언택트 시대의 보안 관제를 위한 최신 기술

온라인으로 함께 하는
제6회 IBM Security Summit

한국IBM
나병준 실장

SECUI
김종현 프로

코로나19와 보안

IBM Security

IBM

사이버 인텔리전스와 보안에 코로나19가 미치는 영향

나타나는 현상

- 관련 스팸의 폭발적 증가
- 더 커진 공격의 양상
- 국가 단위의 표적 악성 코드 증가
- 건강 관리 시설 및 관련 인력을 공격
- 재택 근무 시의 회사 네트워크의 취약성 노출

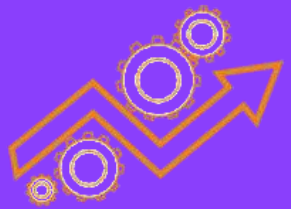
88%

전 세계 회사/조직의
직원에게 재택 근무가
권장 또는 요구되었습니다.

우리가 나아가야 할 방향

Automation

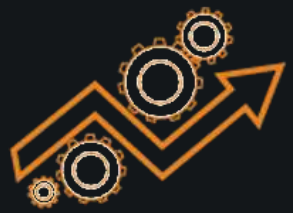
– 빠른 의사 결정이 가능한 민첩성



우리가 나아가야 할 방향

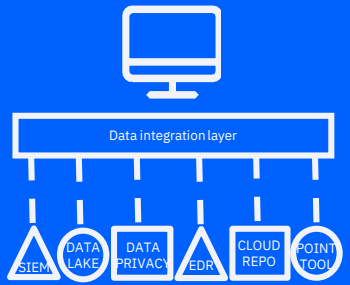
Automation

– 빠른 의사 결정이 가능한 민첩성



