Quad Miners

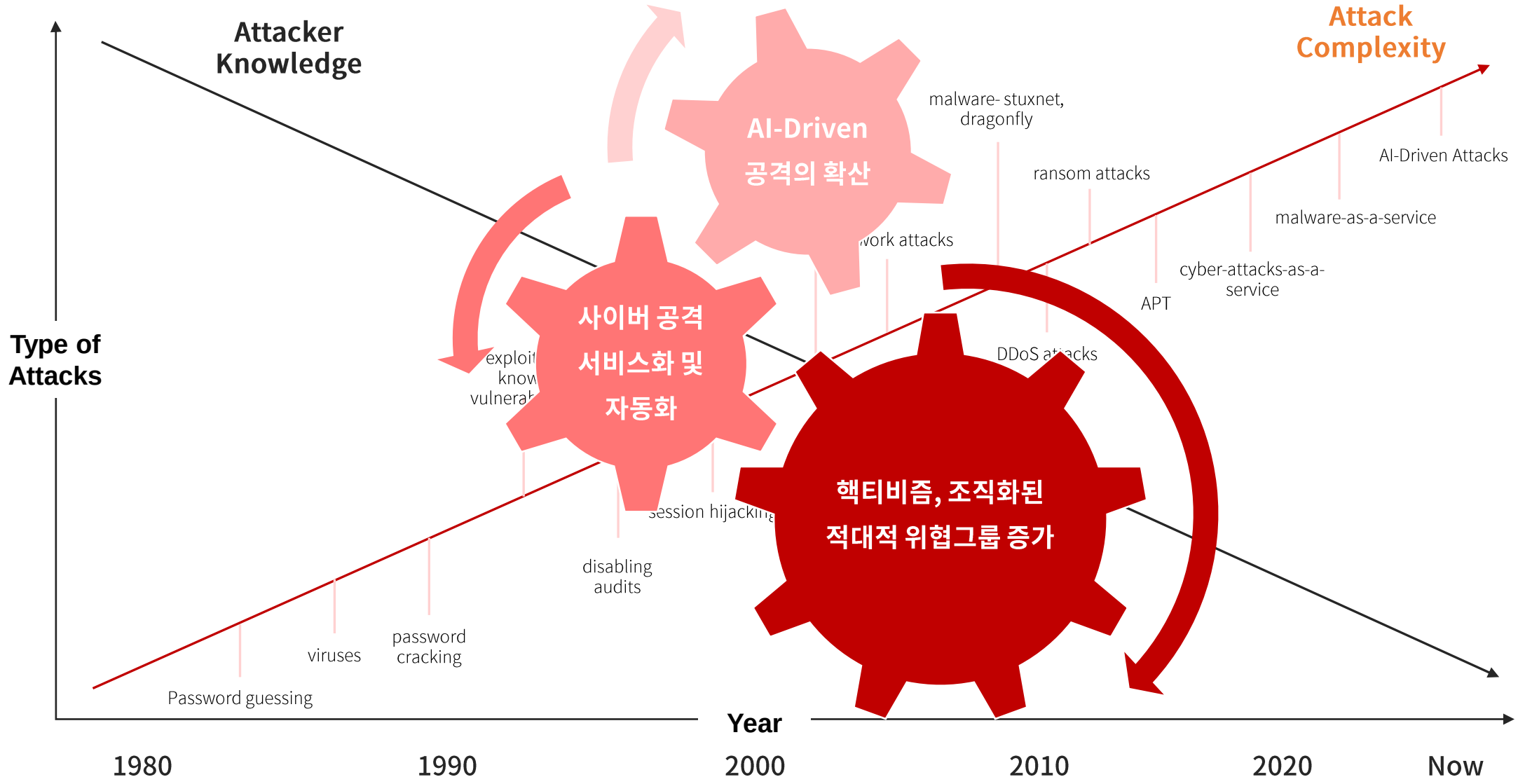
HUNT OR GET HUNTED

보안운영자동화의 과거, 현재 그리고 가까운 미래

김용호 CTO, 전략&마케팅본부

Oct 16, 2024

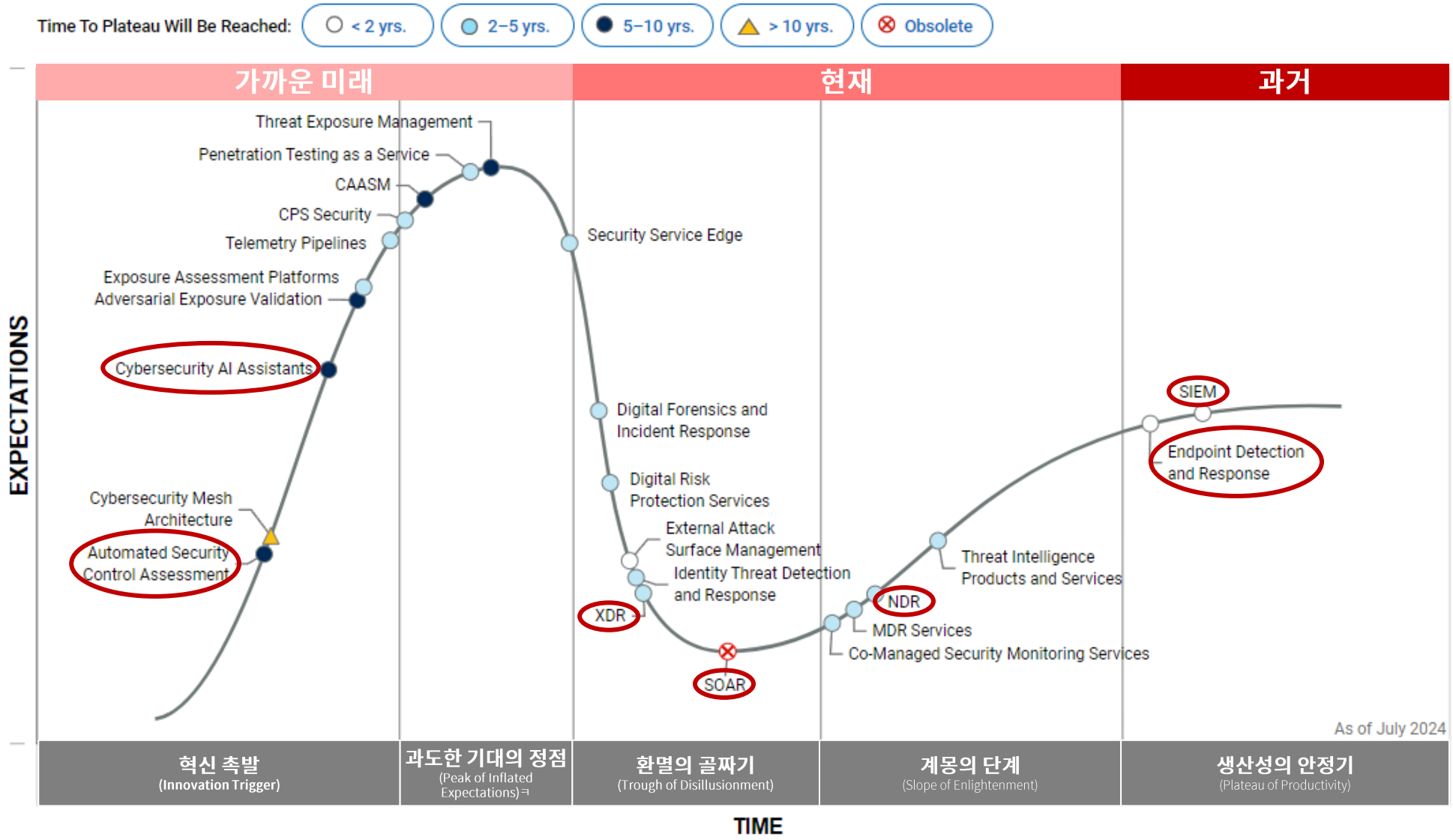
사이버 공격의 진화...당면한 현실



자료출처 : Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A., Akin, E., 2023. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics 12, 1333

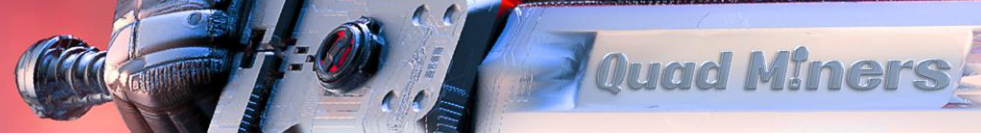
어떻게 대응해야 하나?

Hype Cycle of Security Operation



자료출처 : Gartner Hype Cycle for Security Operations, July 2024

Quad Miners' Network Blackbox



