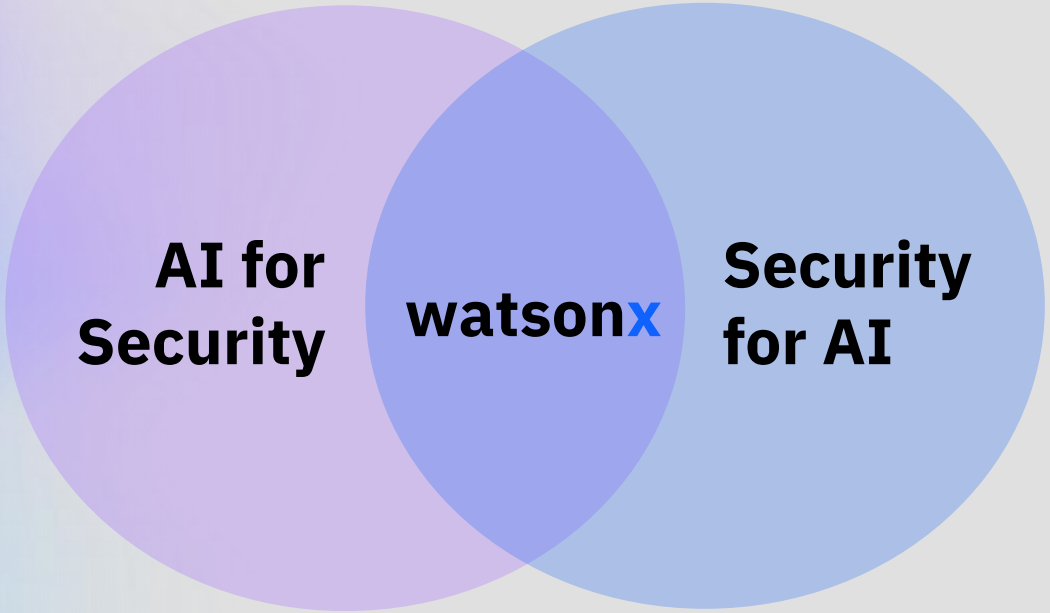
금융 산업 핵심보안 이슈와 차세대 플랫폼 기반 보안 운영 현대화



김강정 상무
IBM 보안사업부 총괄

IBM **Security**

The 2023 CEO Study

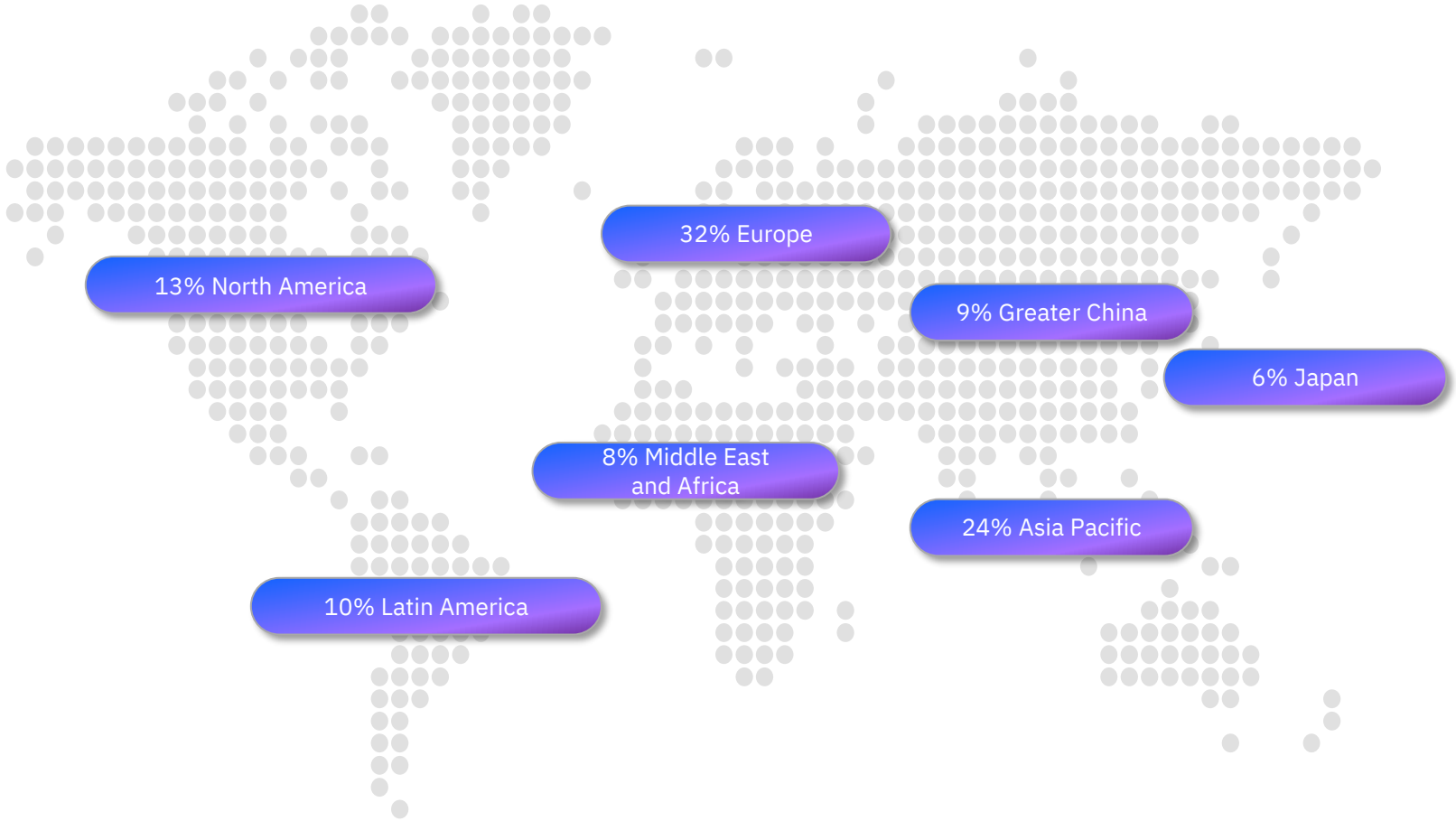
30+
국가

3,000+
CEOs

24
산업

360
금융 산업 CEOs

Global distribution



Data collected 1H 2023 in cooperation with Oxford Economics, a 2Q CEO survey on generative AI adoption* with Oxford Economics, and ~20 in-depth CEO conversations

* With 200 CEOs from the United States.

AI 시대 금융 산업 CEO의 의사 결정

우선 순위와 도전 과제

생산성과 수익성은 **'사이버 보안의 우선 순위'**와 **'기술 현대화'**에 달려 있습니다.

환경 지속 가능성에 대한 기준의 부재는 은행 업계에서 가장 큰 과제입니다.

급직적인 기술 발전과 기대되는 가치

금융산업의 CEO들은 "기존 AI 프로젝트에 비해 생성형 AI의 가치"에 대해 신중한 입장을 취하고 있습니다.

이들은 다른 CEO들에 비해 "양자 컴퓨팅의 잠재력"을 가장 먼저 인식하고 있습니다.

또한 이들은 블록체인이 다른 산업보다 더 많은 가치를 창출할 것으로 기대합니다.

데이터에 대한 이해 및 주도

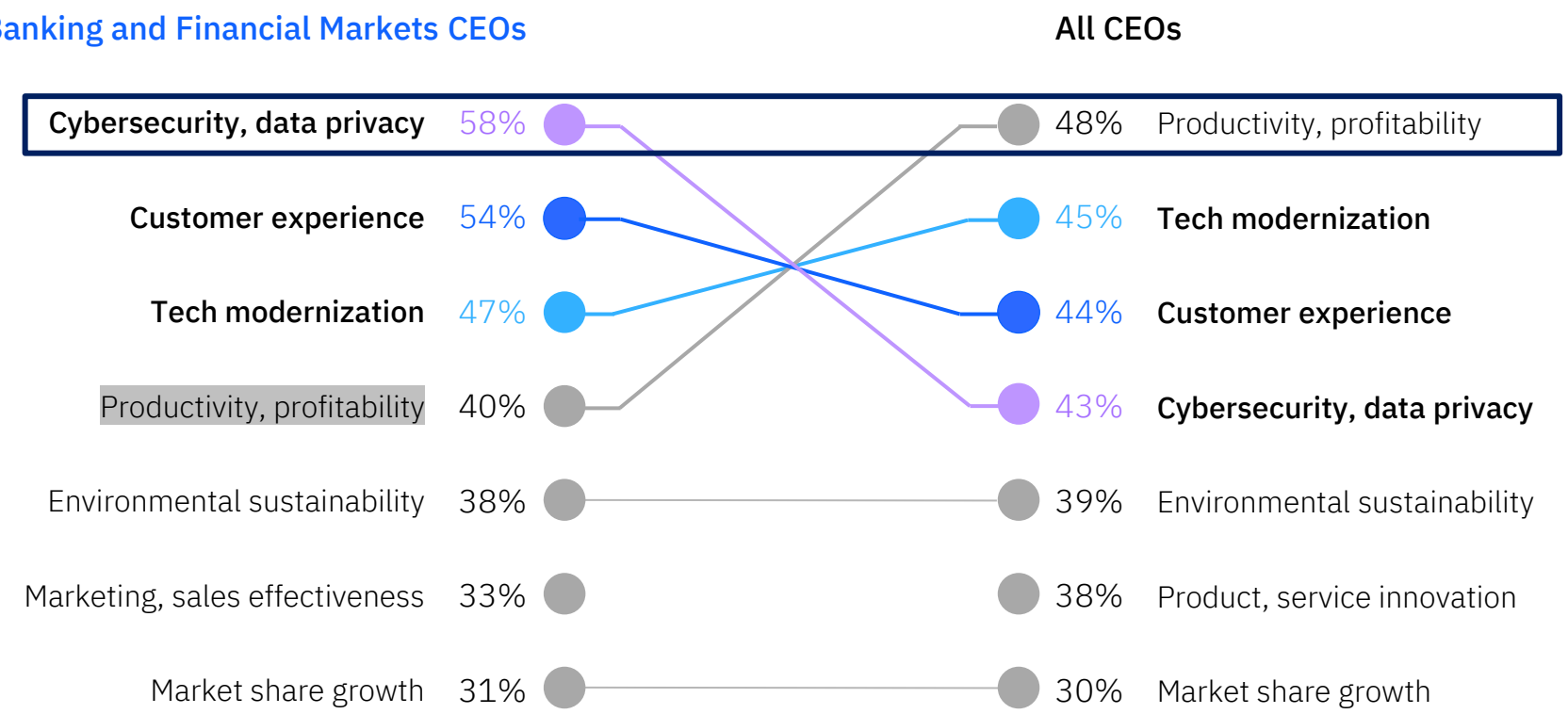
금융 CEO는 데이터와 보고의 가치에 대해 논의할 때 대외적인 측면에 치중하고 내부 관련성에는 덜 신경을 씁니다.

그러나 최고의 CEO는 메트릭을 사용하여 조직을 이해하고 이끌며, 이를 통해 보다 지속적인 성과를 이끌어냅니다.

The 2023 CEO Study
우선 순위와 도전 과제

금융 산업 CEO들은 향후 3년간 사이버 보안, 고객 경험, 기술 현대화의 우선순위에 따라 생산성과 수익성이 달라진다고 밝혔습니다.

Organization's highest priorities over the next 3 years



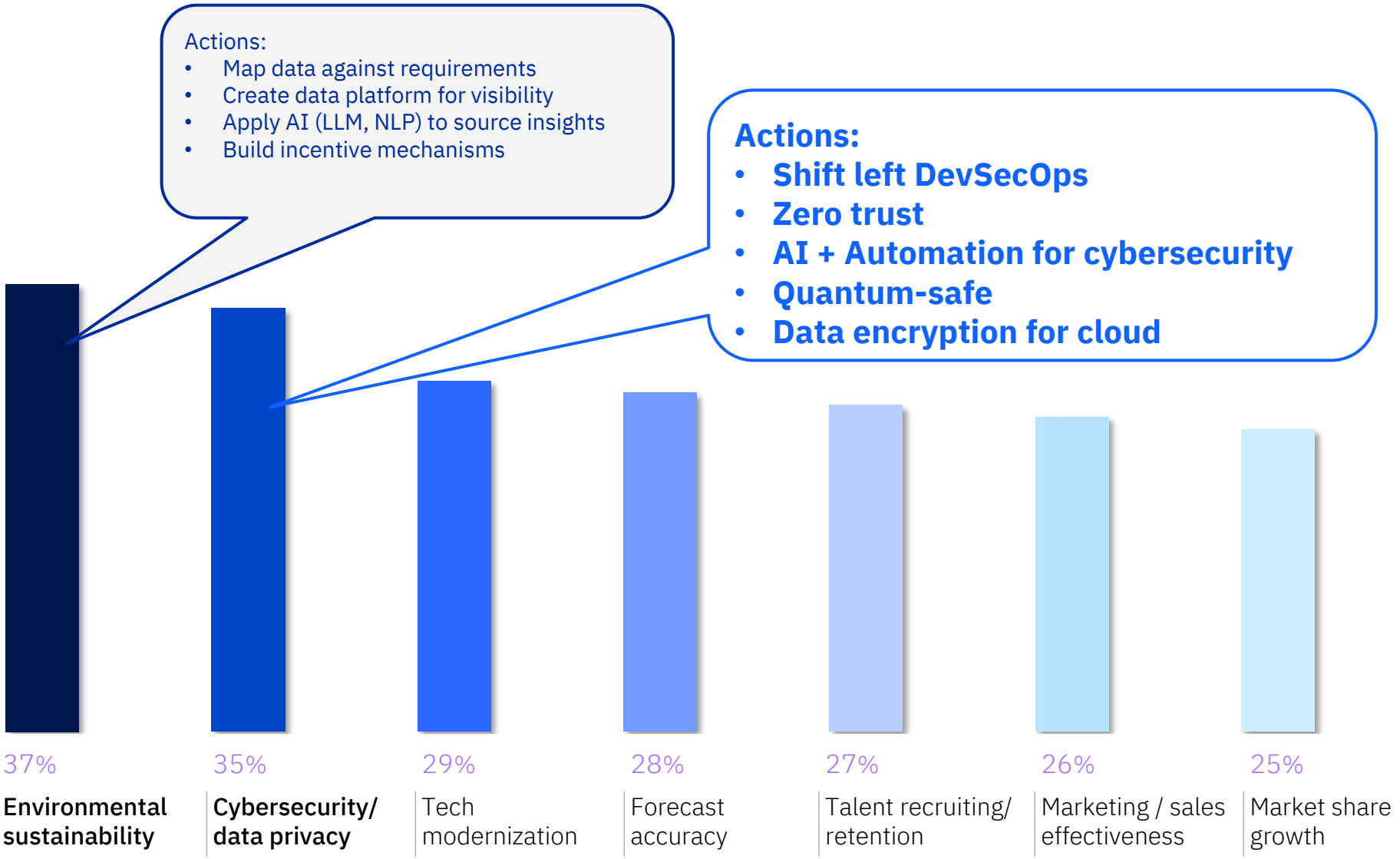
Q1.1. Which of the following represent your organization's highest priorities over the next 3 years?