Anywhere

– 고립을 피하기 위한 비즈니스 중심 협업



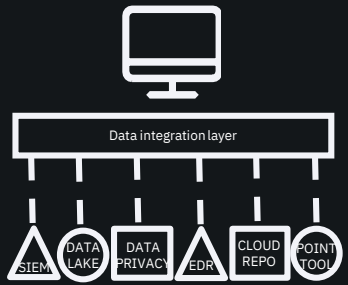
우리가 나아가야 할 방향

Automation

– 빠른 의사 결정이 가능한 민첩성

Anywhere

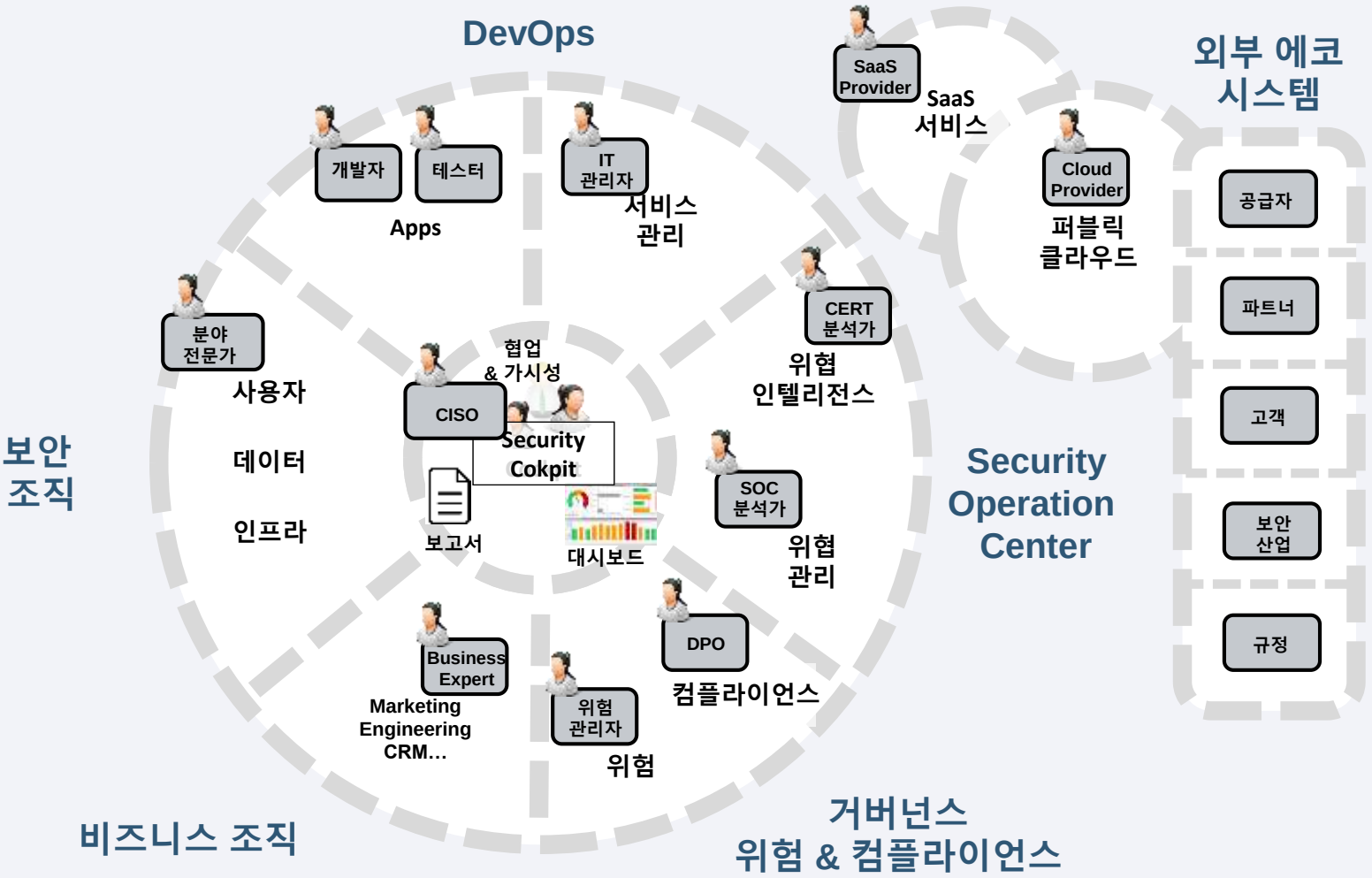
– 고립을 피하기 위한 비즈니스 중심 협업



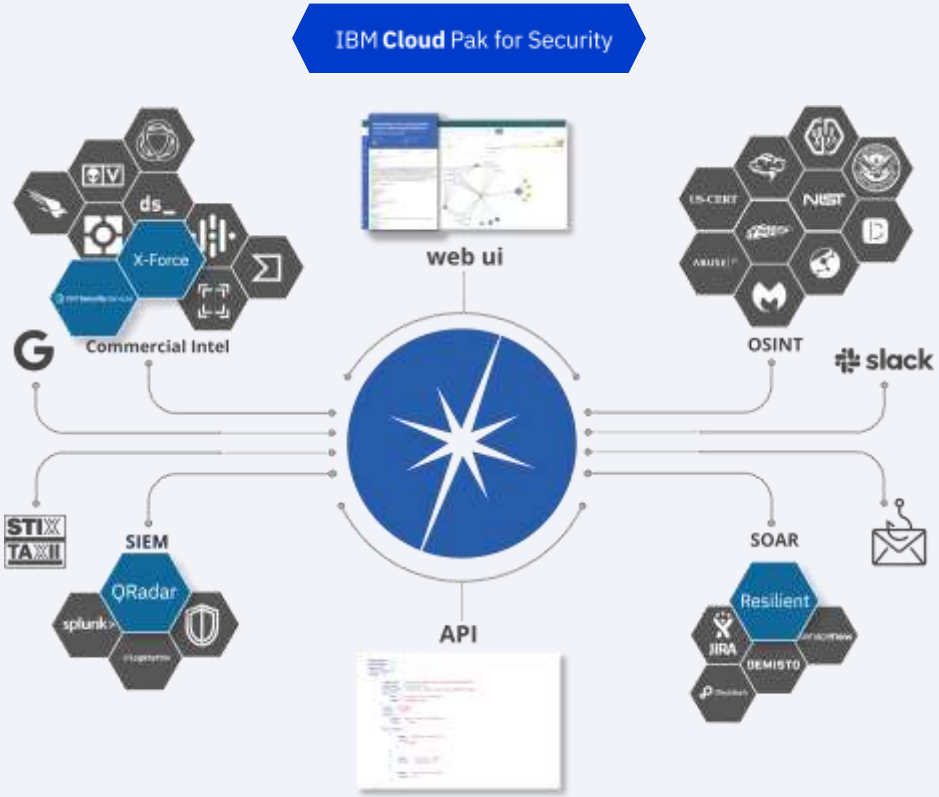
Expertise

– 24x7 전문 보안 지식 활용과 통찰력 확대

“Defend Better Together” Ecosystem



Defend Better Together



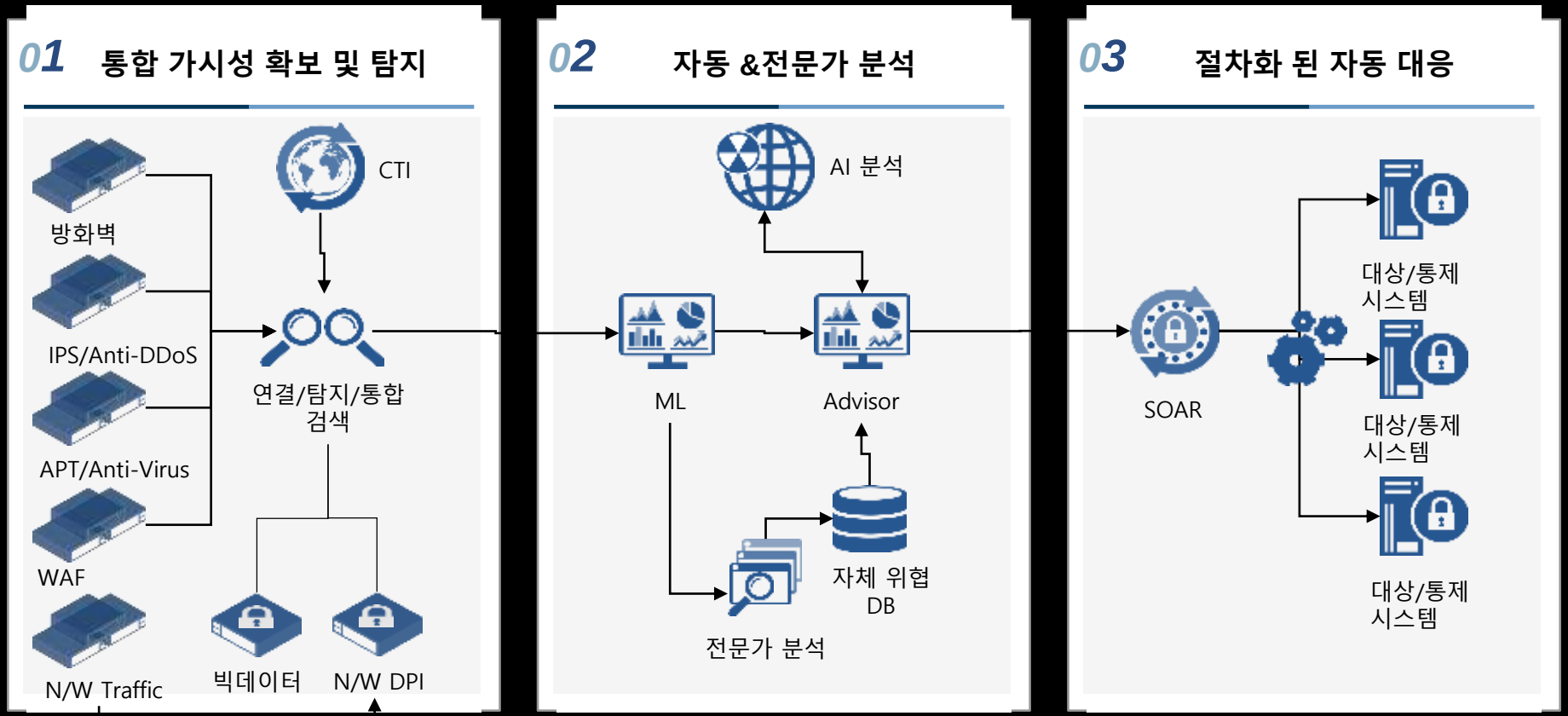
차세대 인텔리전스 리더들은 이제 새로운 도구가 필요합니다

바로 내일

- ✓ 반복 수행 가능
- ✓ 모든 조직과 어디에서나 협업 가능
- ✓ 내부 및 외부 데이터 리소스 활용
- ✓ 지속적으로 데이터를 실행 가능한 인텔리전스로 전환