풀패킷 캡처 기반의 트래픽 전수검사를 통한 보안운영 자동화 지원, 차별화된 차세대 Network Detection and Response 솔루션

패킷스트림

- IP플로우
- 어플리케이션
- 메타데이타
- Geo IP
- 디바이스
- 이메일
- 게시판
- SNS
- 거래내역
- 번역컨텐츠
- HTML 화면복원
- POST Communication
- 파일 추출
- 세션기록

탐지

- 비정상 컨텐츠
- 비정상 세션
- 위협/공격
- 이상 트래픽
- 정책위반

헌팅

- 선제적 위협헌팅
- 알려지지 않은 위협 식별
- 잠재된 위협 식별

포렌식

무엇을, 왜, 언제, 어디서, 누가
그리고 어떻게에 대한 확정적 증적제공

50+ 컨텐츠 복원 및 추출

이메일	Gmail, Yahoo, Naver ...
게시판	Gitlab, Atlassian ...
번역	Google, BING ...
검색	Google, ChatGPT ...
채팅	Slack, Private MSG ...

100+ 파일 타입 추출 (Up/Down)

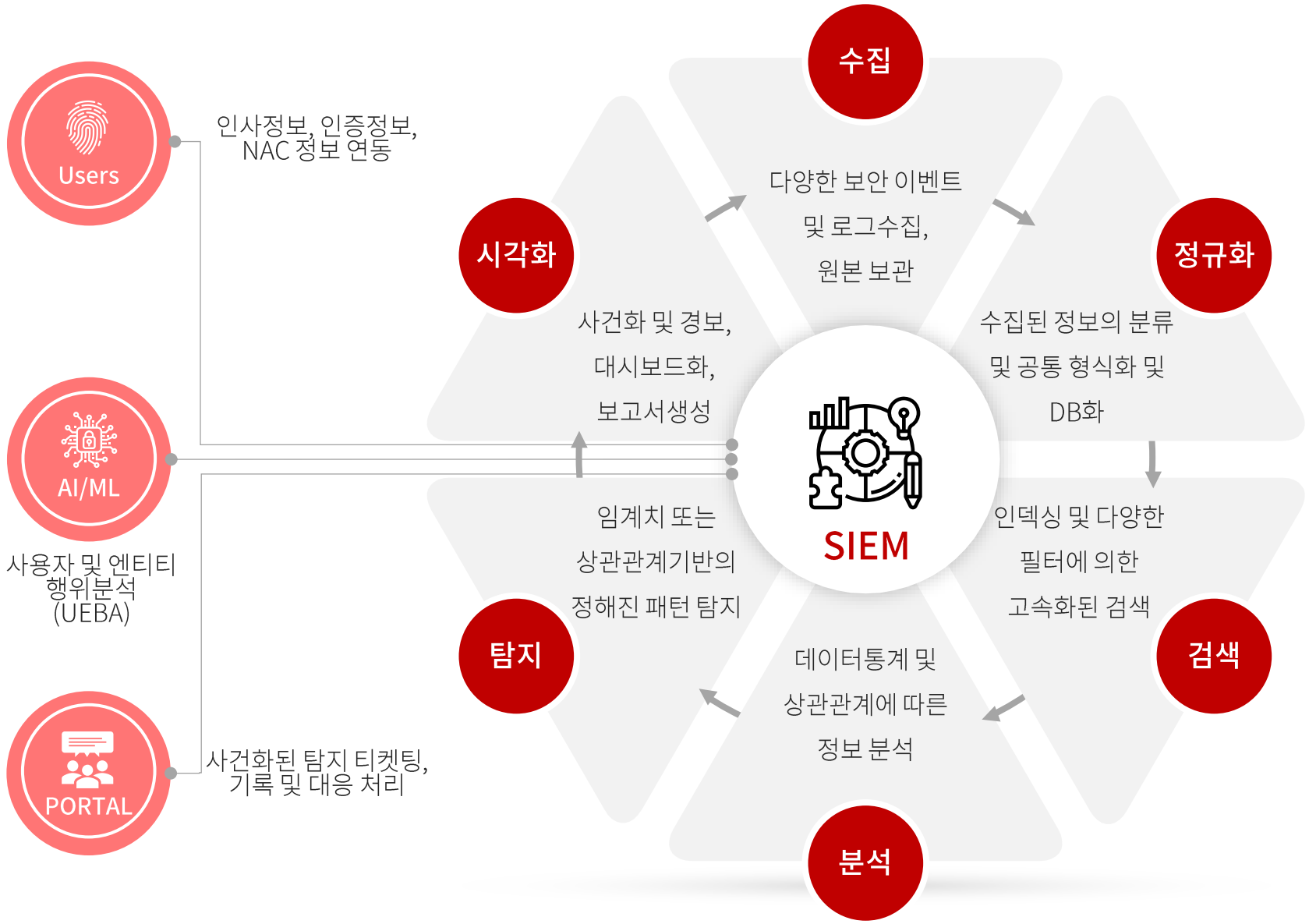
웹페이지, 문서(HWP포함), 이미지, 실행파일, 압축파일, 비디오, 오디오, ...