The 2023 CEO Study
우선 순위와 도전 과제

지속 가능성과 **사이버 보안**을 최우선 과제로 꼽은 BFM CEO들

Organizations' greatest challenges over the next 3 years

BFM



Q1.2. What do you expect will be the greatest challenges for your organization over the next 3 years?

IBM Security X-Force 위협 인텔리전스 인덱스 2023

2023 최신 위협 동향

관찰된 목표에 적용된 주요 조치

21%
백도어 배포를 통한 인시던트 – Emotet

17%
이전 2년간 최상위 조치이던 랜섬웨어의 공격 점유율

상위 초기 접근 벡터

41%
초기 접근에 피싱이 사용된 인시던트 비율

26%
공용 애플리케이션 악용으로 인한 인시턴트

조직에 영향을 미치는 가장 흔한 공격

27%
갈취,
가장 일반적인 공격

30%
갈취로 이어지는 인시던트의 제조 산업 비중

지역 및 산업 트렌드

31%
아시아 태평양, 2년 연속 공격을 많이 받은 지역 1위

25%
제조업, 2년 연속 가장 많이 공격을 받은 산업 1위

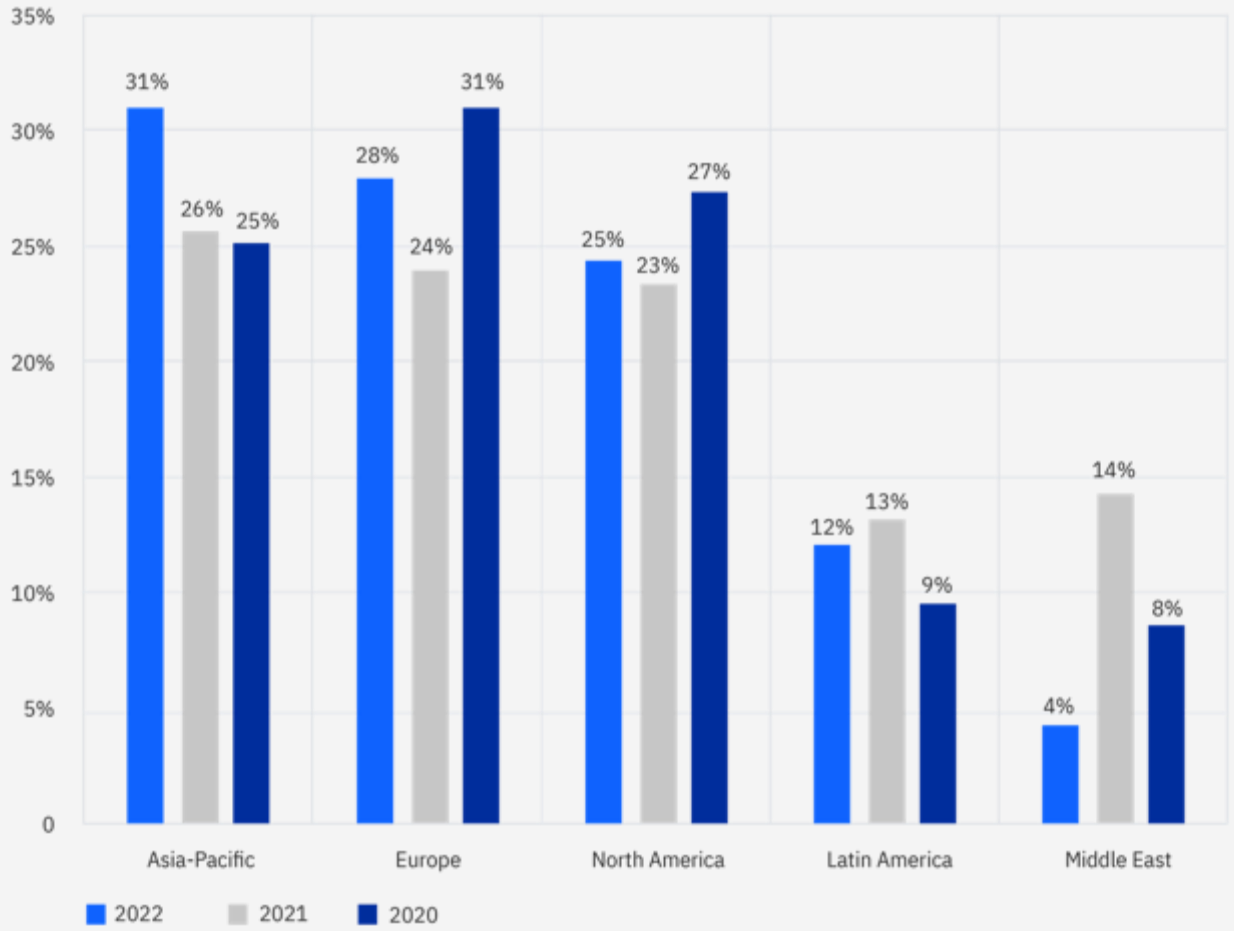
지역별 위협 분포

#1 아시아태평양
이모텟 스파이크

#2 유럽
21% 랜섬웨어

#3 북미
35% 외부 애플리케이션 공격
23% 랜섬웨어

Breakdown of attacks by geography, 2020 – 2022
Source: IBM Security X-Force

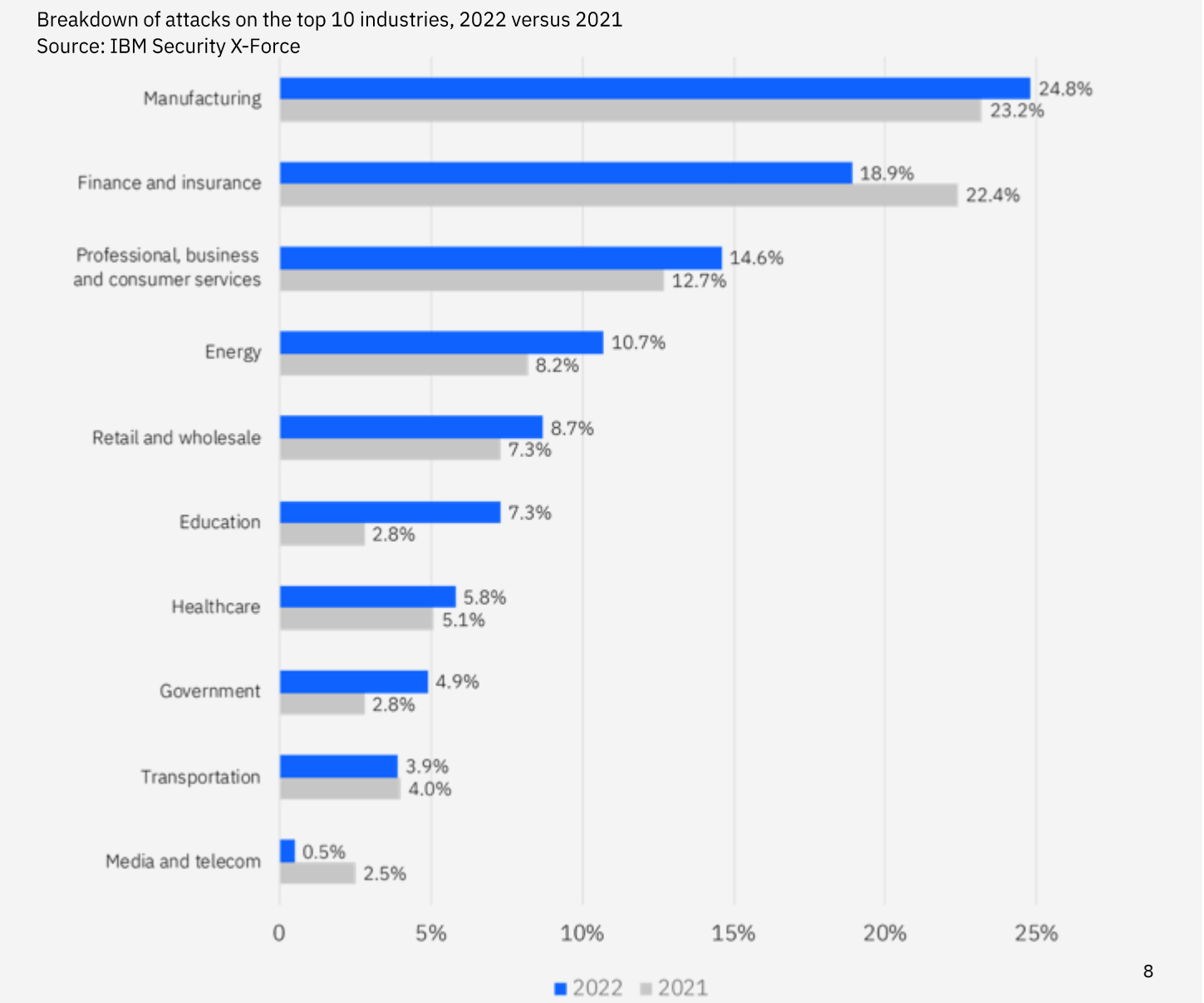


업종별 위협 분포

#1 제조
32%의 갈취

#2 금융/보험업
29% 백도어

#3 서비스/소비재
18% 백도어/18% 랜섬웨어



데이터 유출

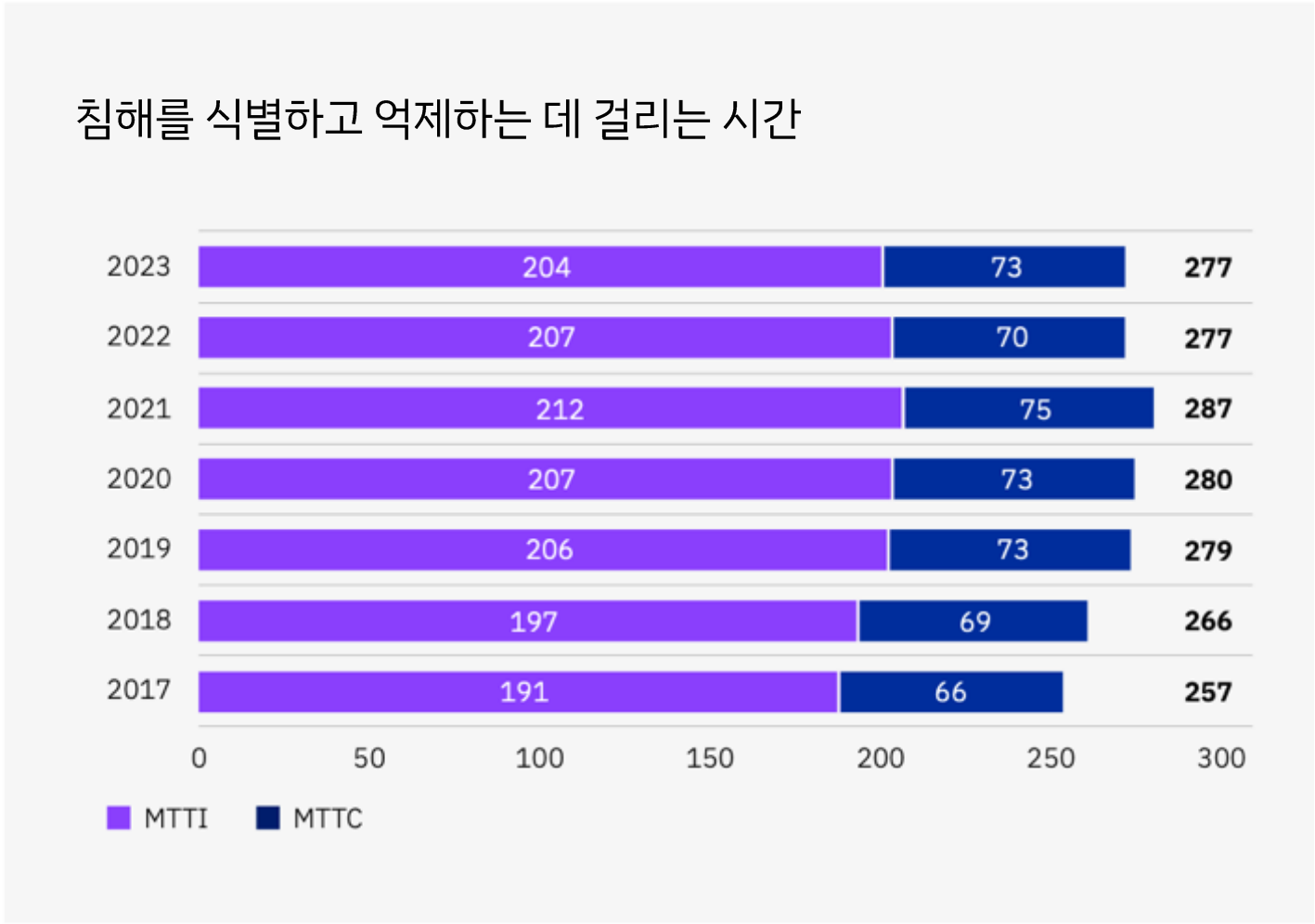
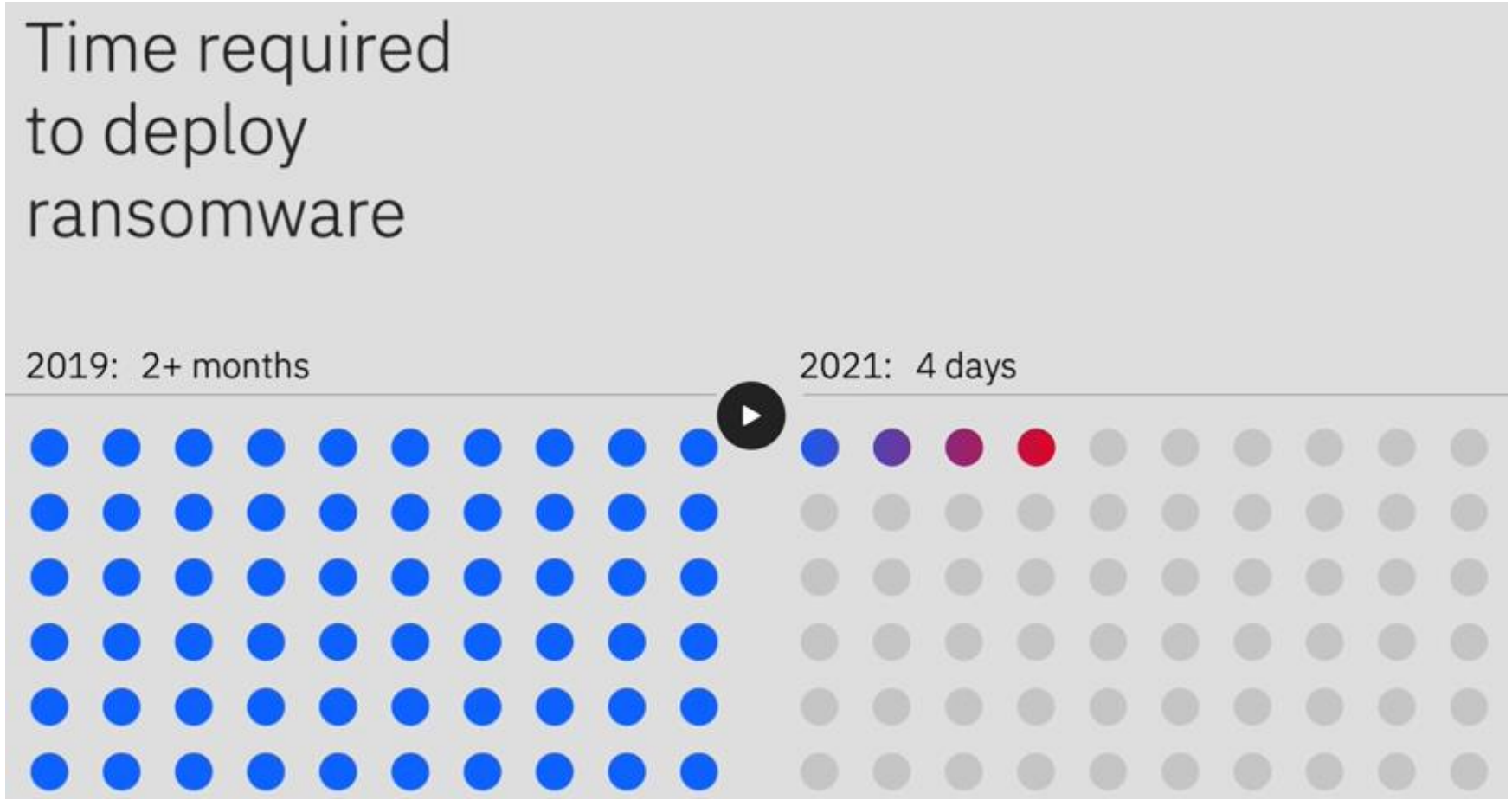


