Quad Miners

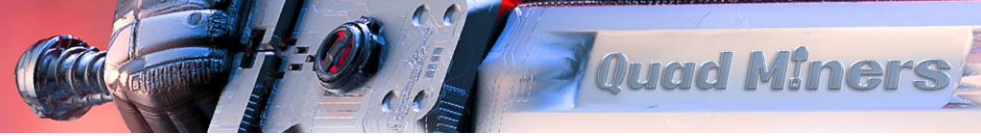
HUNT OR GET HUNTED

NDR을 활용한 네트워크 데이터 수집 및 AI

홍재완

Oct, 2024

목차

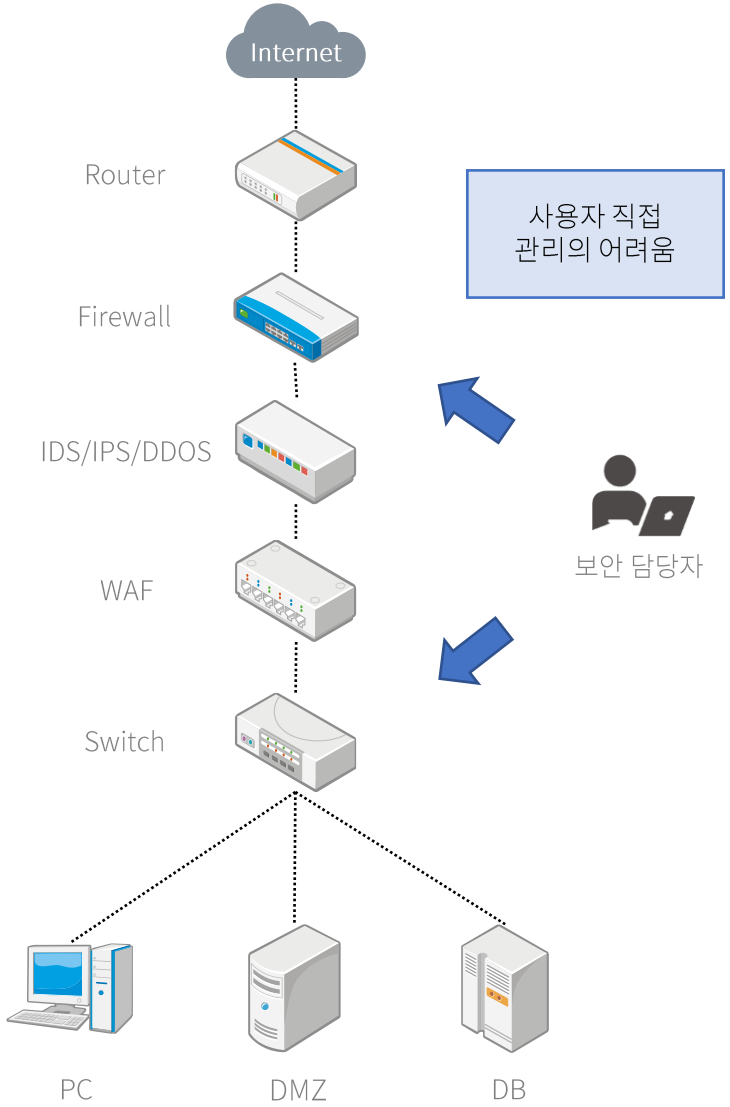


Key Highlight

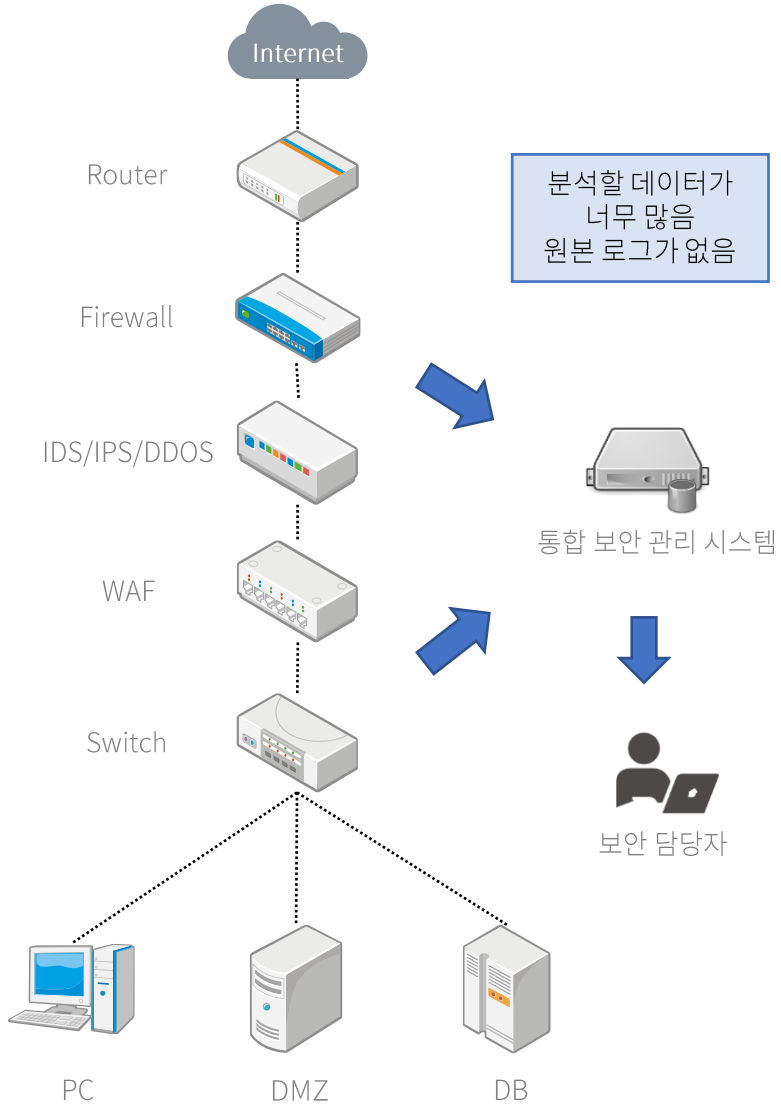
- Network Detection and Response
- Gartner, AI