대응

1. 확인된 침해사고 또는 위협 관리, 조사과정 지원 및 진행상황 추적 관리
2. 탐지된 내용에 대한 분석 및 대응 자동화를 위한 타 솔루션과의 연동
3. 위협인테리전스를 활용한 위협상황 분석과 대응에 대한 의사결정 지원
4. 사후 심층적인 조사 및 원인분석 지원을 통한 선제적 재발 방지 조치 지원

풀패킷 캡처 및 수집 | **탐지** | **헌팅** | **포렌식** | **대응**

과거 : SIEM 기능의 진화를 통한 자동화 노력



기대효과

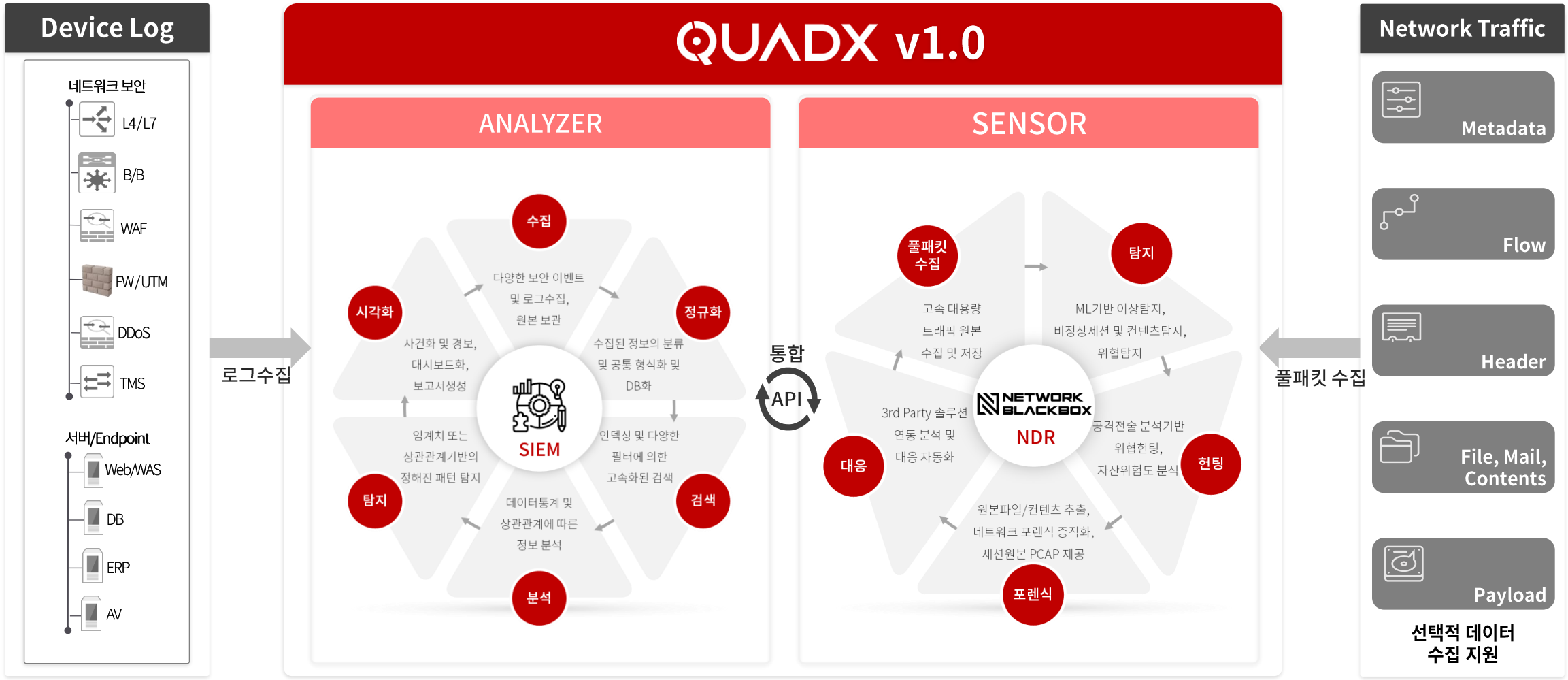
- 로그 관리 중앙화 및 자동화
- 전체적인 보안 상태 가시화
- 로그 관리 및 규정 준수 개선
- 기본적인 이벤트 상관 분석 자동화