Figure 5. Measured in days

Mean Time to Identify(MTTI), Mean Time to Contain(MTTC)

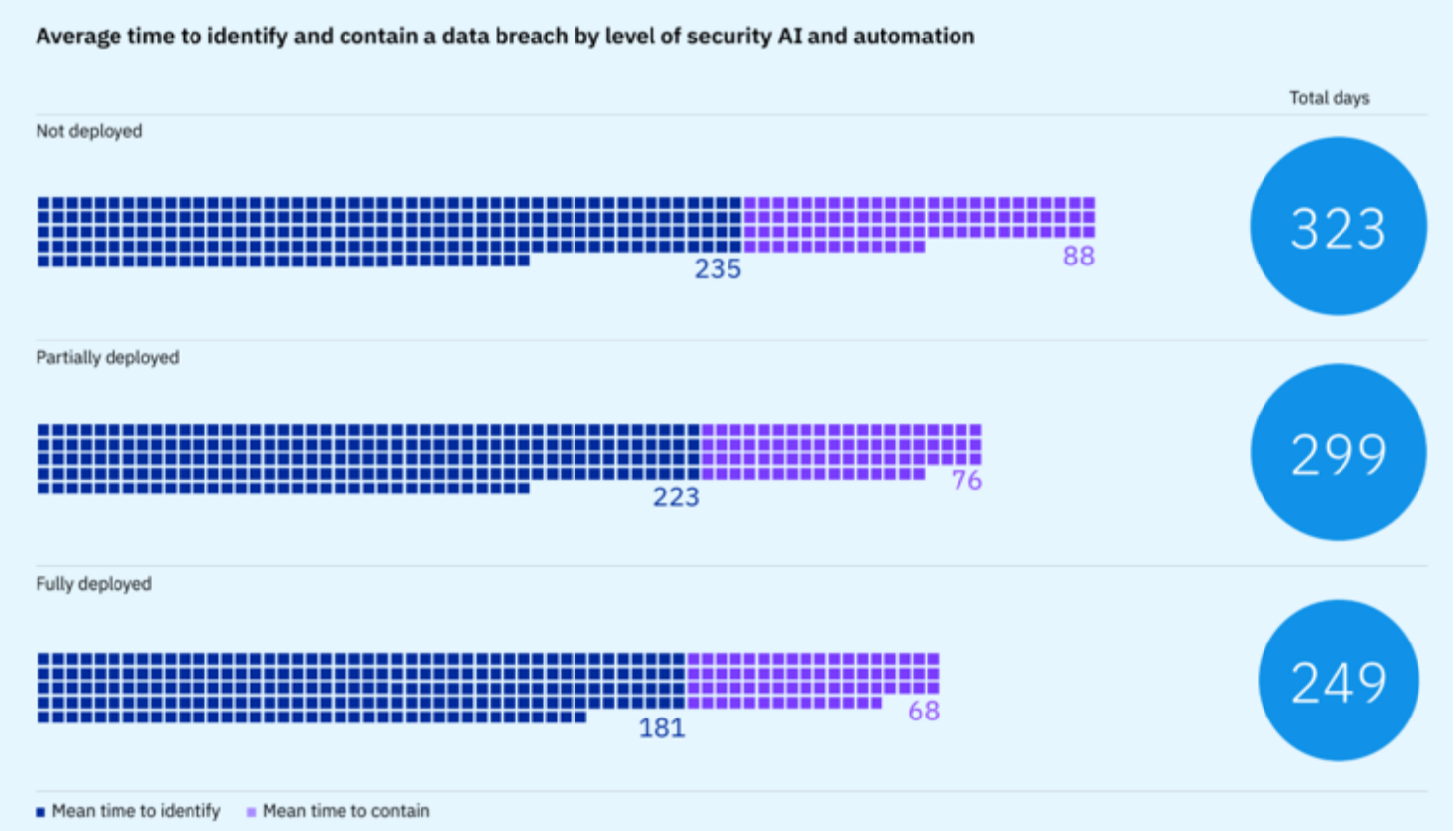
랜섬웨어

93%


Time required
to deploy
ransomware
2019: 2+ months
2021: 4 days

AI Save the time

74 Days



AI & 보안

AI를 악용한 공격

AI

적대적 AI

AI-powered Attacks
to strengthen attacks and evade detection

Leveraging Adversarial AI
to defeat protections and steal or influence AI

AI-powered Defenses
to proactively protect and disable AI-powered attacks

Countering Adversarial AI
to fortify AI to withstand adversarial environments

AI를 활용한 보호

AI

기업 AI 보호

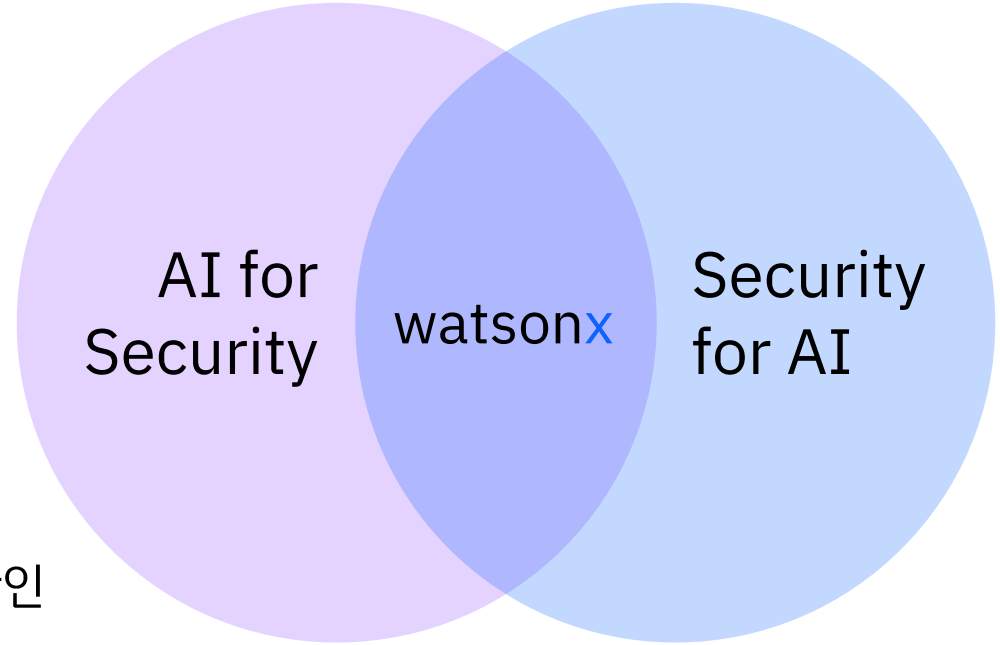
IBM의 보안과 AI 전략

보안 분야의 생산성을 향상시키는 AI

반복적인 보안 태스크 관리
- 경고 요약
- 로그 분석

보안 컨텐츠 생성
- 탐지, 워크플로우, 정책
- 급변하는 위협에 대한 빠른 탐지 및 실시간 대응

신속한 대응 학습/수행
- 유사 인시던트 발견, 감염 시스템 확인 및 취약점 패치
- 역량 강화 및 소요 시간 최적화



안전한 기업 AI 사용을 위한 보안

AI 학습 데이터의 보호
- 민감데이터 분실/조작
- 컴플라이언스 위반

AI 모델 사용에 대한 보호
- 데이터/프롬프트 유출
- 모델 대상 공격 경고 (evasion, poisoning, extraction, inference attack)