NDR의 개발 기획

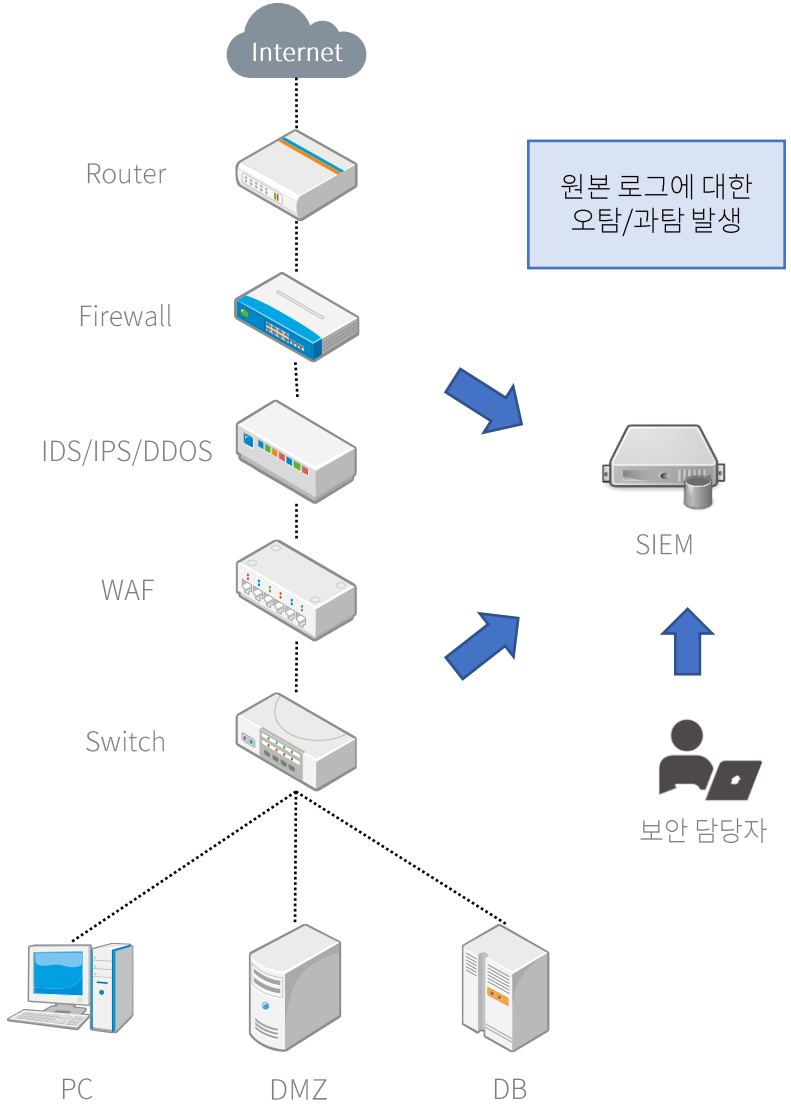
1. 직접 접근 분석 방식