제약사항

- 높은 오탐율
- 사건 수동 조사 필요
- 확장성 문제
- 경고 피로

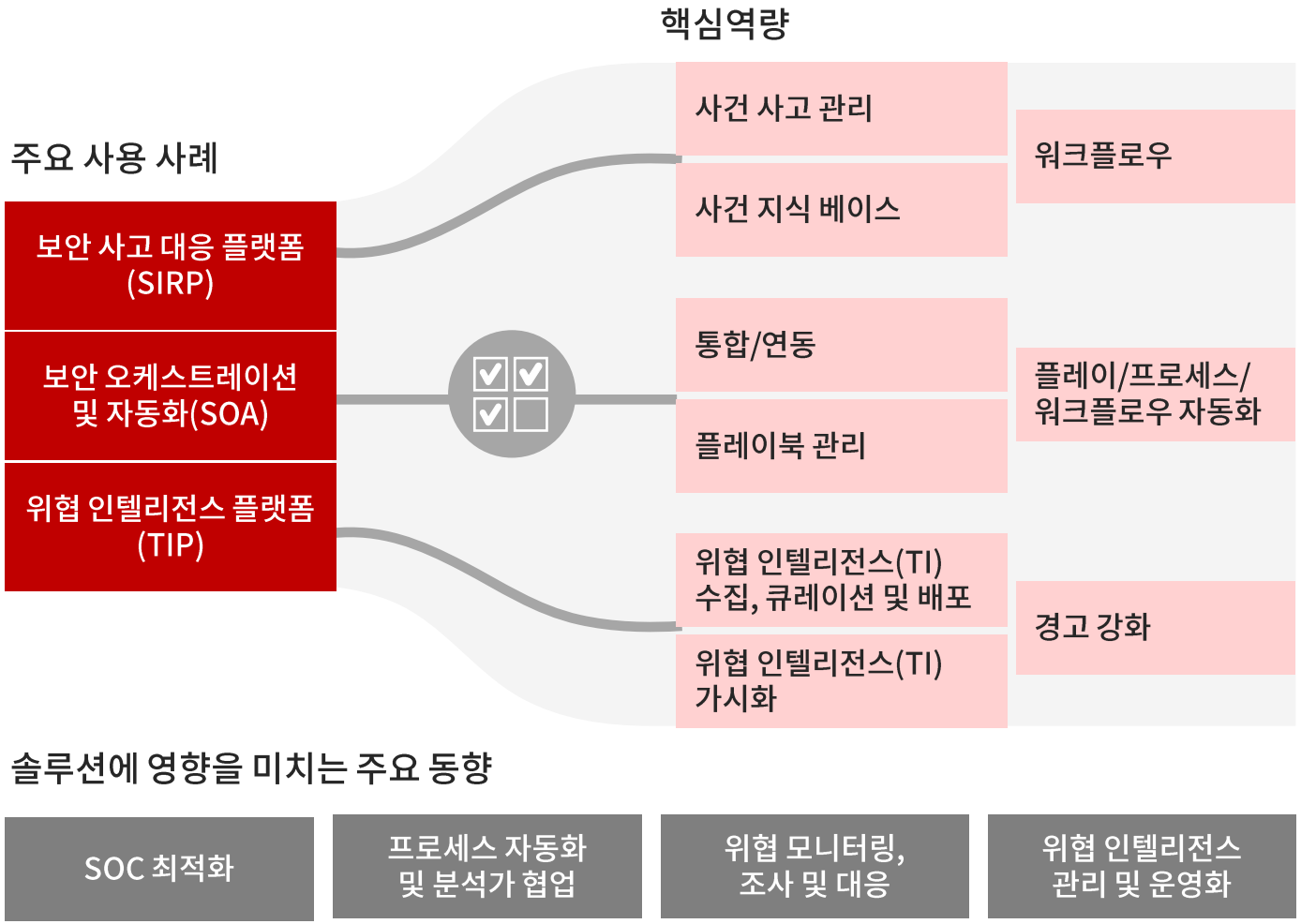
과거: SIEM with Quad Miners = QUADX v1.0

SIEM에서 탐지된 사건들에 대한 **수작업 형태의 추가적인 조사 없이** Sensor(NDR)을 통해 **확보된 원본 증적데이터를 기반**으로 **오탐을 줄이고 즉각적인 대응**연계가 가능한 **Next Generation SIEM** 으로 진화된 솔루션 제공



현재 : SOAR를 이용한 보안운영 자동화 시도

Security Orchestration, Automation and Response Solution



기대효과

- 수동 작업 감소, 가시성 향상.
- 탐지 및 대응 시간 단축.
- 보안 운영 효율성 증가.
- 탐지 및 대응 능력 향상.