AI 대상 공격에 대한 보호
- 개인화된 피싱
- AI 생성 멀웨어
- 조작된 신원

보안 관제 업무 프로세스

Review open incidents

Choose highest priority

Triage and investigate incident

Respond

Perform root-cause analysis

Mitigation steps

Incident

Close incident

Investigate in tool 2

Investigate in tool 3

Investigate in tool 4

Determine validity / severity

Determine response steps

Build / alter playbook

Respond in SOAR

8
tools/screens

19
steps

hours - days
response time

현재의 보안 관제

수동적 방어

보안 툴 중심

전문가에 의존

독점 생태계

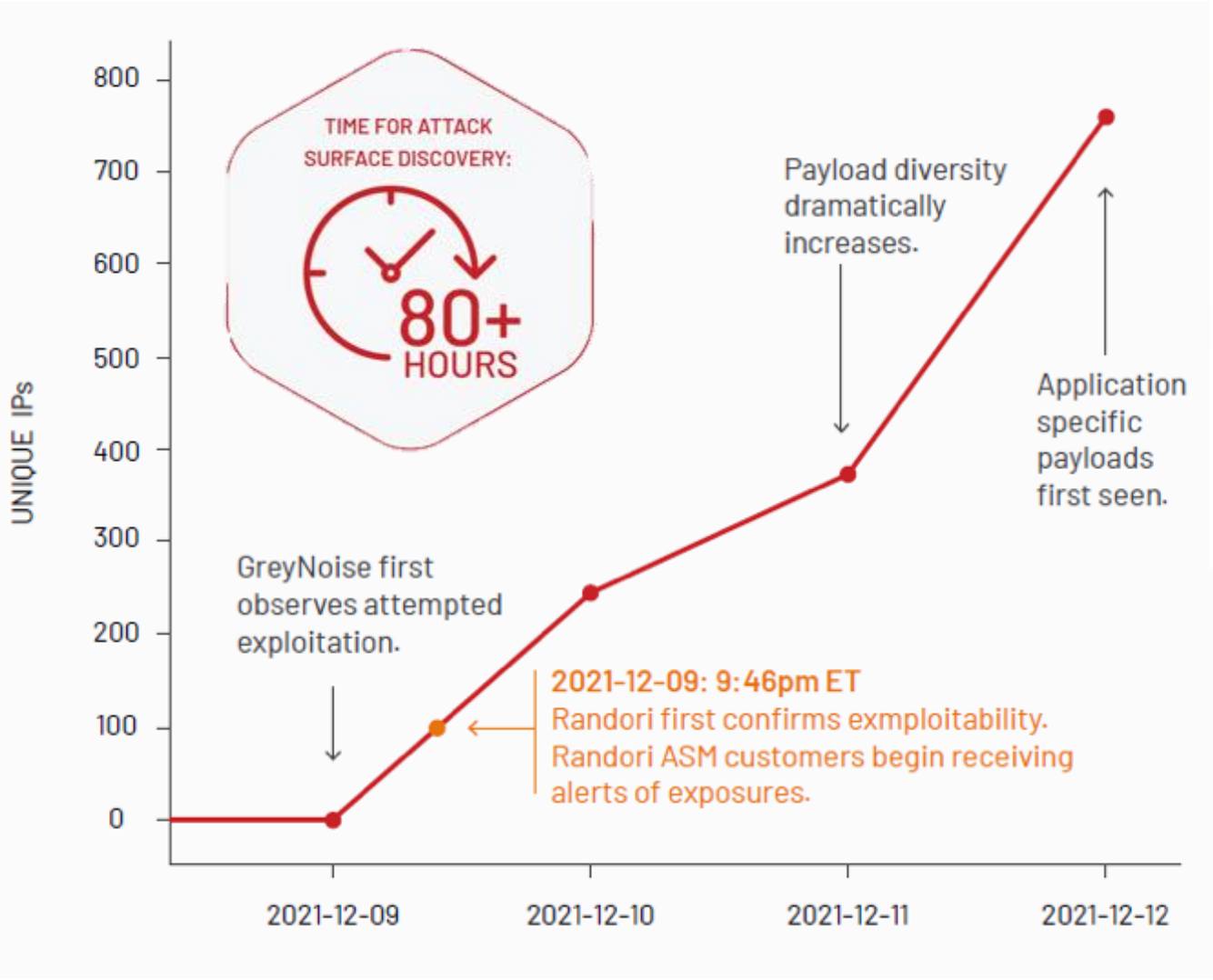
검토되지 못하는 수많은 경보

현대화된 보안 관제

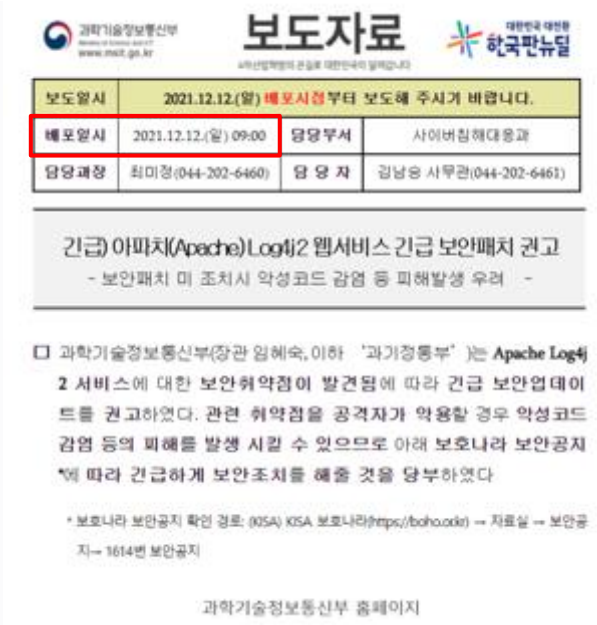
- 선제적 식별
- 분석가 중심
- 전문 지식과 AI로 확장
- 커뮤니티 협업
- 유연하게 확장되는 SOC

공격자 관점의 선제적 식별

“오늘의 위협”에 “어제의 기술”로 대응하고 있습니까?



Sources: The State of Attack Surface Management 2022, Randori



보도자료

한국판뉴딜

보도일시	2021.12.12.(일) 배포시점부터 보도해 주시기 바랍니다.		
배포일시	2021.12.12.(일) 09:00	담당부서	사이버침해대응과
담당과장	최미정(044-202-6460)	담 당 자	김남윤 사무관(044-202-6461)

긴급) 아파치(Apache) Log4j2 웹서비스 긴급 보안패치 권고

- 보안패치 미 조치시 악성코드 감염 등 피해발생 우려 -

□ 과학기술정보통신부(장관 임혜숙, 이하 '과기정통부')는 Apache Log4j 2 서비스에 대한 보안취약점이 발견됨에 따라 긴급 보안업데이트를 권고하였다. 관련 취약점을 공격자가 악용할 경우 악성코드 감염 등의 피해를 발생 시킬 수 있으므로 아래 보호나라 보안공지에 따라 긴급하게 보안조치를 해줄 것을 당부하였다

* 보호나라 보안공지 확인 경로: (KISA) KISA 보호나라(https://boho.or.kr) → 자료실 → 보안공지→ 1614번 보안공지

과학기술정보통신부 홈페이지

“Log4j 취약점 사고에 대해, Randori의 실시간 가시성은 사고대응용이 아니라 공격자보다 앞서 있었다. 공격의 첫주 우리는 log4j 관련하여 4천여건의 공격을 받았으나 우리는 이미 안전하게 조치를 완료하였다. Randori를 통한 지속적인 모니터링과 실시간 경고가 성공적 대응의 핵심이었다.”

— Philip Keibler, CISO

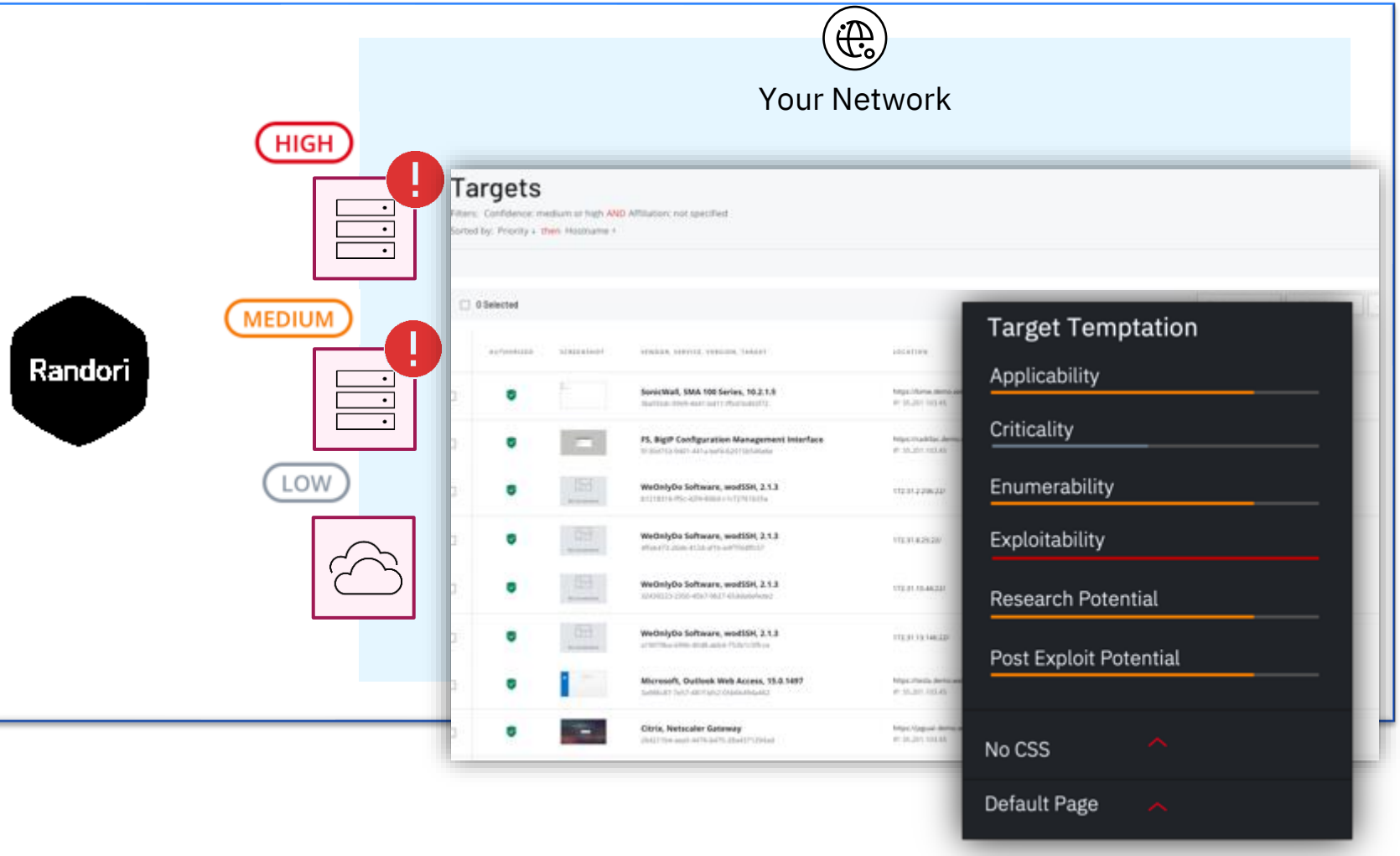
meijer

선제적 공격형 보안을 통한 지속적인 자산과 위협의 식별 - 우선순위화

02

노출 우선순위화

Randori는 특허 출원 중인 Target Temptation 모델을 통해 고위험 대상의 우선 순위를 지정하고 식별합니다.
이 모델은 적대적 통찰력을 비즈니스 범위 및 상황과 결합하여 포괄적으로 위험 지수를 산정합니다.



선제적 공격형 보안을 통한 지속적인 자산과 위협의 식별 - 최적화

05

전문가 참여 작업

재검증 & 지원

레드 팀은 공격 성공과 실패 결과를 분석하여 Gap를 포함한 상세 보고서를 제공하고 회복 탄력성을 강화하기 위한 카테고리별 지침을 제공합니다.

분석가 중심의 보안 운영

분석가 중심 설계 기반 운영 효율 제고

신속하고 빠르게 더 좋은 결정을 내릴 수 있는 공통의, 간소화한, 단일 통합 분석 환경 (Unified Analyst eXperience, UAX)

전통적인 보안 운영

8개 이상 보안 UI들

30시간 이상 툴 사용법 훈련

2일 이상 대응 시간

수동 조사

Unified Analyst Experience

1개의 공통 UX

지속적 학습

< 30분 이내의 대응 시간 [1]

자동 조사

– What?

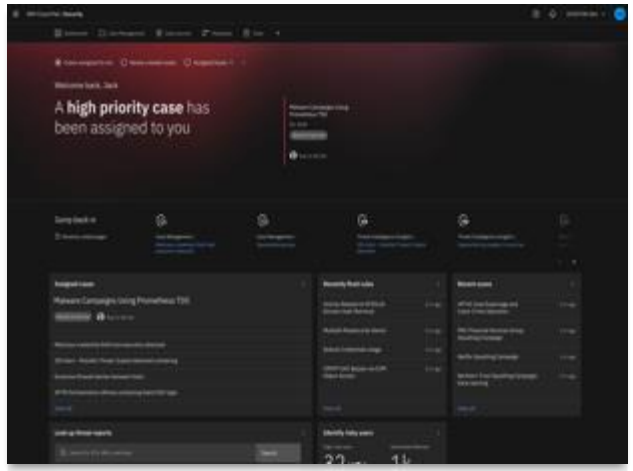
– When?

– Where?

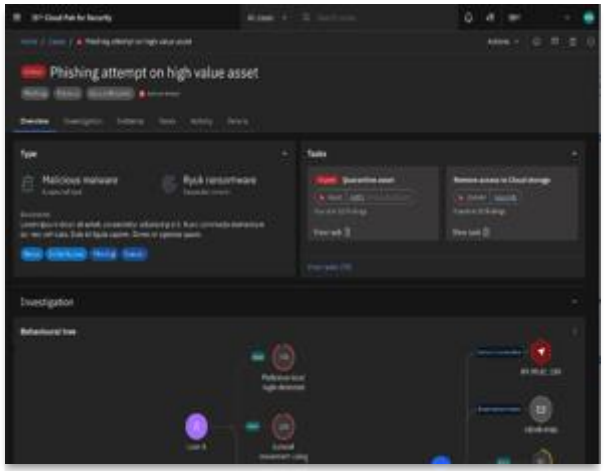
– Who?

– How?

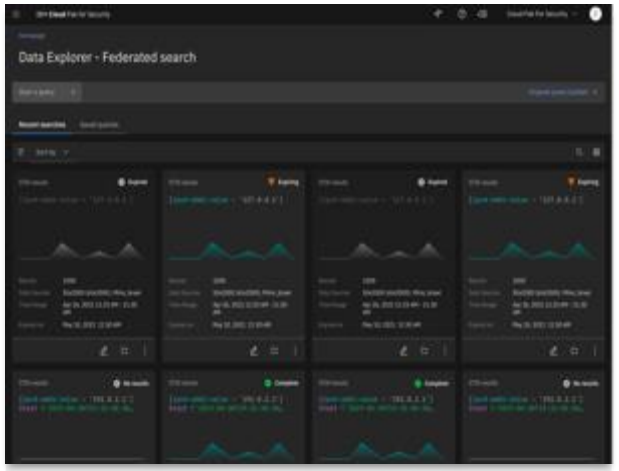
Take action



Enrich, correlate, and prioritize



Automated investigation and response recommendations



Federated search and threat hunting

90%+

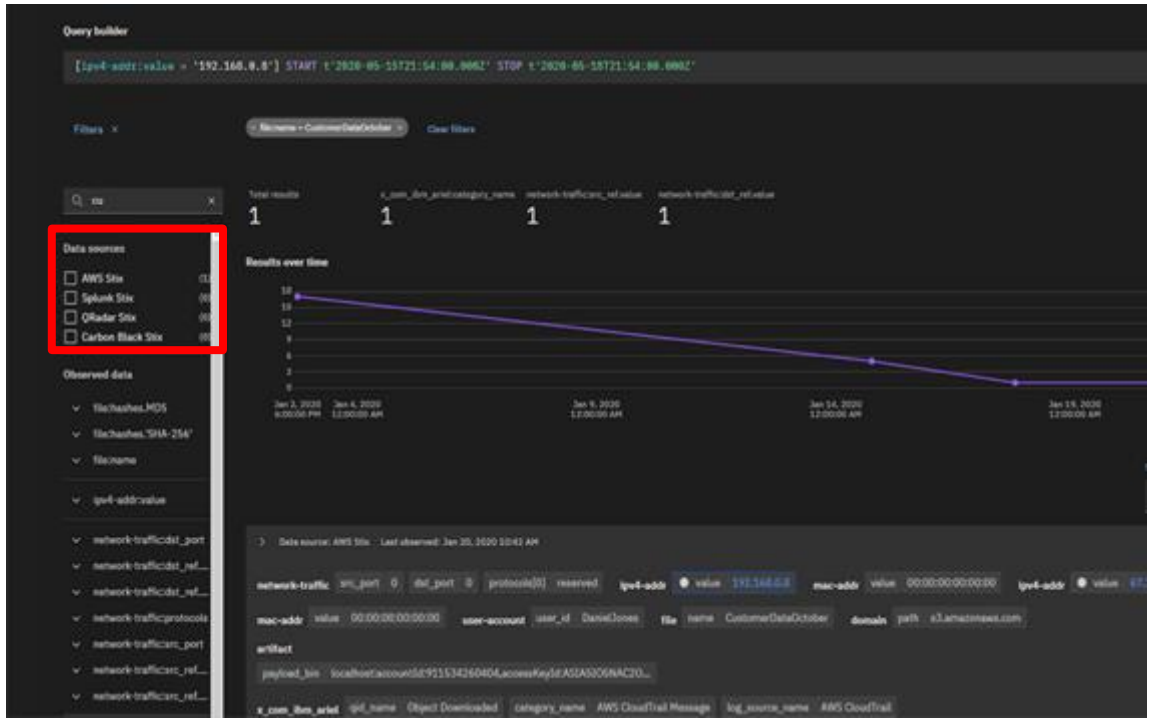
사건 조사에 소요되는 분석가의 시간 절약[2]