SOC를 위한 개별 기술

가시성 통합과 탐지, 분석, 대응

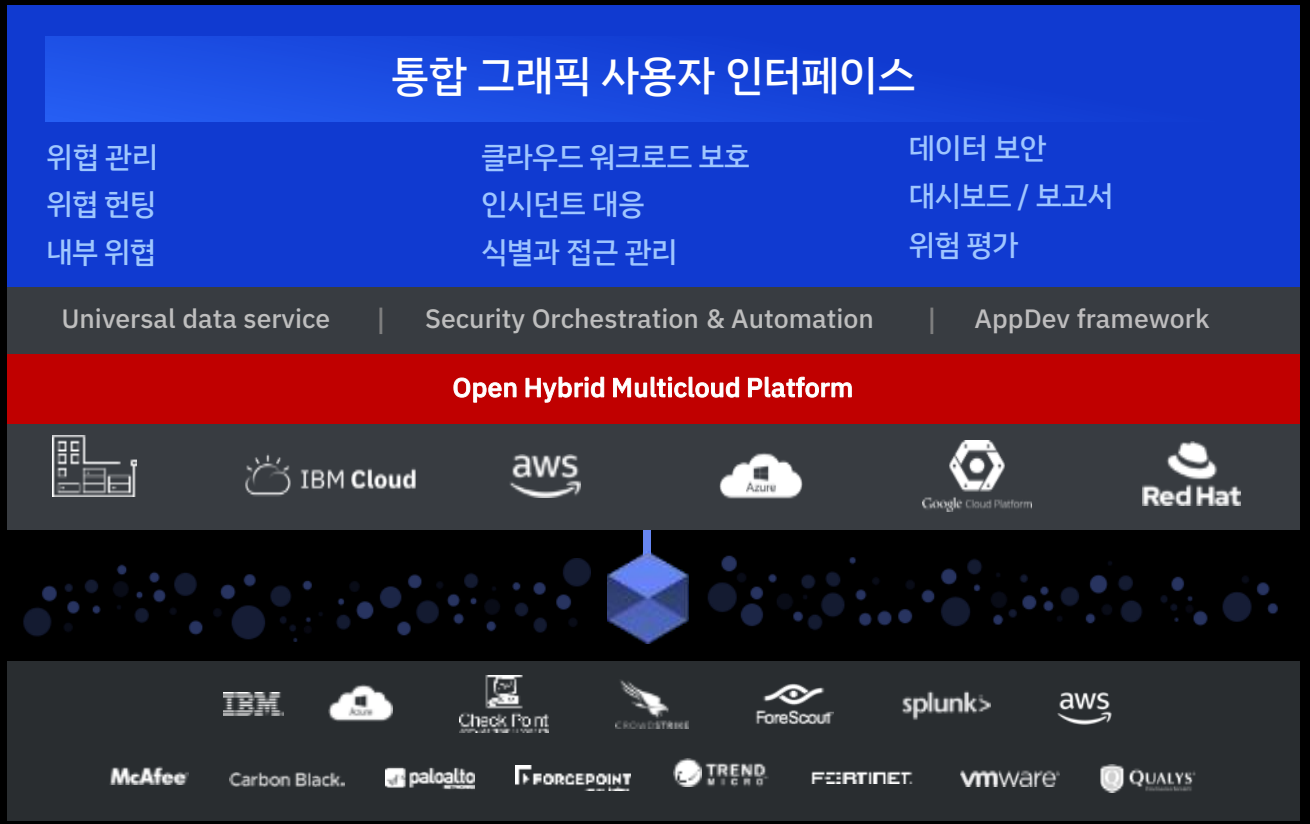


IBM Cloud Pak for Security

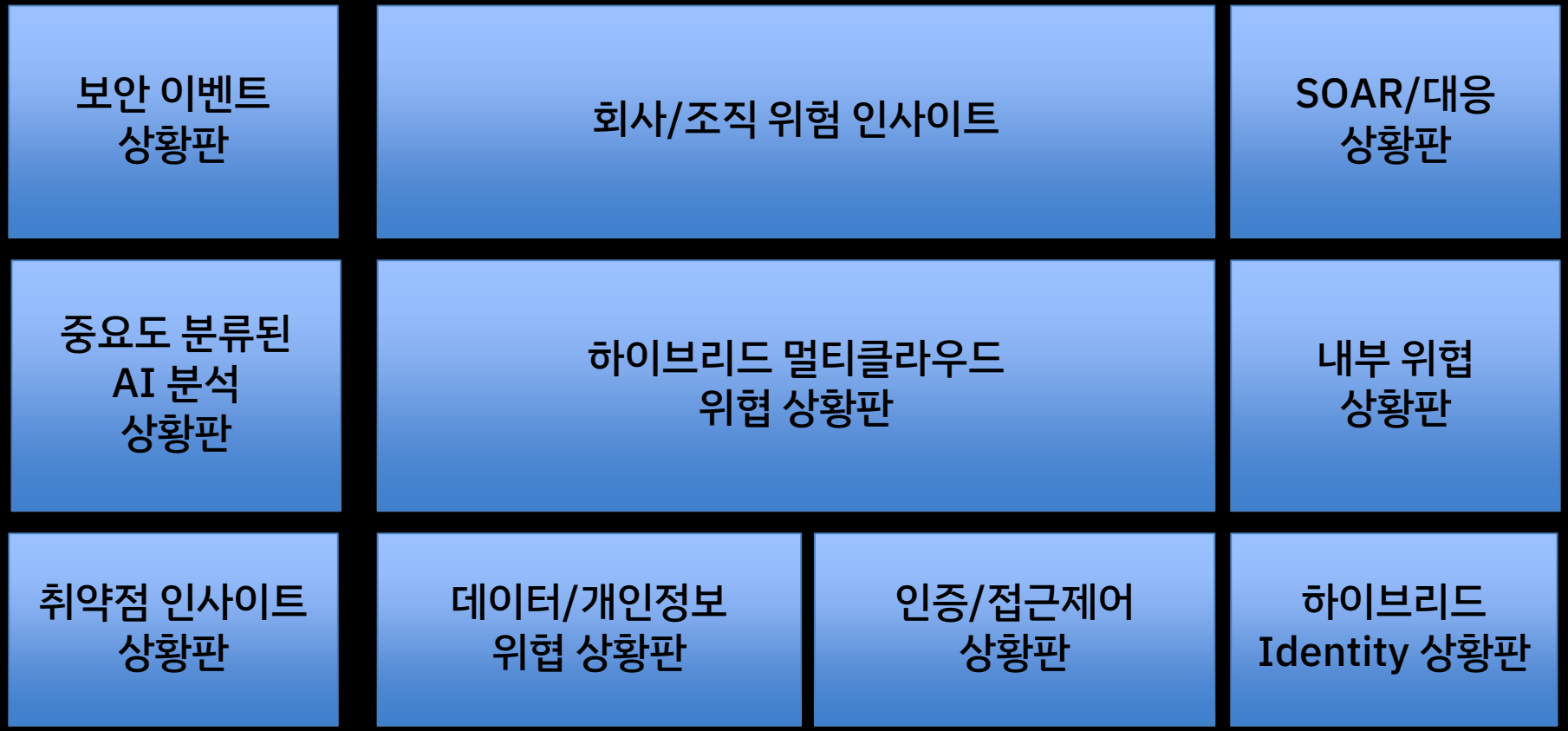
Composable
보안 솔루션

하이브리드 멀티클라우드
아키텍처

기존 보안 도구와의
열린 통합



모든 것이 연결된 엔터프라이즈 보안 상황판



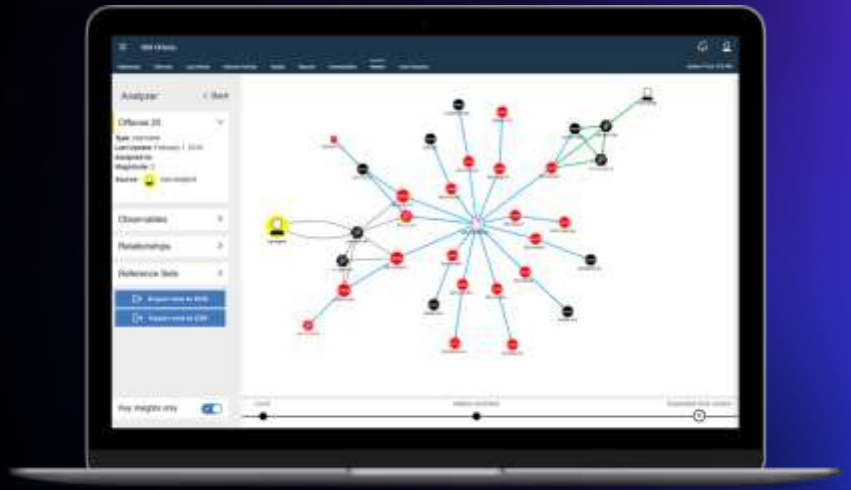
자동 탐지 및 분석

IBM QRadar User Behavior Analytics

머신 러닝과 함께 위협 탐지

- 악의적인 엔티티/사용자를 예측하는 행동을 지속적으로 학습
- 개별 사용자에 대한 상세한 위험 점수 생성
- X-Force App Exchange에서 16K회 이상 무료 다운로드

IBM QRadar Advisor with Watson



AI로 팀의 효율성 극대화

- 보다 확실한 위협 수준 상승을 위해 자동으로 연결 지점 생성
- MITER ATT&CK을 사용하여 반응 속도를 높이고 공격 단계를 시각화
- Watson의 100억 개 이상 보안 데이터 포인트를 통한 통찰력 확보