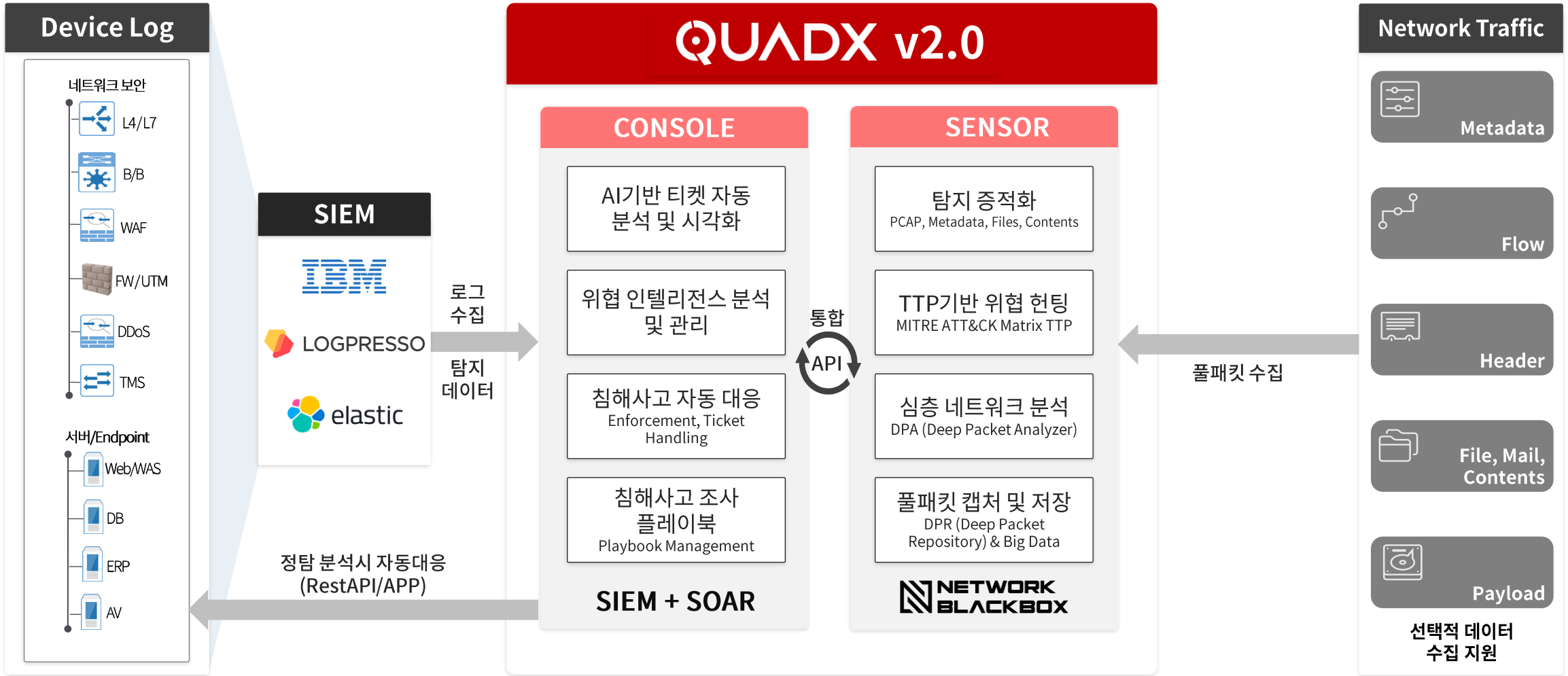
제약사항

- 복잡한 통합 과정.
- 벤더 종속 및 유지 비용.
- 지속적인 튜닝 필요.
- 유지관리를 위한 전문적 스킬 필요

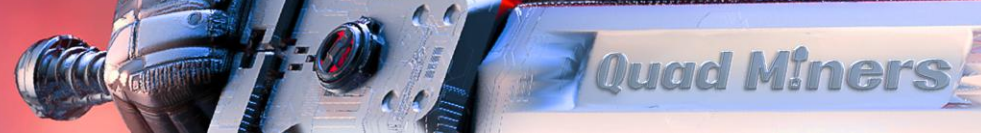
자료참고 : Gartner Market Guide for Security Orchestration, Automation and Response Solutions, June 2023

현재: SIEM+SOAR with Quad Miners : QUADX v2.0

SENSOR(NDR)에서 제공되는 **탐지 증적화 데이터와 다양한 고급분석 데이터를 자동으로 통합**, 기존 SOAR에 의한 보안 운영자동화시 최종적인 위협판정을 위한 분석가 수작업 확인 과정없이 **시스템에 의한 즉각적인 대응 자동화를 지원**하는 **XDR 솔루션** 제공



현재: QUADX v2.0 기대효과



기존 보안장비들을 우회하거나 알려지지 않은 공격과 잠재된 위협에 대한 **AI기반의 탐지-분석-대응 전과정에서의 보안운영자동화 지원**

QUADX V2.0은 담당자분들이 궁금해하는 **Why** 라는 질문에 대한 답을 즉시에 제공합니다.
이를 통해 보안위협 **대응 시간을 50% 이상 줄일 수 있습니다!**

자동화

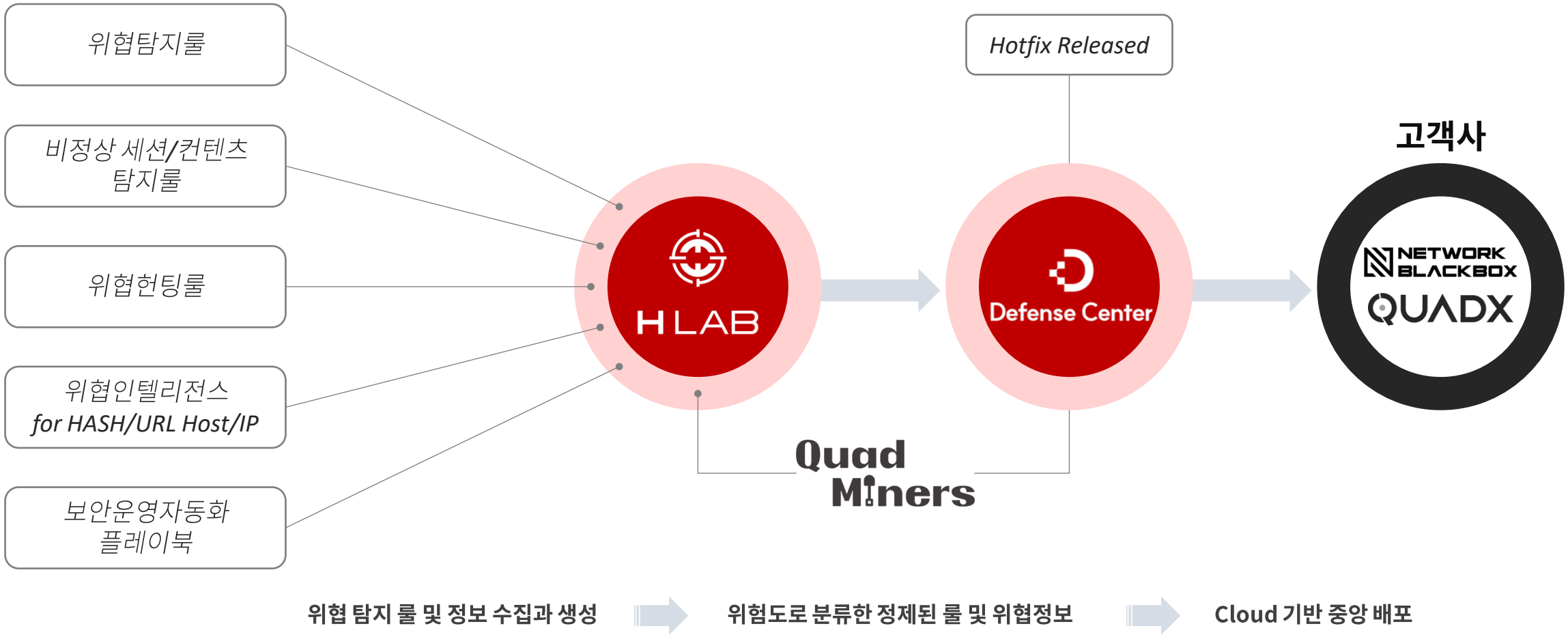
정보수집 및 탐지 → 탐지증적확보 → 상관관계분석 → 인공지능분석 → 위협정보분석 → 타임라인분석 → 침해사고대응