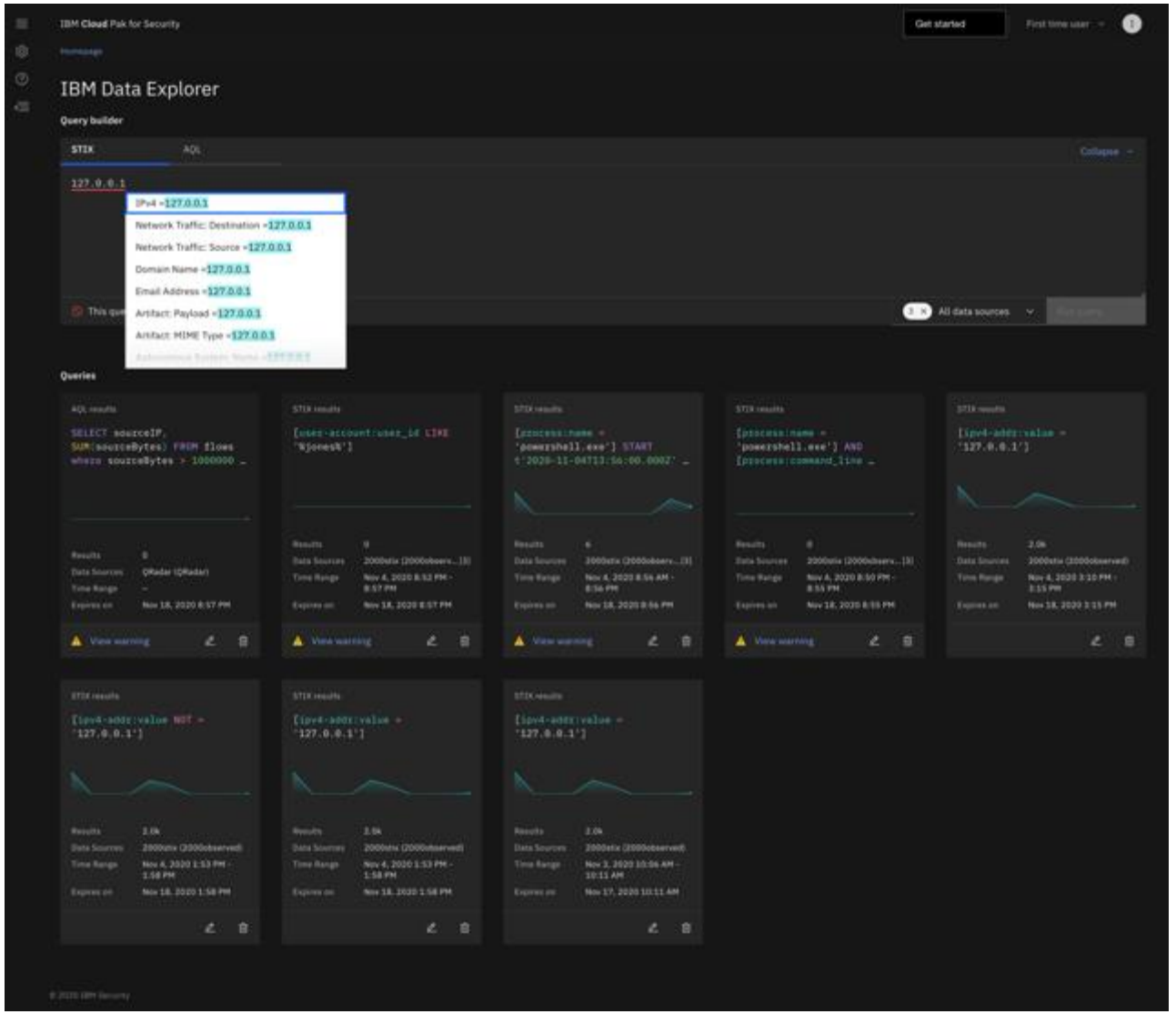
"I equate the UAX to five additional FTEs. It was easier to get better data out of my tools with AI, than investing in more people. It made my people faster and better at their job." [1]

[1] North American State Government Agency

[2] Forrester's TEI Study of QRadar SIEM, April 2023

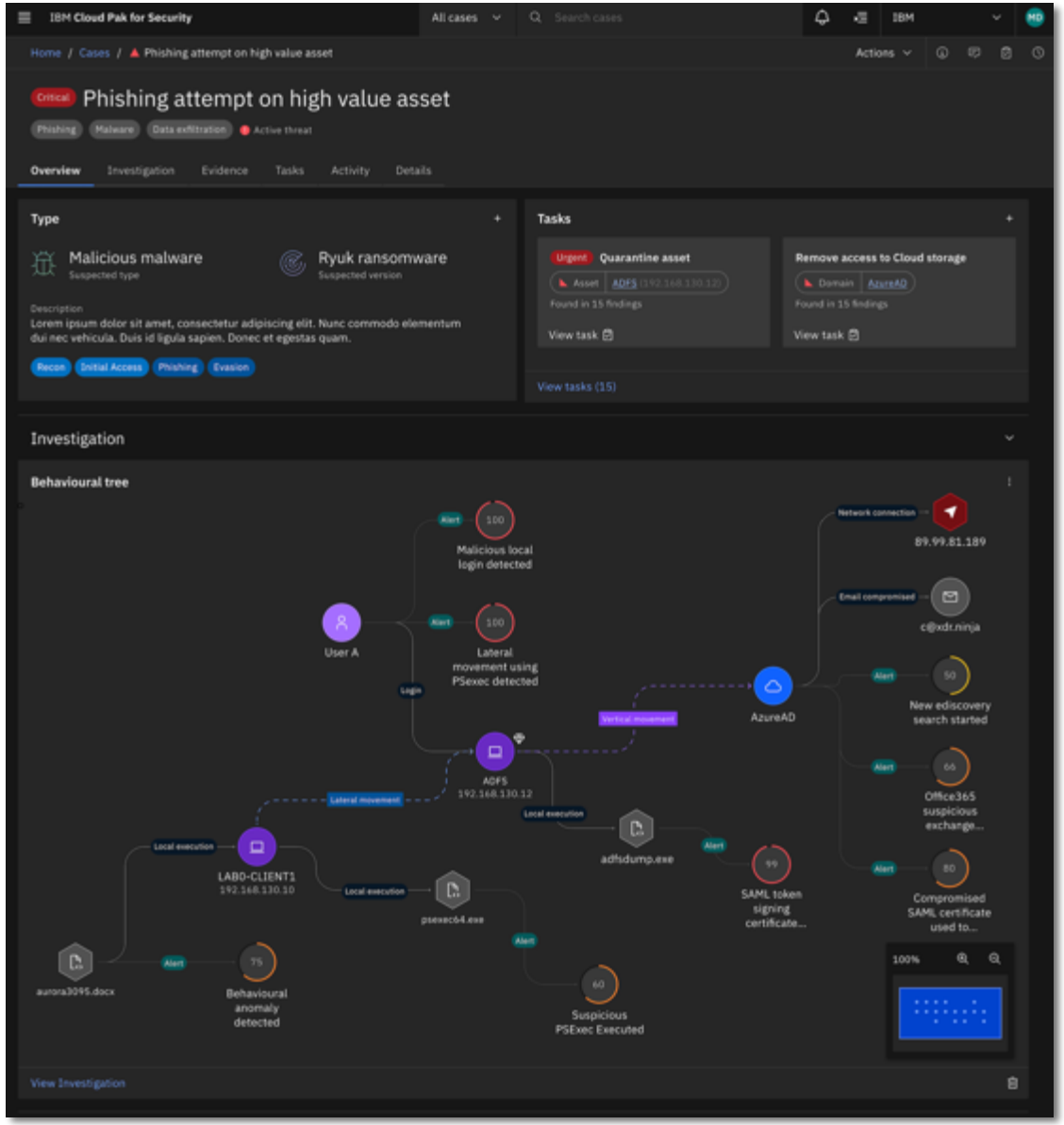
단일 UAX 분석환경에서의 통합 검색 및 조사: Data Explorer

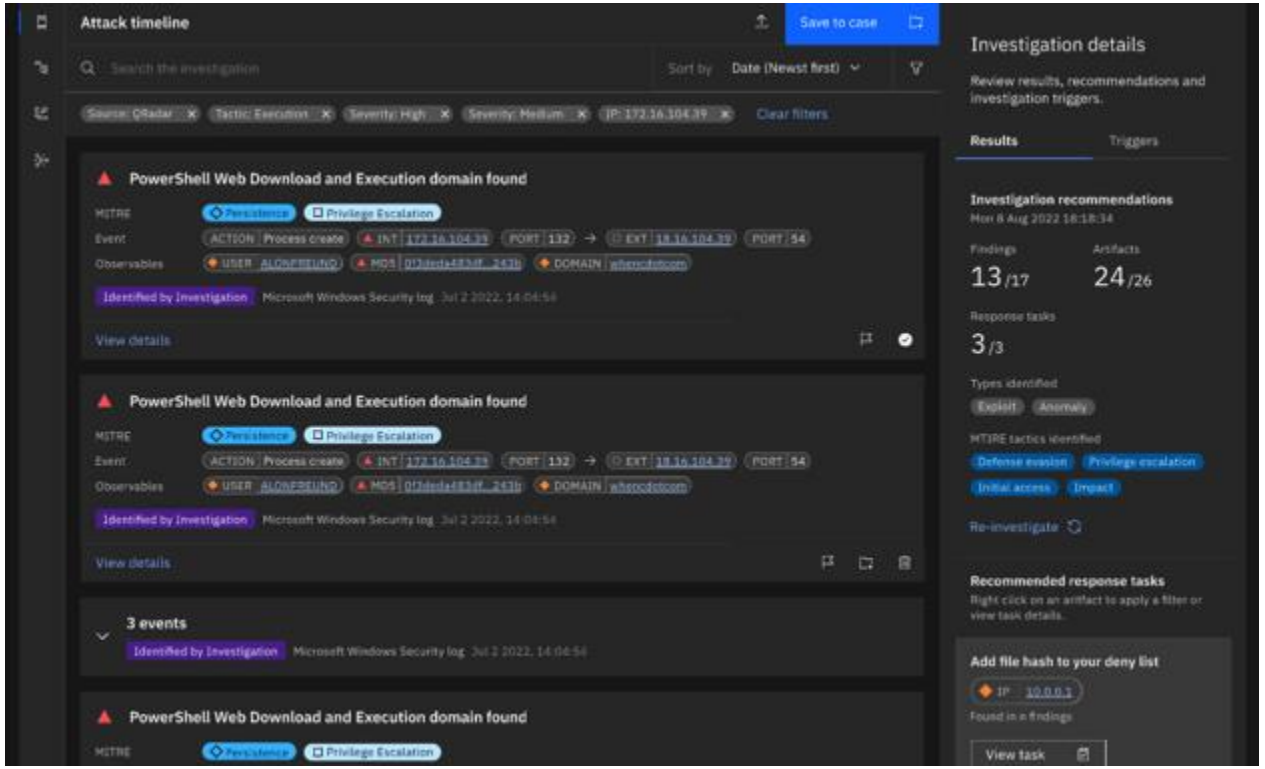




- 데이터 통합 없이 모든 **중요 보안 데이터에 대한 가시성 확보**
- 모든 데이터 소스에서의 **조사 및 위협헌팅을 위한 단일 언어**
- 위협 인텔리전스/DB, 자산 연동으로 **데이터, 속성 자동 보강**
- **쿼리가 필요 없는 통계적 통찰력** 기반 즉각적인 분석

자동화된 위협 조사 및 대응 권고를 통한 신속 대응: Threat Investigator





분석가 조사

근본 원인 조사

공격의 타임라인 보기

MITRE TTP/
위협 인텔리전스

AI

분석가 심층 분석

연결된 전사 툴에 통합 검색

현재 위협의 환경과 영향을 받는지 이해

놓친 경보와 이벤트의 분석

AI 기반 자동화된 탐지대응

AI/자동화 기반 신속하고 정확한 통찰력 확보

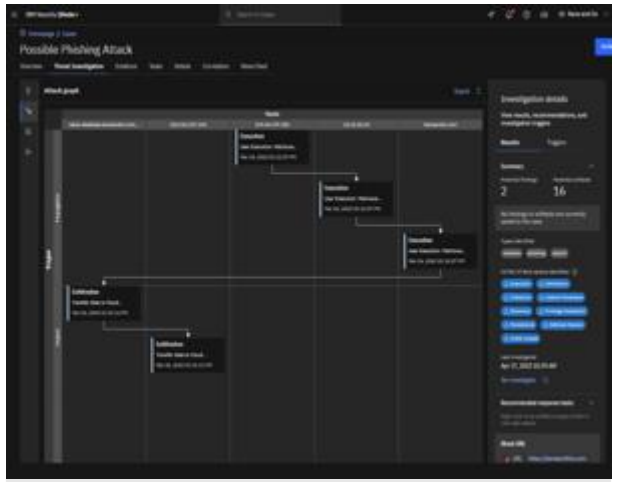
자동화되고 지능적인 감지 및 대응으로 SOC 간소화

위협에 대한 자동화된 대처

지속적으로 업데이트되는 X-Force, 커뮤니티 위협 방지, 탐지 인텔리전스 및 AI는 이전에 볼 수 없었던 위협을 거의 실시간으로 자동으로 감지하고 대응함