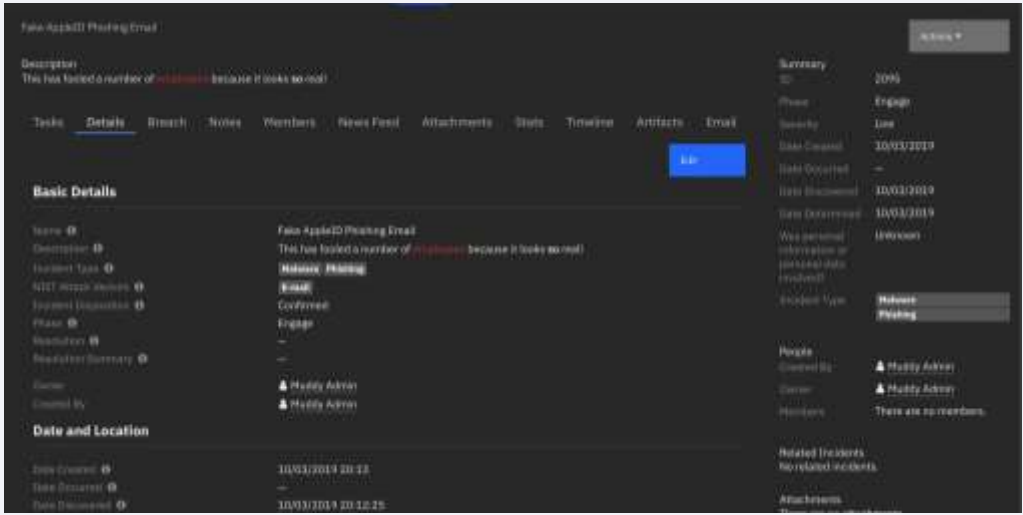
절차화된 자동 대응

IBM Resilient

보안 그룹을 업계 최고의
인시던트 대응 플랫폼으로 지원

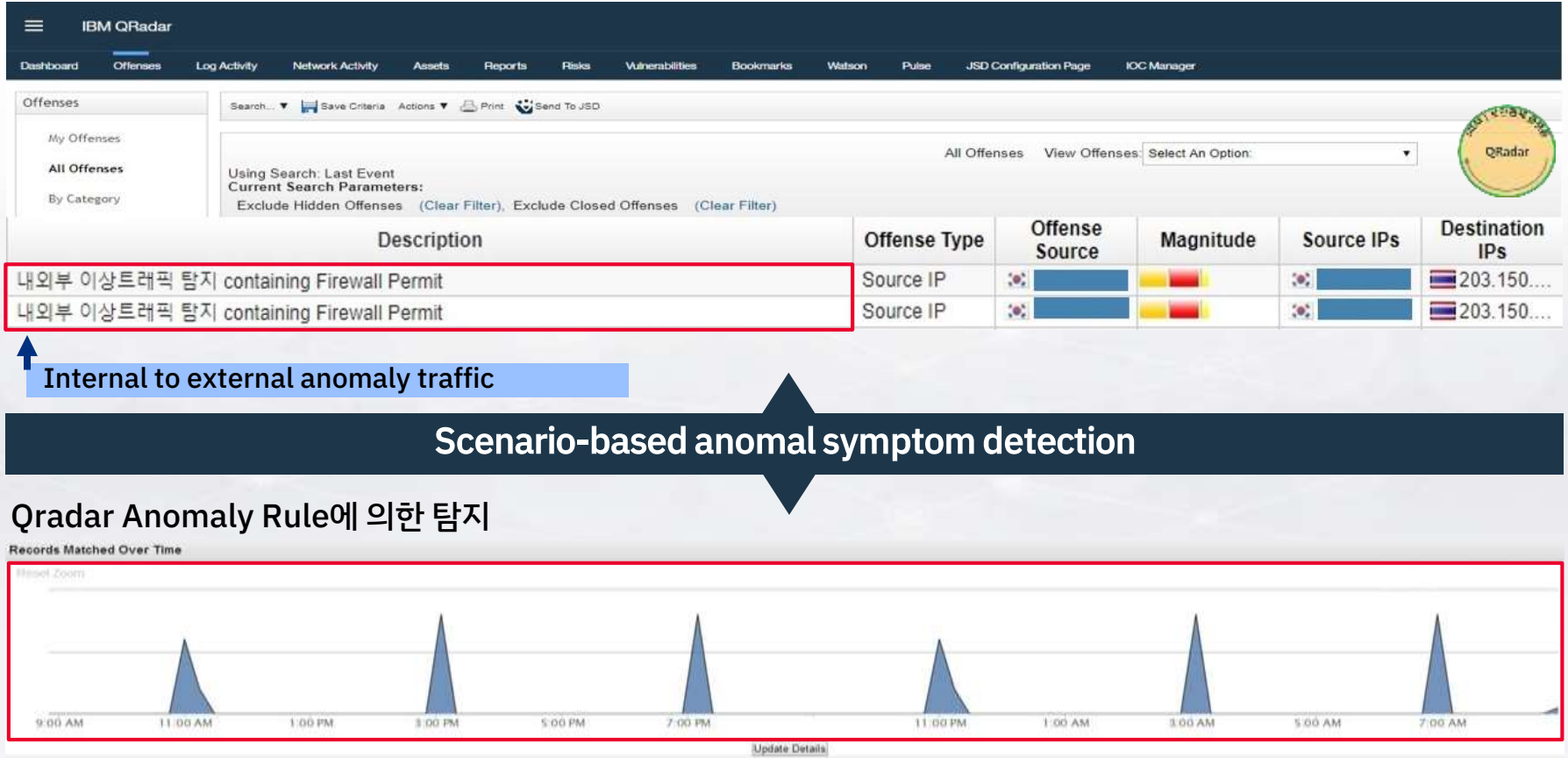
40x

사람들, 프로세스 및 기술을 조율하는
동적 플레이 북을 사용하여 전반적인
대응을 가속화



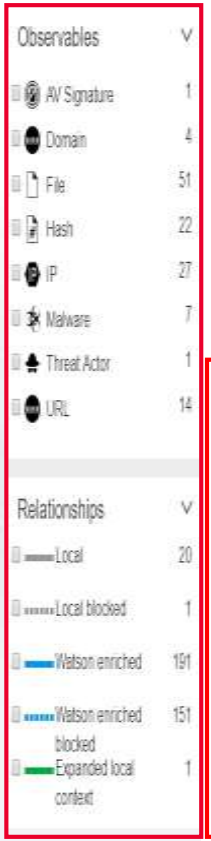
AI를 이용한 실제 보안 분석의 사례 – SECUI

QAW를 이용한 탐지 사례 – 복합 위협 분석

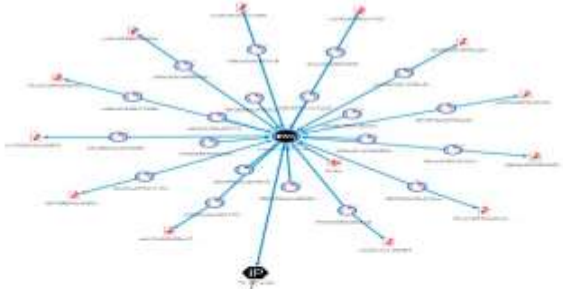


