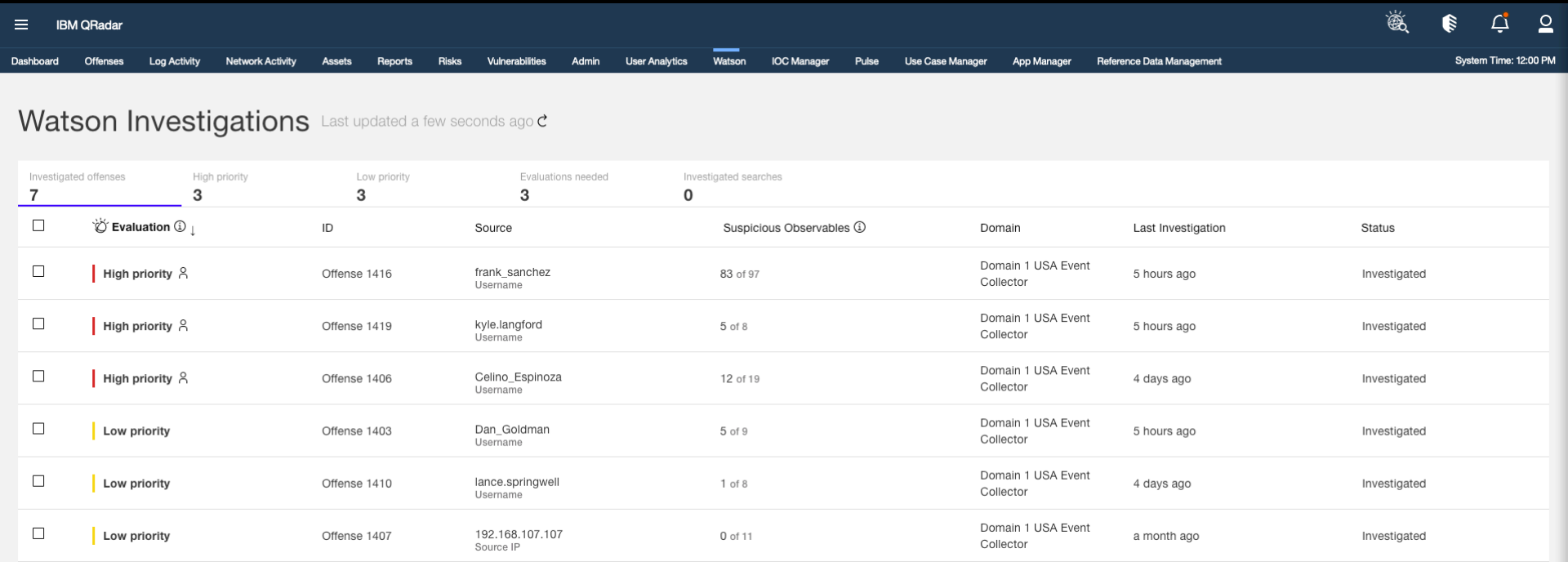
Offense # 152는 Offense # 29, # 53 및 # 112와 유사함.이 모든 것은 과거에 오탐으로 처리되었음.

오펜스 #221

Advisor 권고:
이 조사는 이관되었음.

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

오펜스 우선 순위 AI 모델 – 예시



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

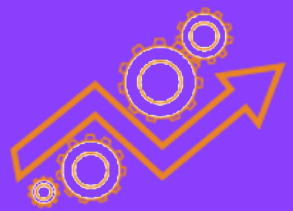
조직 보안성 증가로 651,936$(약 7억원) 효과 얻음
- 평균 분석 시간 감소와 NOC인력을 L1조사로 활용하여, 조사대상 기업이 연간 분석하는 개수가 1,800개에서 7,000개로 증가함 (기존에는 분석이 안되거나 대응이 안되고 있었음)
- 증가한 분석수로 인해 심각한 보안 사고가 8% 감소

* 본 내용은 ”A Forrester Total Economic Impact Study Commissioned by IBM Security May 2019” 내용을 근거로 함

AI 기반 위협 탐지 및 분석의 이익&효과

보안 운영 팀의 노력이 배가 됨

- 반복적인 SOC작업의 자동화



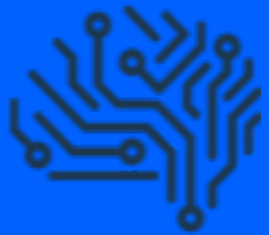
AI 기반 위협 탐지 및 분석의 이익&효과

보안 운영 팀의 노력이 배가 됨

- 반복적인 SOC작업의 자동화

일관되고 더 자세한 조사 및 분석을 수행함

- 중요한 보안 사건에 대해 실행 가능한 통찰력을 확보



AI 기반 위협 탐지 및 분석의 이익&효과

보안 운영 팀의 노력이 배가 됨

- 반복적인 SOC작업의 자동화

일관되고 더 자세한 조사 및 분석을 수행함

- 중요한 보안 사건에 대해 실행 가능한 통찰력을 확보

휴지 시간을 단축시킴

- 보다 신속하고 결정적인 에스컬레이션 프로세스 채택

Thank you

_

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

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.