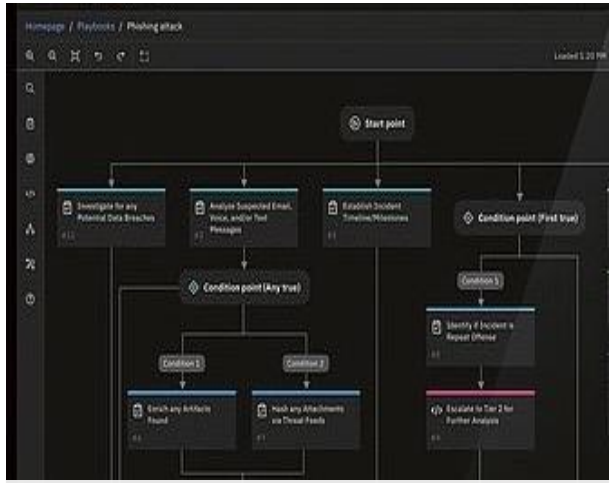
Threat Investigator로 분류 및 조치를 가속화함

AI를 활용하여 위험의 신뢰성, 관련성 및 심각도를 기반으로 충실도가 높은 경고를 신속하게 조사하고 우선 순위를 지정함



자동화 및 오케스트레이션으로 더 빠르게 대응함

사람, 프로세스 및 기술을 결합하는 동적 플레이북으로 7배 더 빠르게 대응함



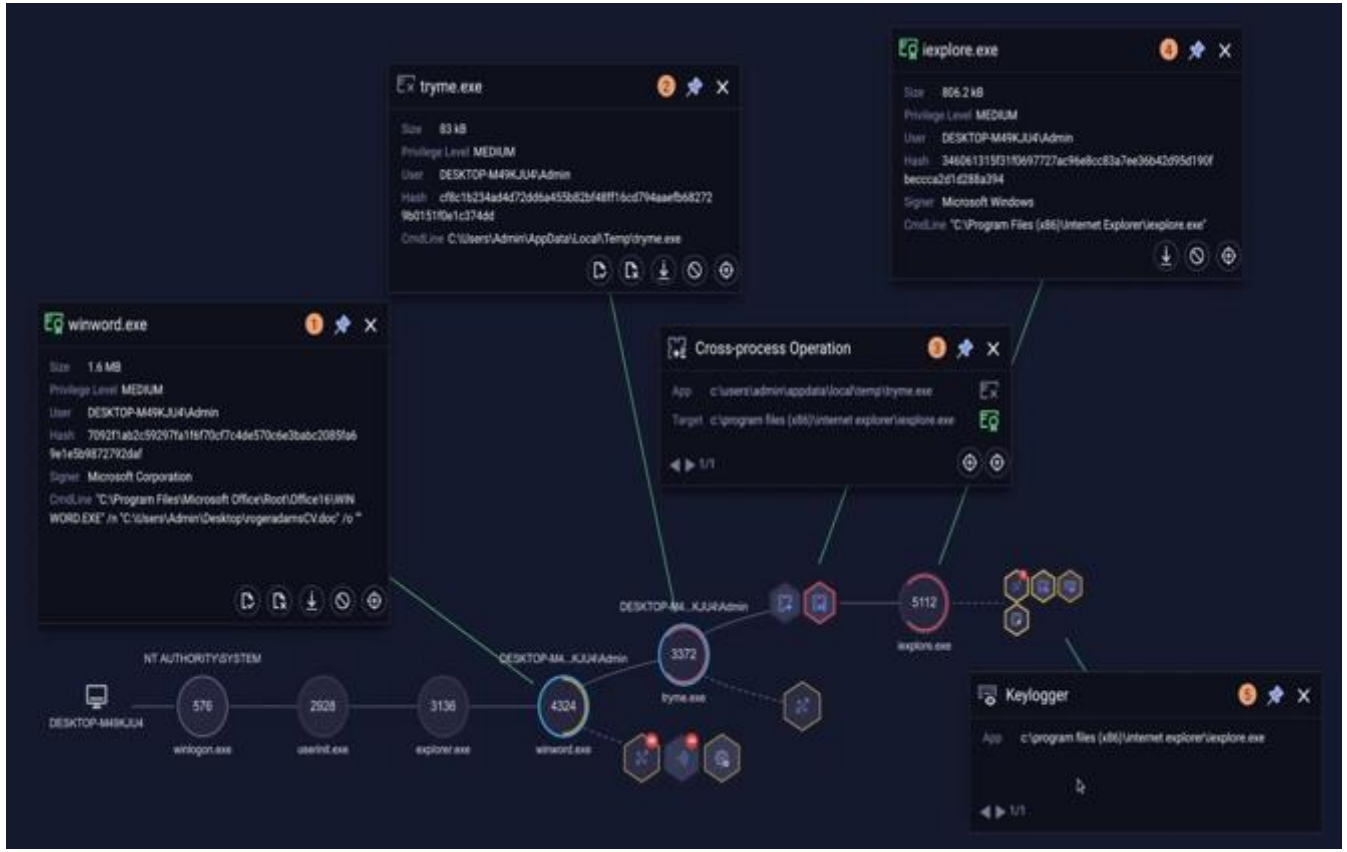
85%
침해 대응 시간 절감[1]

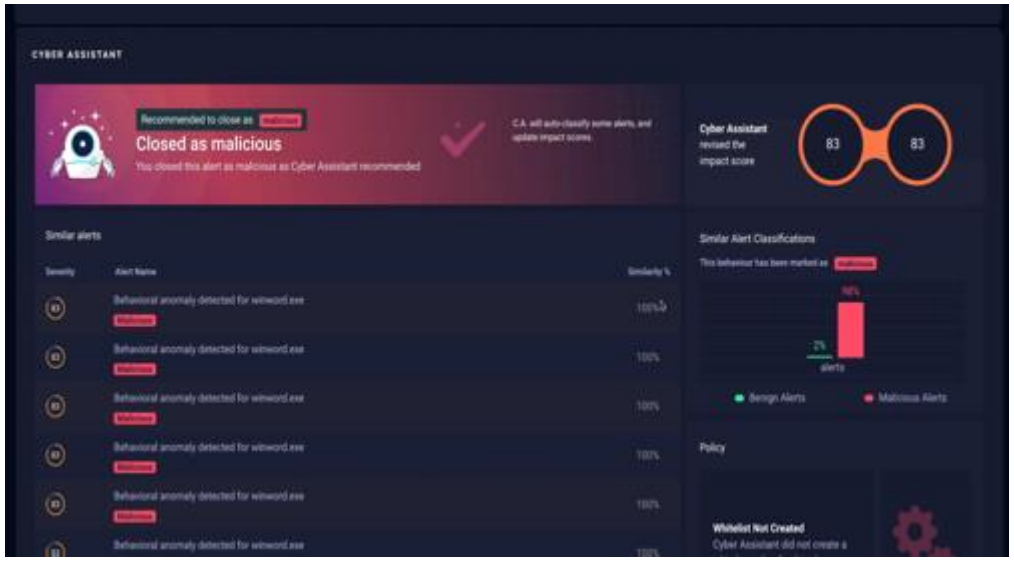
75%
보안 침해 위험 경감[2]

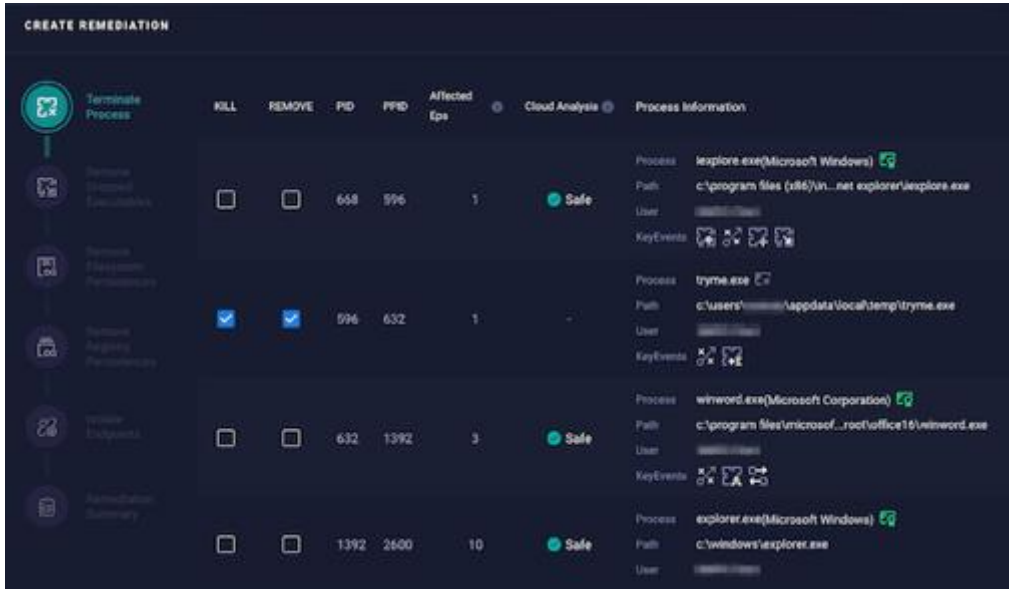
[1] ibm.com/case-studies/doosan-digital-innovation
[2] Forrester's TEI Study of QRadar SIEM, April 2023

운영 부담을 최소화하는 자동화된 보호: Endpoint Detection and Response

- **직관적 대시보드의 가시성**과 즉각적 대응 실행력
- **상관분석 기반의 최소화된 이벤트 및 경고** 통해 효율적 운영
- **AI 기반 탐지와 대응 자동화 및 추천**으로 실시간으로 자동 탐지, 경보 처리 및 신속하고 정확한 대응







오픈 생태계 기반 확장

기 보유한 보안 솔루션을 활용하여 원하는 방향으로 확장함

연합 검색을 통한 개방형 접근 방식은 데이터가 있는 곳에서 데이터에 액세스하거나 필요할 때 통합할 수 있는 유연성을 제공합니다

3,000+ Open Sigma SIEM rules

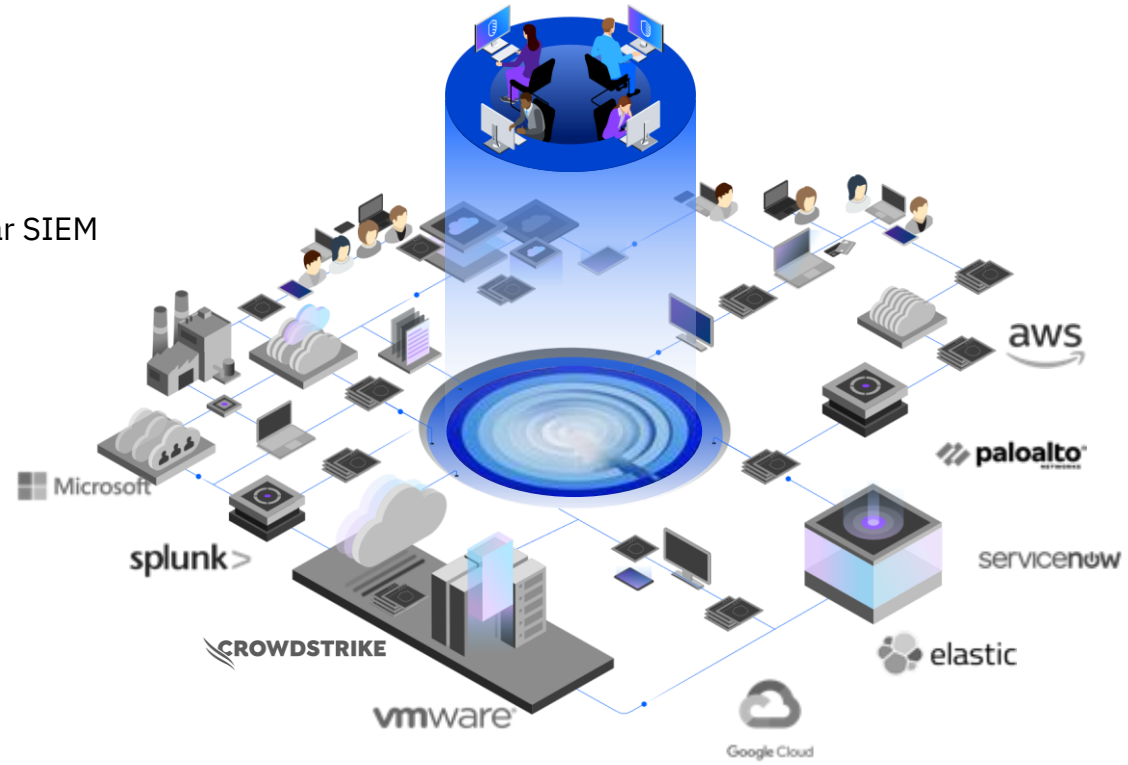
550+ Log adapters and apps for QRadar SIEM

300+ QRadar SOAR integrations

40+ Federated search sources

10+ Threat intelligence sources

150+ Open ecosystem vendors



"QRadar can be deployed and quickly start working from day one."[2]

"The extensive information captured in QRadar provides insights and time savings for users beyond the security team."[2]