보안운영자동화를 위한 필수 정보

AI기반 행위 및 위협 탐지-분석 정보		공격유효성 및 영향도 증적(대응) 정보	
위협공격 TTPs 관점으로 공격 형태 분류 각 위협별 공격의 위험도 자체분류 탐지 결과 및 종합적 위협 지표 제시	**비정상 행위/컨텐츠** 다양한 네트워크 트래픽 및 컨텐츠 추출 유형으로 부터 비정상 행위 인지 및 비정상 컨텐츠 추출	**세션정보** 세션 및 Bytes 기반 트래픽은 물론 출발지, 목적지, 국가, Port 등 다양한 통계 제공	**컨텐츠 본문** 수집된 풀패킷 데이터 스트림 리빌드로 사용자 화면 복원 및 컨텐츠 추출 제공
자산위험도 네트워크 트래픽을 분석하여 위협이 탐지된 자산 자동 식별 및 분석	**TTPs 기반 위협헌팅** TTPs 관점으로 공격자의 시각에서 잠재적인 위협요소 식별 및 Hunting	**원본파일** 다양한 타입의 파일 원본 추출 DB화 및 분석을 위한 Hash 값 자동산출	**로우레벨 패킷원본** Full-packet(확정적 증적 자료) 수집을 통해 공격의 전반적인 행위를 확인 위협 대응 및 잠재적 리스크 대비

현재: QUADX v2.0 자동화 지원 자원

위협헌팅 전문가들에 의한 **OSINT 기반의 사이버 위협 정보 수집 및 다양한 탐지룰 생성** 후 **자사 SECaaS인 Defense Center** 를 통한 **온/오프라인 업데이트**



가까운 미래 : AI-Enhanced Network Blackbox

Quad Miners 는 **세계최초 AI/XAI 기반의 사이버위협 탐지·대응·예측기술**의 효율적 연구개발을 위해 국내 최고 연구기관과 과제를 수행하고 있으며, 상용화를 위해 고객사들 및 파트너사들과 이미 협력의향서를 체결하여 수요처 사전 확보

AS IS

탐지중심의 한계	기존 NDR은 단순통계(ML) 및 정의된 패턴 탐지 공격행위 탐지·분석 후 대응 **느린 대응 및 미탐된 비정상행위 확인 불가 한계**
탐지·판단 근거 부재	ML을 활용한 분석결과에 대한 근거를 확인하기 어려워 보안 담당자가 탐지된 패킷을 **재확인 수행에 따른 효율성 저하**
신·변종 및 우회 공격 탐지 한계	ML 비지도학습기반 기술의 높은 오탐율의 한계 및 시그니처 기반 방식의 경우 **변조, 우회 시 분석, 탐지 한계**

TO BE

AI기반 탐지 위협 및 비정상 탐지	네트워크 트래픽 전처리 및 효과적인 이상·정상행위 분석을 통한 최신 **AI기술 기반 사이버공격 탐지 기술 개발**
XAI 기술개발을 통한 탐지·판단근거 제시	네트워크 행위기반 AI 탐지모델의 판단 근거 생성 및 신뢰 가능한 XAI 기술개발 및 **핵심특징 추출, 영향도 판정 기술 개발**
신·변종 및 우회 공격 탐지	네트워크 단위공격(Technique), MITRE ATT&CK 공격전술 분석 (TTPs), **강화학습 기반 시퀀스 예측 기술 개발**

공동 연구 기관

KiSTi (www.kisti.re.kr)

- KISTI는 대한민국의 대표적인 과학기술 연구기관으로 61개 국가, 공공 기관에 대한 통합정보보안 서비스 및 연구개발 수행.

BAMBOOS

- Bamboos는 빅 데이터, 데이터베이스 및 에지 컴퓨팅 분야에서 선도적인 기업임.

공공/민간 분야 실증

주관기관

Quad Miners

NDR 원천기술 | 상용화 및 사업화

확정적 사업화

상용수요처 및 파트너사

협력의향서 체결 | 확정적 수요처

선도기술 연구

공동 연구 기관

KAIST

- KAIST는 세계적인 과학기술과 국내 최고의 연구중심대학으로 사이버 공격 시나리오 생성 및 개발에 특화되어 있음.

Gachon University

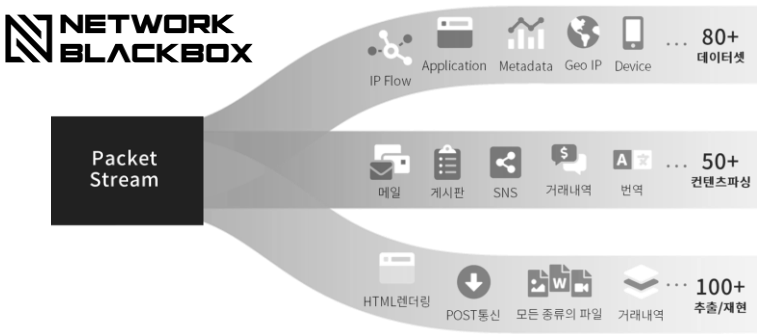
- 가천대학교는 2019년 국내 최초로 AI소프트웨어학과를 신설했고, 실제 네트워크 환경대상 AI 기반 이상징후 연구개발 수행함.