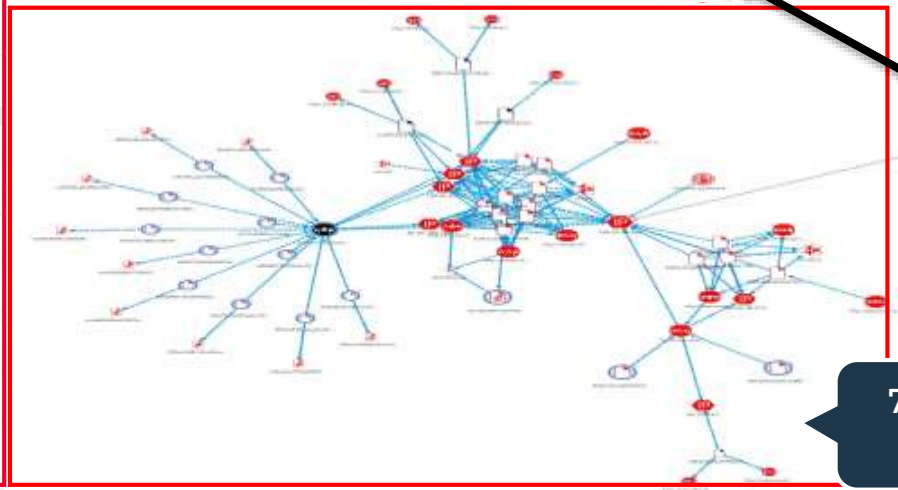
QAW를 이용한 탐지 사례 – 복합 위협 분석

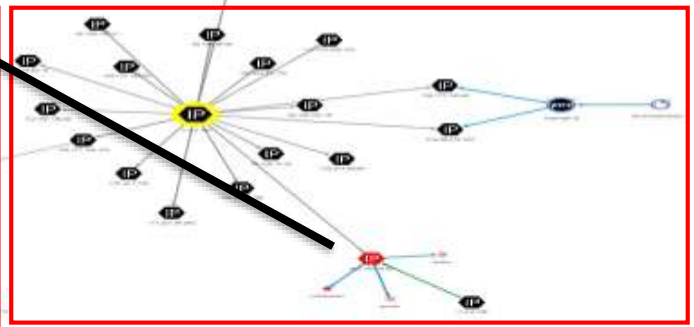
Watson에 질의한 Source IP
통신이력 外, 로컬 자산 중 악성 IP에
접근한 이력 추가 확인



추가로 발견된
로컬 위협 자산

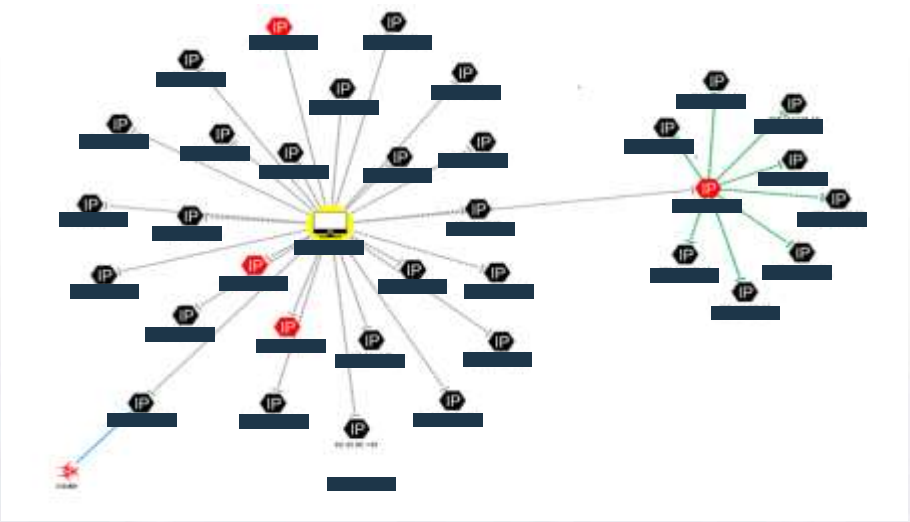


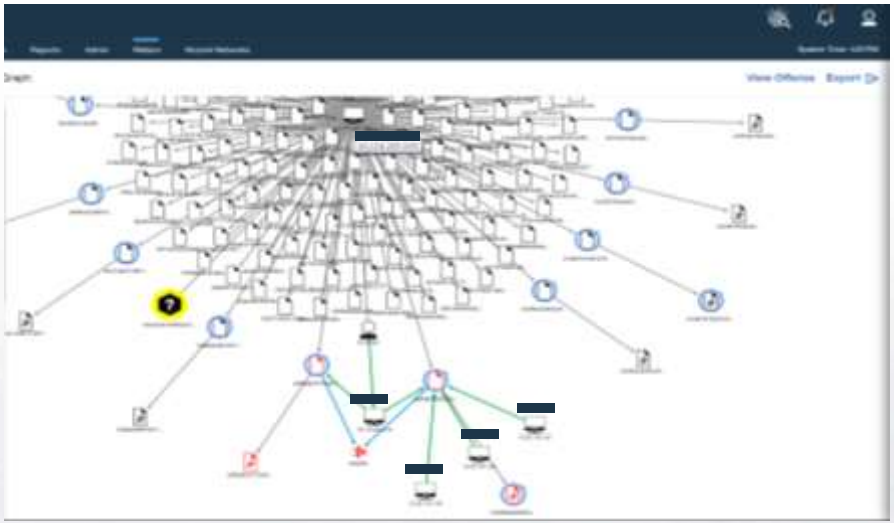




7개의 Malware, 1개의 Antivirus Signature,
다수의 도메인 및 URL, 관련 IP 확인 가능

QAW를 이용한 탐지 사례 – C&C(악성코드 포함) 및 Malware 감염 분석





분석

위협 탐지 IP 외에 추가적으로 외부 위협 통신 시도 발견하였으며,
C&C 서버와의 통신을 하려하는 내부 IP 발견 되었음 해당 IP 백신 검사 요망
현재는 방화벽 거부로 통신 연결은 되지 않음

대응 가이드

위협 탐지 IP에 대해 C&C 감염된 IP에 대한 시도가 있었으나 방화벽에 의해 차단됨,
하지만 위협탐지 IP에서 외부 위협식별 IP로 연결 시도 발견,
연결 시도한 외부 위협식별 IP에서 내부 다수 IP로 연결 시도가 있었음
(단말에 대한 악성코드 검사 후 감염 식별 됨)