[1]G2 Customer review
[2]Forrester's TEI Study of QRadar SIEM, April 2023

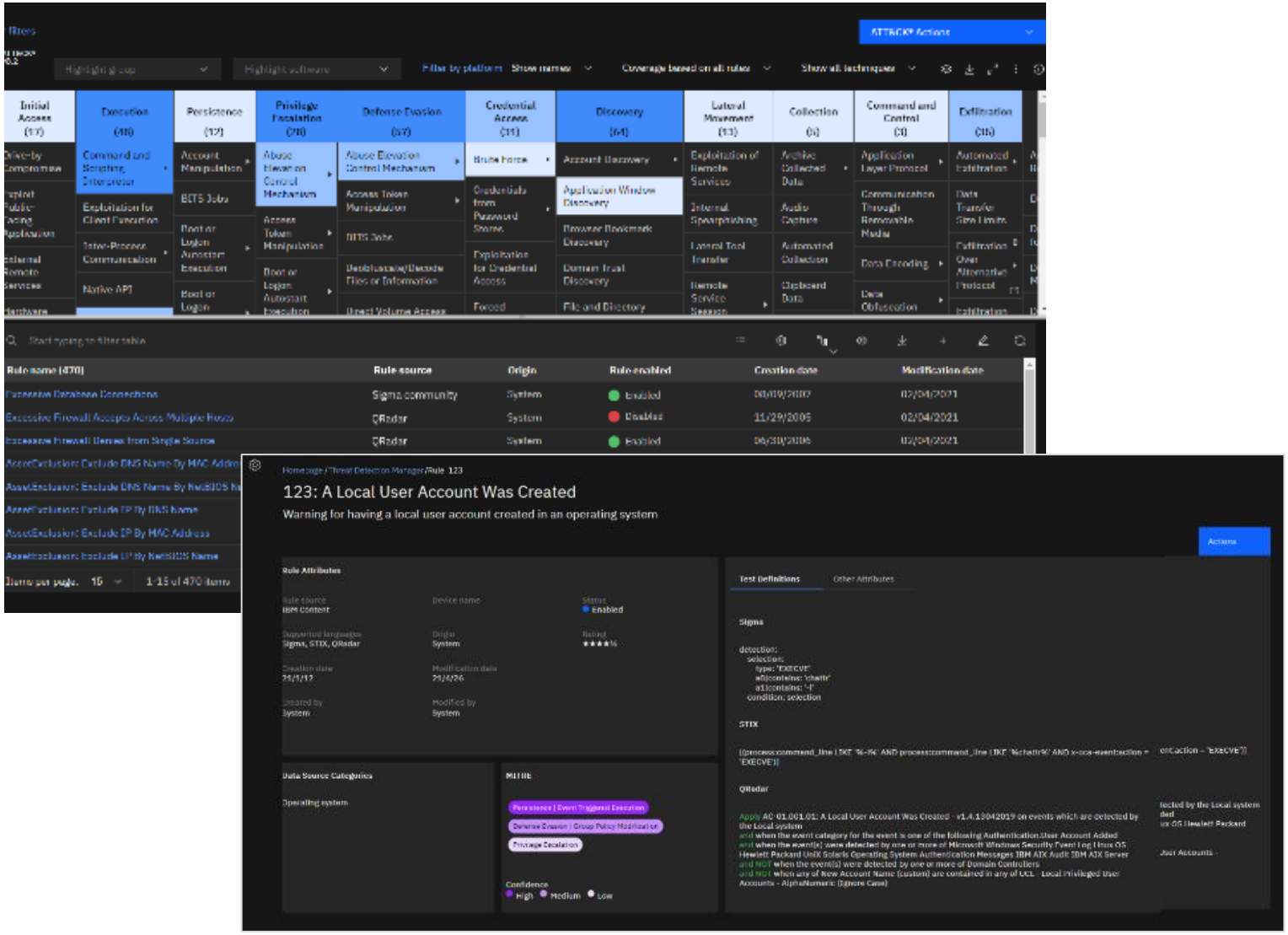
생태계의 중심에 있는 수천 개의 개방형 통합

오픈 소스와
오픈 커뮤니티

유연하게 확장되는 SOC

지속적인 위협 관리의 확장: Threat Detection and Response Center

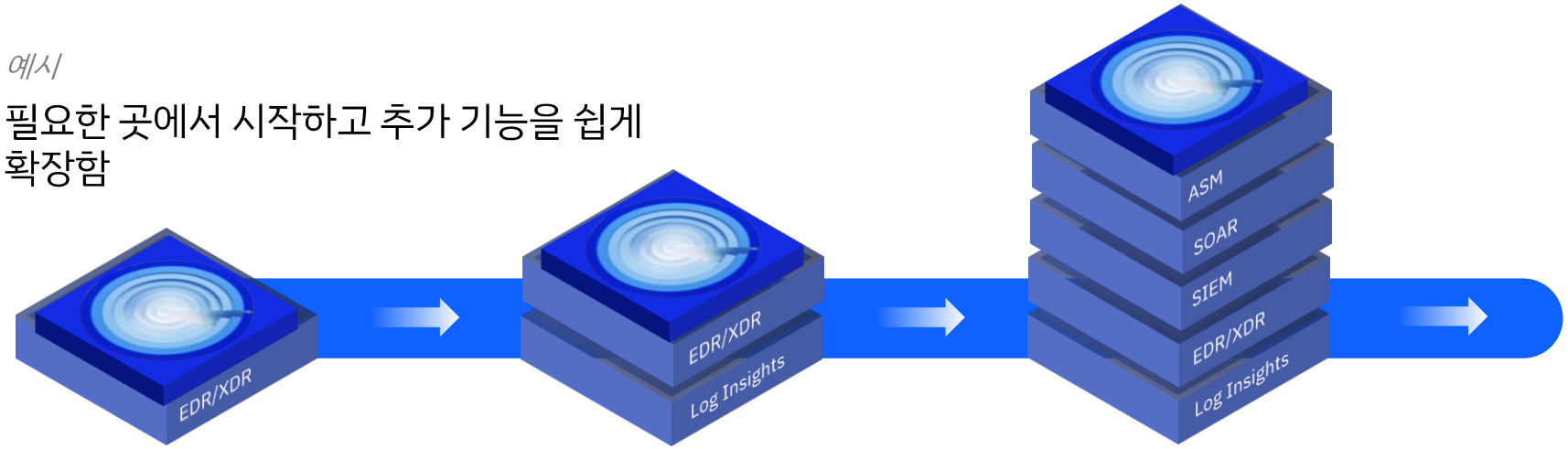
- 탐지, 위협 헌팅, 대응 사용 사례 및 적용 범위의 중앙 집중식 관리
- **새로운 유즈 케이스 채택**이 쉬워 짐
- 탐지 및 대응 최적화
- 다양한 SIEM 및 EDR 플랫폼 지원
- 유즈 케이스를 위한 **SIGMA 룰** 지원
- **MITRE Framework** 기반 룰 커버리지



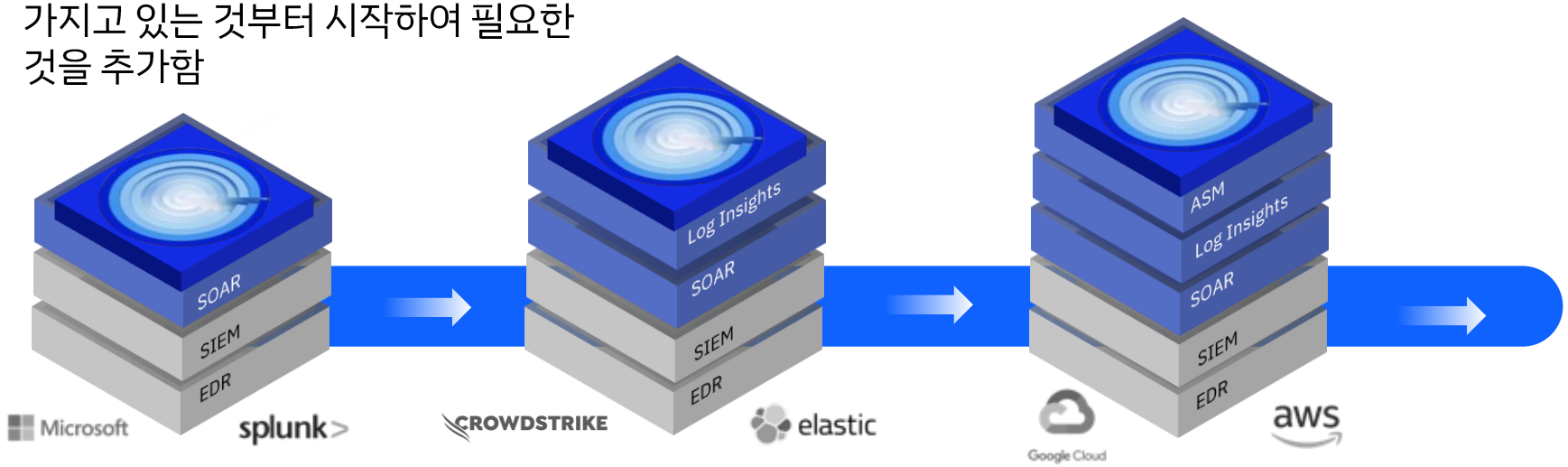
필요한 곳에서 시작하여 보안을 가속화 하십시오

예시

필요한 곳에서 시작하고 추가 기능을 쉽게 확장함



가지고 있는 것부터 시작하여 필요한 것을 추가함



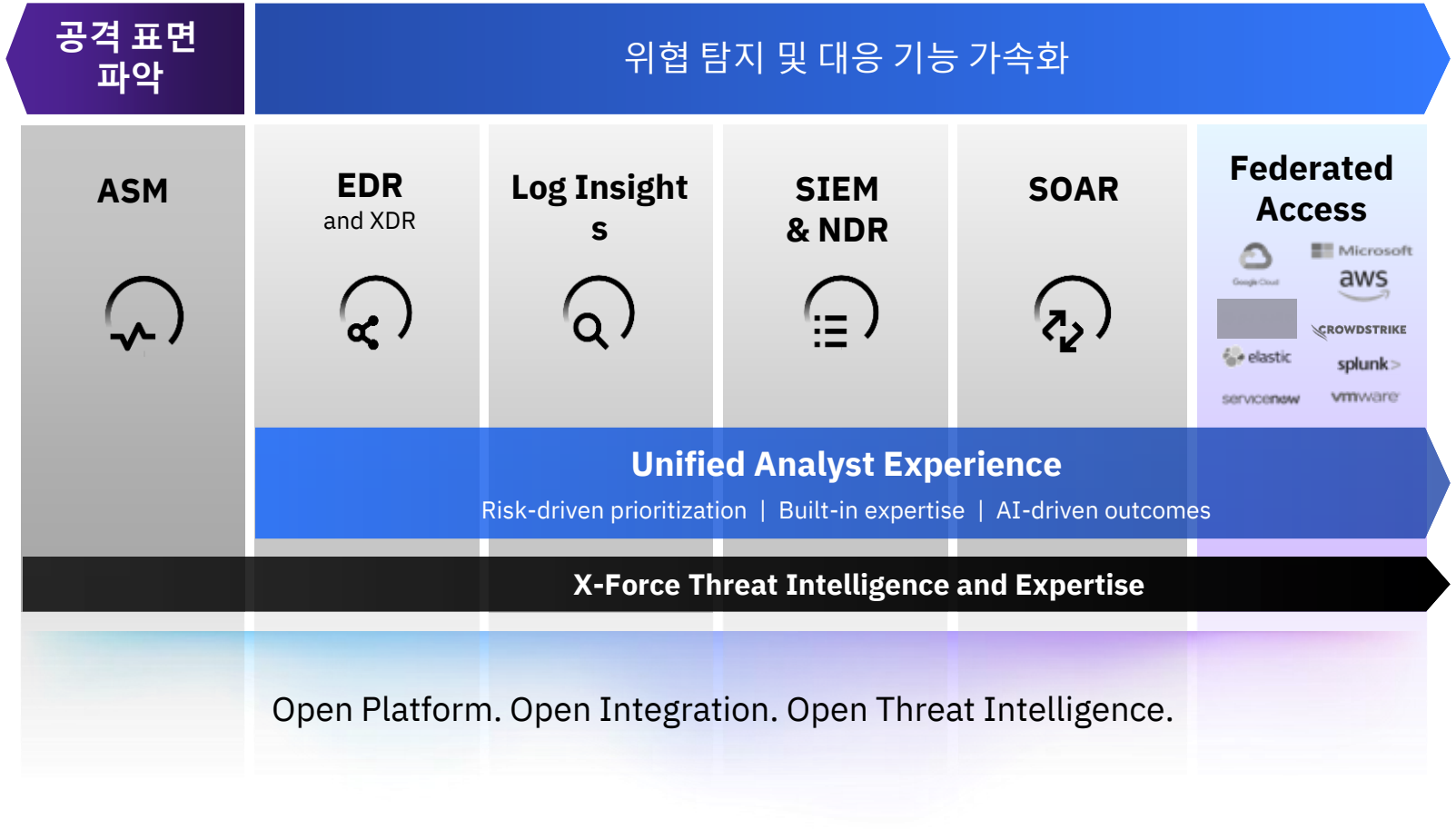
- 단계별 채택을 허용하기 위해 기존 솔루션과 함께 사용할 수 있는 광범위한 통합 세트 제공
- IBM 솔루션의 폭넓은 채택은 약간의 추가 교육 또는 통합으로 분석가 경험에 기능, 컨텍스트, 통찰력 및 자동화를 추가함
- 라이선스 소프트웨어 또는 SaaS로 사용 가능

보안 현대화를 지원하는 IBM QRadar Suite

더 빠른 속도와 가시성으로 보안 운영 현대화

Predict, prevent, and respond to modern threats

IBM Security QRadar Suite 의 진화



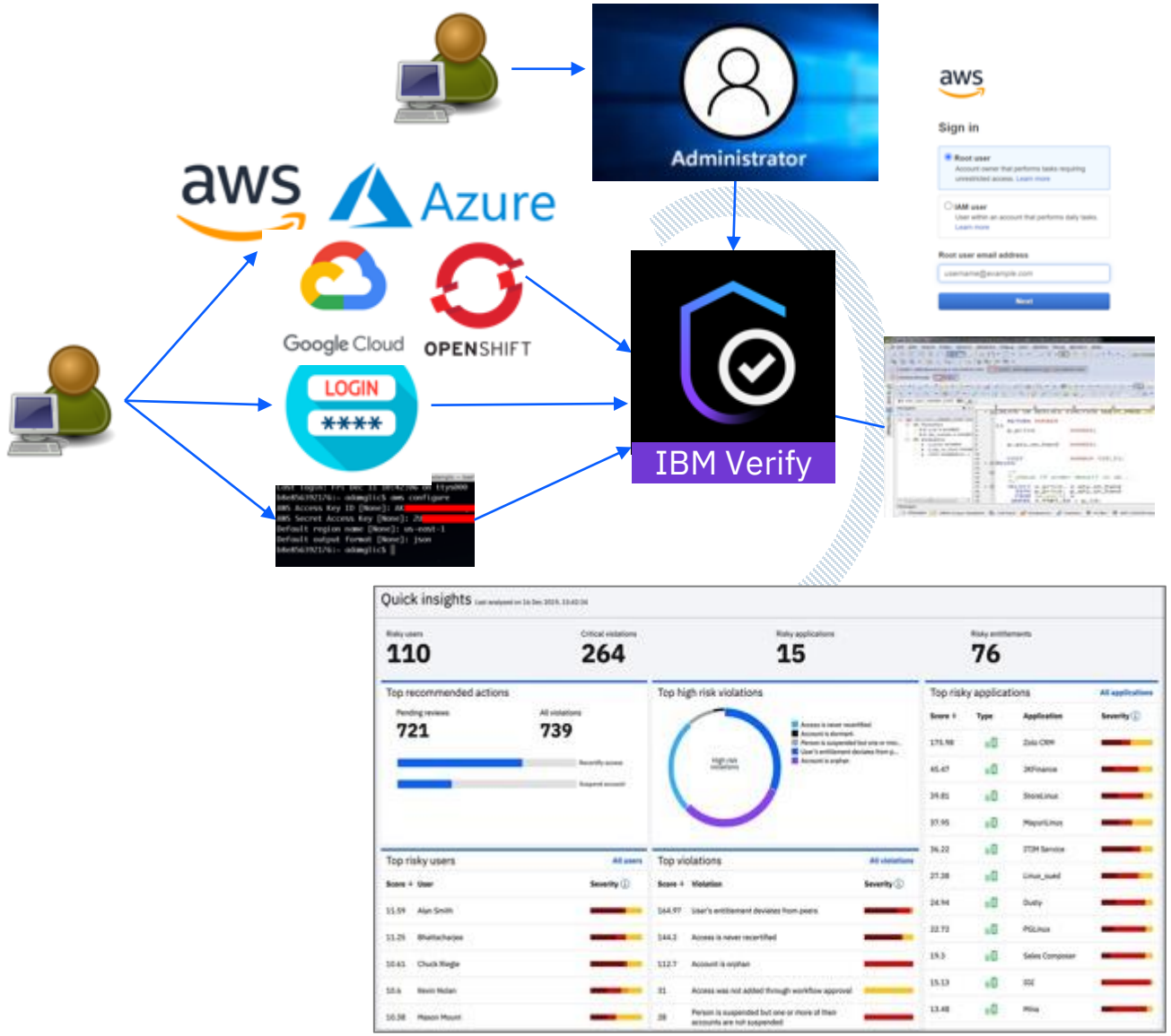
분석가 경험을 중심으로 설계
신속하고 빠르게 더 좋은 결정을 내릴 수 있는 공통의, 간소화한 통합 분석 환경 (UAX, Unified Analyst eXperience)