가까운 미래 : AI-Enhanced QUADX v3.0

SENSOR 역할의 **Network Blackbox 에서 수집된 빅데이터**를 기반으로 **LLM과 RAG 기술을 이용한 AI Assistant** 를 통해 보안운영상에서 발생될 수 있는 **다양한 분석 및 조사과정 자동화**

QUADX v3.0

SENSOR



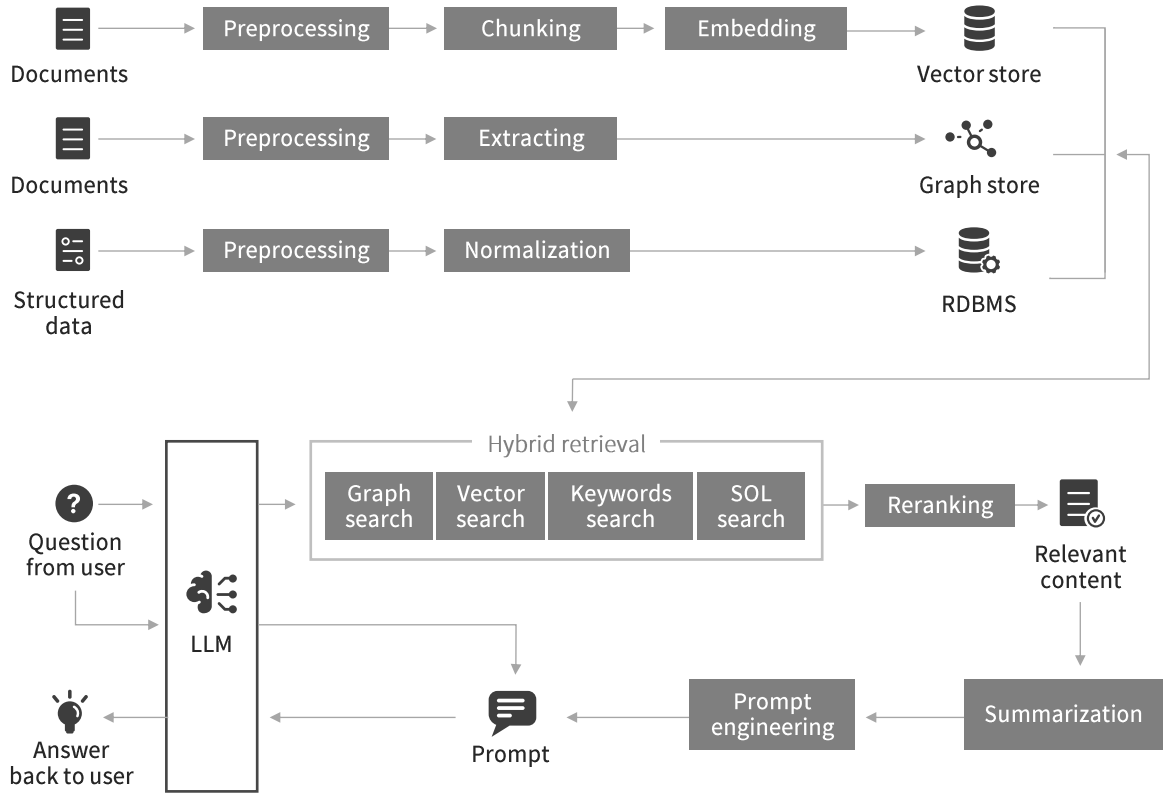
AI Assistant

데이터

질의

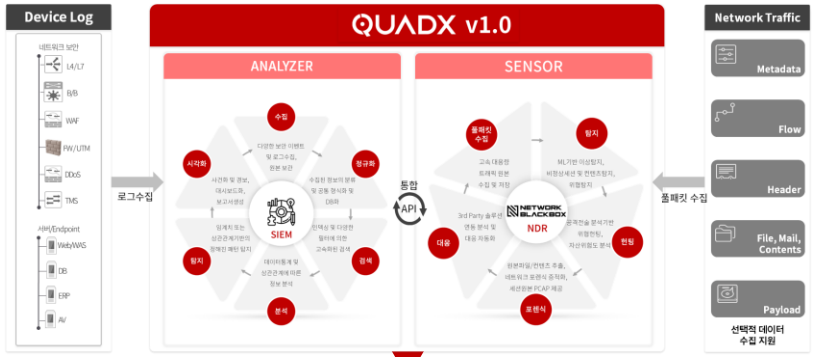
응답

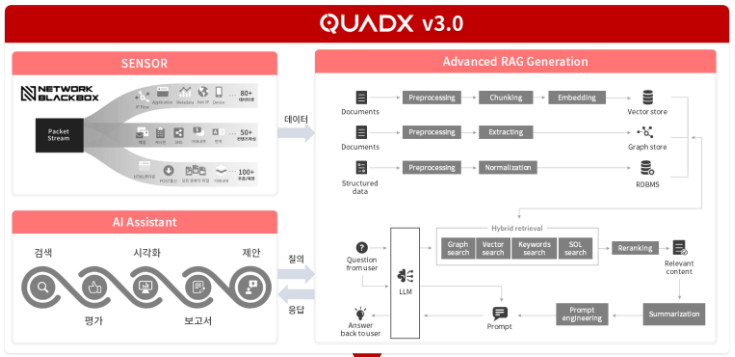
Advanced RAG Generation



보안운영자동화를 위한 여정... 그리고 비전

NDR 원천기술을 토대로 Network Blackbox 가 제공하는 빅데이터 및 원본데이터를 기반으로 **AISecOps 구현**

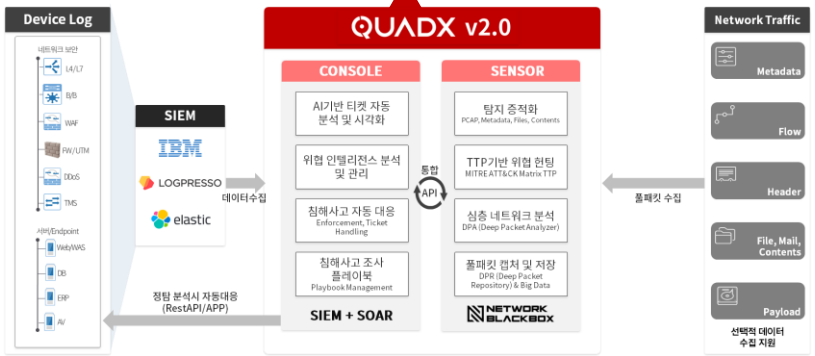




XDR
현재

과거
NGSIEM

가까운 미래
AISecOps



Quad Miners Overview

Quad Miners

회사명	쿼드마이너
설립일	2017년 11월 24일
대표자	박범중, 홍재완
대표솔루션	Cyber Defense Blackbox
웹사이트	www.quadminers.com

81
임직원
R&D 인력 (70%)

90
고객사
대기업, 글로벌기업,
공공기업, 제1금융사 등

42
파트너사
국내 29개 업체,
글로벌 13개 업체

28
특허출원
국내외 특허 등록
11건

한국법인 서울본사
서울특별시 강남구 테헤란로 138, 성홍타워 6층 (06236)

일본법인 도쿄본사
東京都千代 田区霞が関3 - 2 - 5　霞が関ビル5階 (〒100–6090)

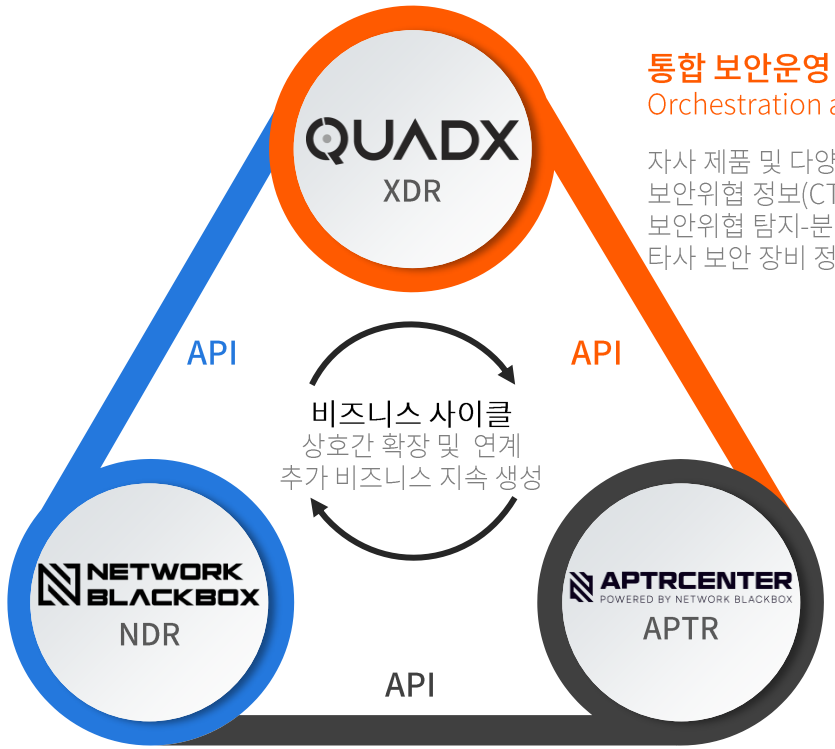
일본법인 나고야지사
名古屋市中村区那古野1−47−1 名古屋国際センタービル18階 (〒450–0001)

싱가폴법인
9 Straits View, Marina One West Tower #05-07, Singapore (018937)