분석

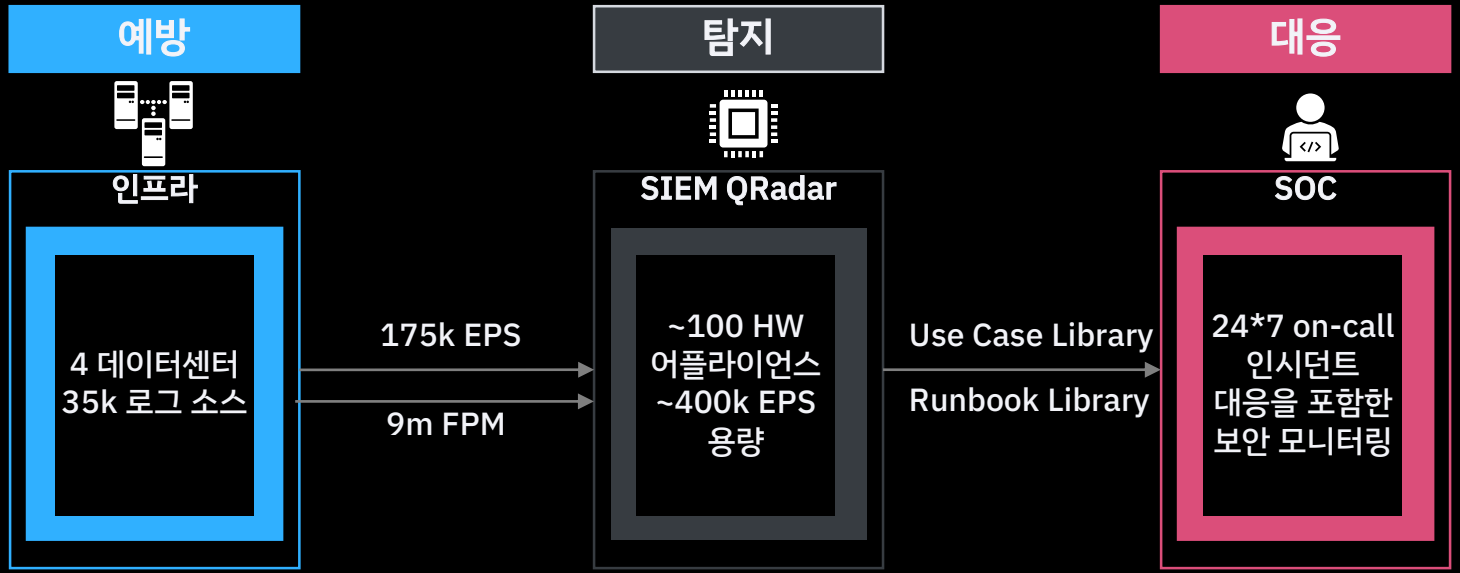
malware family type인 renamer가 발견되는 내부 호스트를 추가로 분석함으로써
동일 malware 가 내부 시스템에 전파되는지에 대해 추가로 분석한 결과

대응 가이드

위협 탐지 IP에서 접근한 파일에 대해서 Hash값 비교를 통해 Malware로 의심되며,
다수의 다른 위협 탐지 IP에서도 해당 파일에 접근 시도.
Malware 파일에 접근한 IP들은 EDR 솔루션에 의해 차단되어 추가적인 위협 없음,
Malware 감염 파일의 유입 경로 확인 후 차단 대응이 필요.

결론

독일 협동 금융 네트워크의 IT서비스 Provider인 Fiducia & GAD IT는 코로나19 대응을 위해 SOC를 원격 작업으로 전환



코로나19 상황

단 1주일 만에 사이버 방어 센터를
현장에서 원격 작업으로 전환

코로나19에 대한 준비로 보안 팀 역량 강화

위협 인텔리전스 경계

- 급격하게 발생하는 많은 양의 코로나19 관련 스팸 활동 관찰
- 전세계적인 관심 주제를 통해 공격자는 공휴일에 초점을 맞추지 않고 대상 확장
- DDoS를 통한 의료 시설 및 인력 목표 공격 발생
- 코로나19 스팸과 관련된 복잡성 및 악성코드 수가 증가

인시던트 대응 준비

- 팀이 재택근무인 경우 사이버 위기 관리 계획을 훈련하고 전문 인시던트 대응 회사와 상담
- Quad9(IBM 및 파트너가 제공하는 무료 리소스)을 이용하여 스푸핑 및 악성 도메인 탐지
- 보안의 기본 사항으로 돌아가 스팸과 같은 가능성 높은 요소를 경계하고 의심스러운 링크를 피하기 위한 조치 수행

위협 인텔리전스 완화

- IBM 보안 파트터인 TruSTAR를 통해 X-Force IRIS와 위협 인텔리전스를 공유
- https://ibm.biz/covid-19. 사이트에 사인업
- X-Force Exchange에서 코로나19와 관련된 인텔리전스 구독

감사합니다

Follow us on:

ibm.com/kr-ko/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

IBM Security

IBM