신속하고 정확한 인사이트 확보
분석가를 위해 설계된 자동화 및 AI, 지속적으로 업데이트되는 위협 X-Force 위협 탐지 및 대응 전문 지식을 통한 워크플로 간소화

기존 보안 솔루션 기반 유연한 확장
연합 검색을 포함한 양방향 통합을 통해 개방형 모듈식 플랫폼, 표준 및 에코시스템을 사용하여 상황에 맞게 구축

기업 보안 현대화 사례

#1 인증 체계 강화와 보안 인텔리전스를 활용한 제로 트러스트 구현 사례



Zero Trust Approach

- 다중 인증 (MFA) 및 통합 인증 기반 인증 체계 강화
- 애플리케이션/서비스 단 마이크로 세그멘테이션 구현
- 아이덴티티 기준 소프트웨어 정의 경계 수립

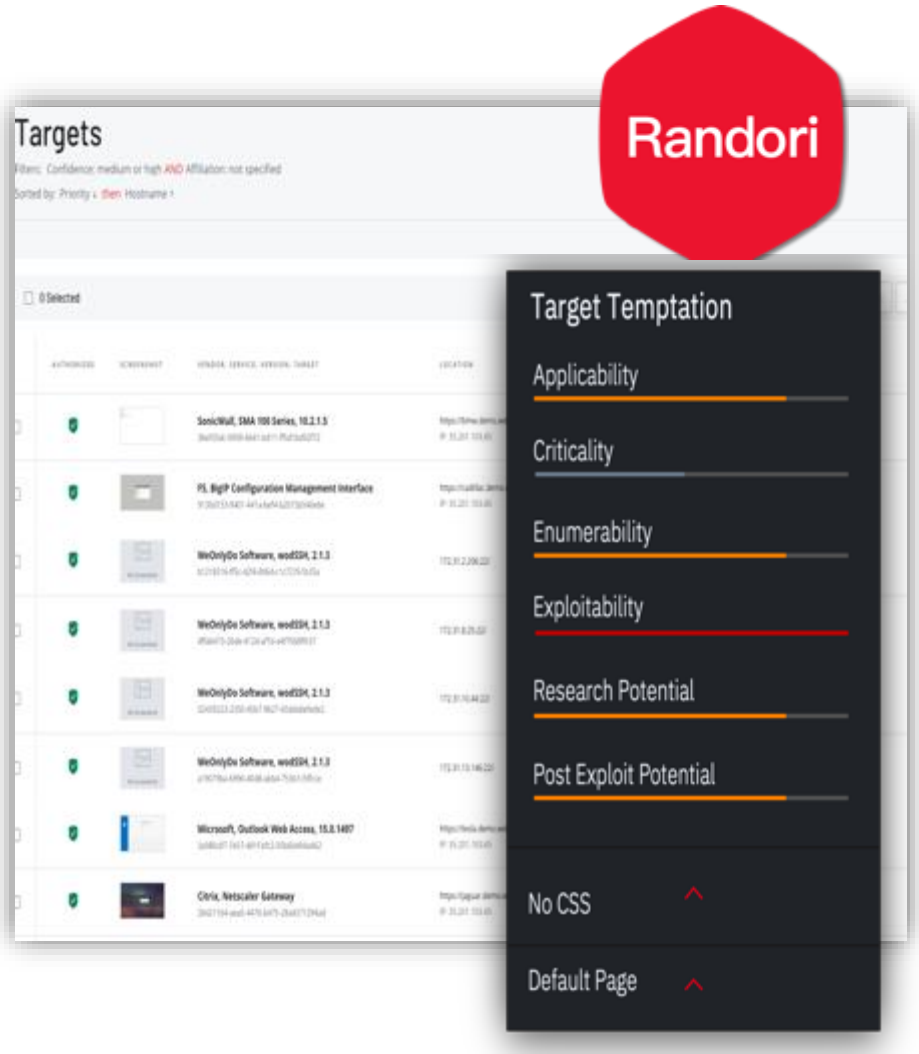
Risk based Access

- 위험 사용자 식별/과도한 권한 제거를 위한 진단
- 신뢰도 기반 동적 인정 정책 수립 및 위험 기반 인증
- 사용자 경험 개선

Threat and Fraud Integration

- 이상 접근 패턴 기반 의심 사용자 탐지
- 위협/사기 대응을 위한 신원 재확인
- 계정 활성화를 위한 재인증

#2 공격 표면 관리를 통한 선제적 위협 대응 사례



Attack Campaign #1

- RDP 연결 확인
- 레드 팀 사후 보고서 브리핑
- 고객: 공격 가능 윈도우 검토 후 대응없이 종료

Attack Campaign #2

- RDP 연결 접근
- 잘못된 구성과 USB 드라이브 연결
- 관리자 계정 복호화
- 평문화된 계정정보 탈취
- 전체 도메인 정보 탈취
- 레드 팀 사후 보고서

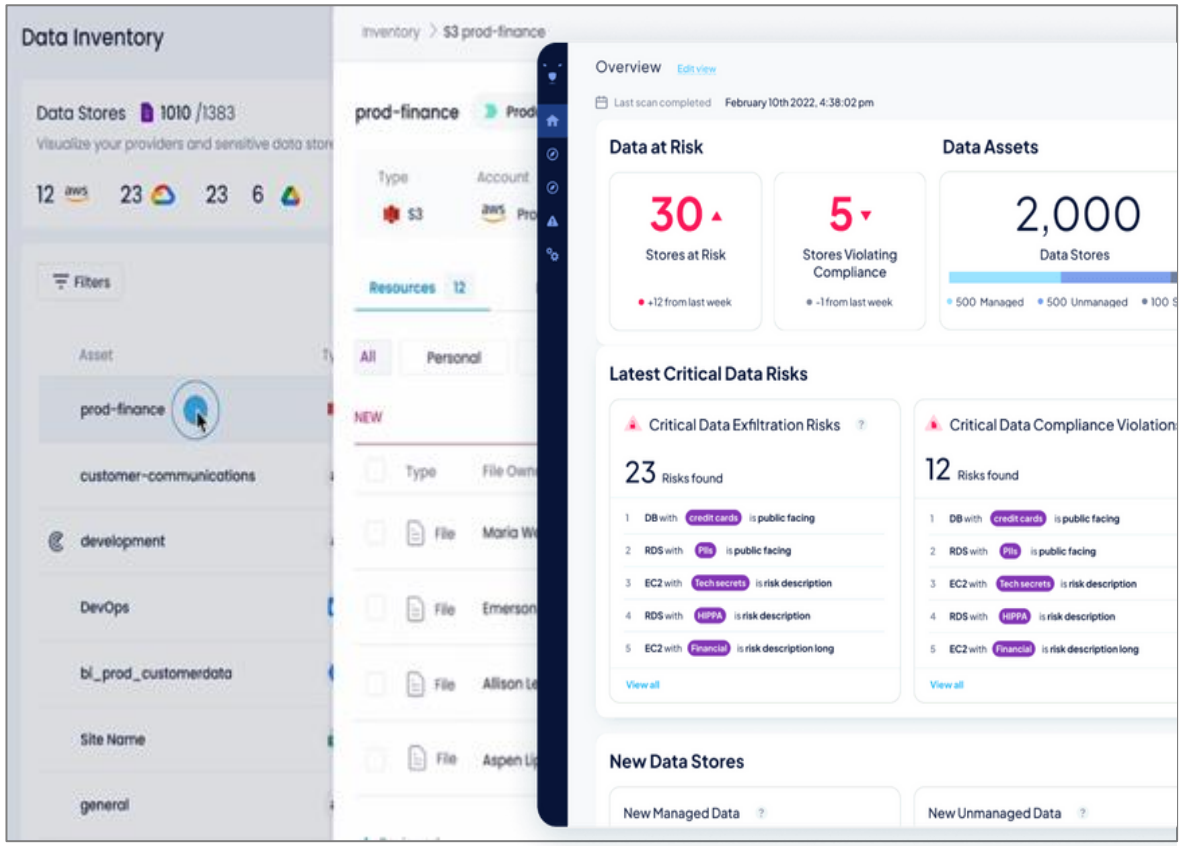
고객 자원 프로비저닝 정책 변경

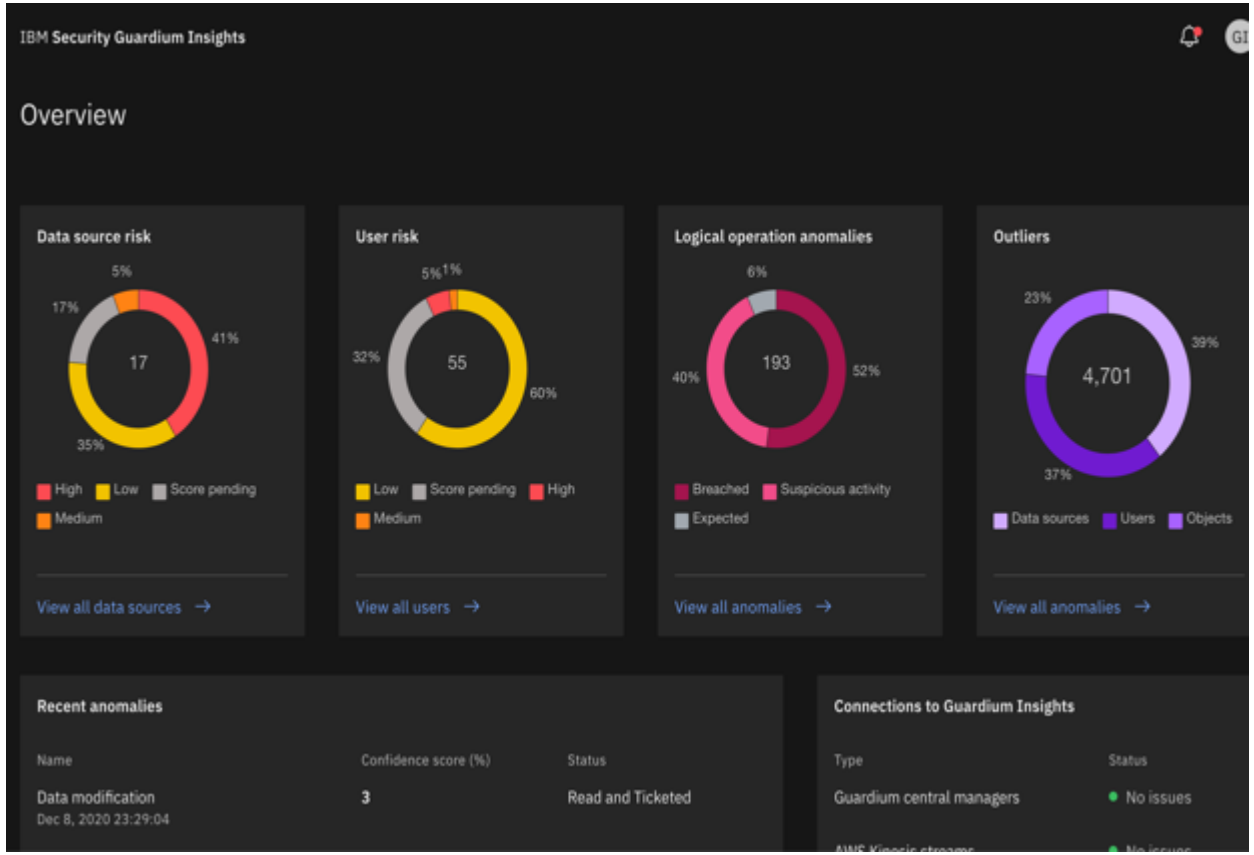
발견
RDP 연결 공개

위치
외부 피싱 캠페인 통해
내부 침투

시사점
전체 도메인 탈취

#3 클라우드 데이터 보안 형상 관리와 이상징후 분석 사례





Data Security Posture Management

- Shadow 데이터 식별 및 데이터 플로우 분석
- 데이터 취약점 식별/대응

Outlier Detection

- 데이터 접근 이상징후 탐지
- 특권사용자 이상패턴에 대한 위험 경고

기업 보안 현대화를 위한 권고사항

01 임직원과 고객에 대한 계정과 인증에 대한 위협을 관리하십시오

02 공격 표면 관리와 IR 활동을 통해 보안 회복 탄력성을 강화하십시오

03 보안 AI와 자동화를 통해 신속성과 정확성을 확보하십시오

04 하이브리드 클라우드 데이터 보안 프로그램을 현대화 하십시오


IBM