- **Gartner Report** 가트너 리포트에 4년 연속 등재 • **T- 2** 기술신용평가기관 최상위 기술기업

Quad Miners 비즈니스 모델 및 포트폴리오

API 를 이용 자사 제품간 또는 타사 제품과의 기능 통합 및 확장을 통한 보안운영 자동화 지향

사업영역	사업 포트폴리오	사업형태
클라우드 솔루션	Cloud Blackbox 클라우드 보안위협 가시화 및 분석 Cloud Visibility and Analytics Packet Insight Cloud POWERED BY NETWORK BLACKBOX 온디멘드 네트워크 포렌식(SECaaS) OnDemand Network Forensic	구독형
온프레미스 솔루션	 **통합 보안운영 자동화** Orchestration and Automation 자사 제품 및 다양한 IT 제품 로그 및 이벤트 수집 보안위협 정보(CTI) 관리 체계 자동화 보안위협 탐지-분석-대응 자동화 타사 보안 장비 정책 및 설정 자동화 및 오케스트레이션 **네트워크 보안위협 가시화 및 분석** Network Visibility and Analytics 풀패킷 캡처기반의 트래픽 전수검사 이상,비정상행위, 위협 탐지 잠재된 보안 위협헌팅 네트워크기반 포렌식 및 위협대응 연계 **파일관련 통합 위협관리** APT Response API 및 다양한 방식의 파일 수집 수집된 파일에 대한 자체 TI기반 위협식별 파일 원본들에 대한 다중 APT 솔루션 병렬 분산검사 랜섬웨어등 식별된 악성파일 자동 보고 및 대응 조치	판매형
서비스	H LAB • 탐지룰 최적화 서비스 • 위협헌팅 서비스 • 침해사고 대응 서비스 Defense Center • 위협탐지룰 정제 및 업데이트 • 비정상세션/컨텐츠 탐지룰 업데이트 • OSINT 수집/정제 및 업데이트 • 라이선스 및 제품 업데이트 PROFESSIONAL SERVICES • NBB/CBB 설치 및 지원 서비스 • QUADX 설계, 설치 및 지원 서비스 • SIEM 설계, 설치 및 지원 서비스 • SOAR 설계, 설치 및 지원 서비스	구독형 /판매형

HUNT OR GET HUNTED

Revolutionizing cyber warfare with **Network Blackbox**

Quad Miners