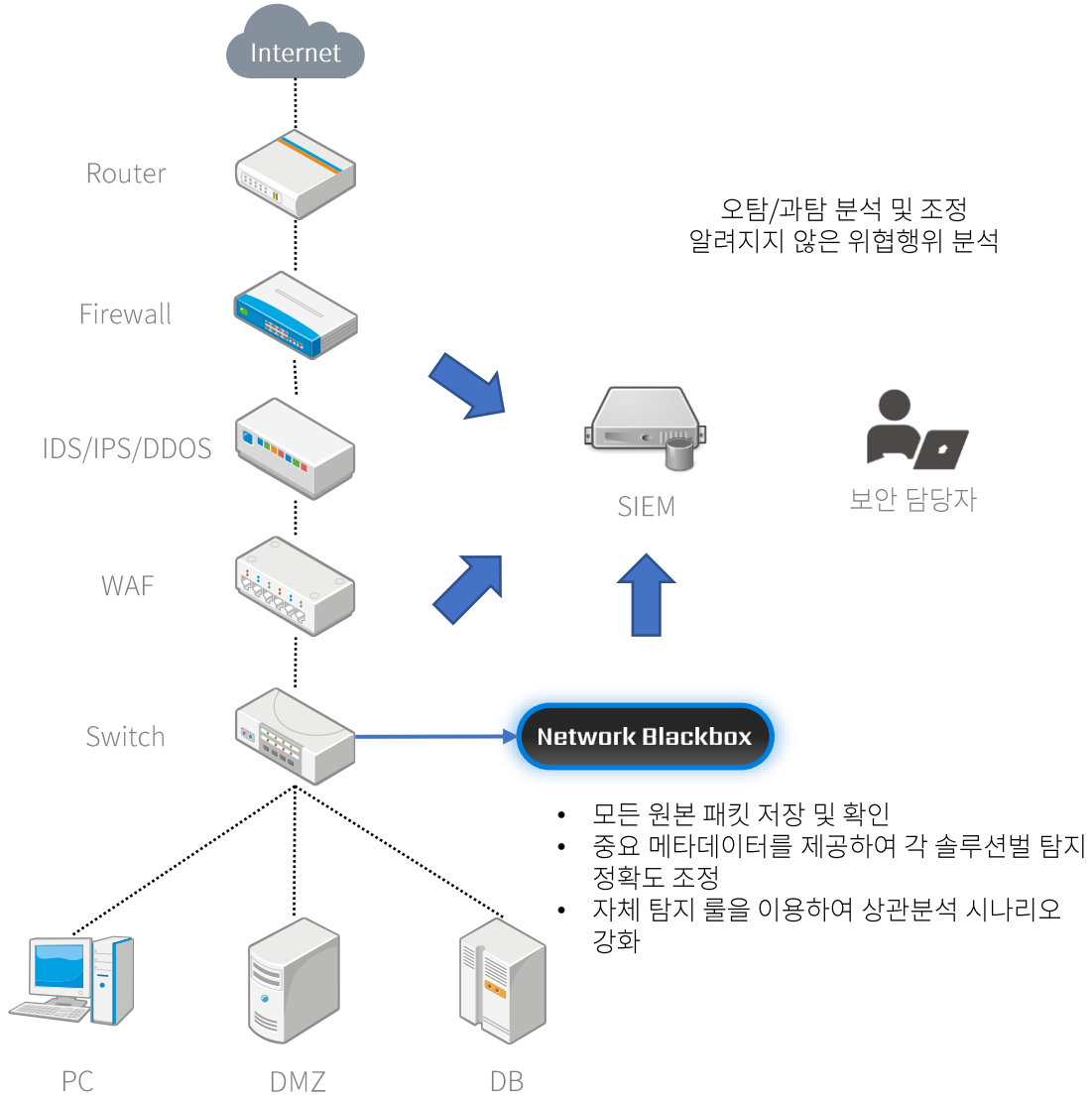
2. 로그 수집 분석 방식



3. 시나리오 분석 방식

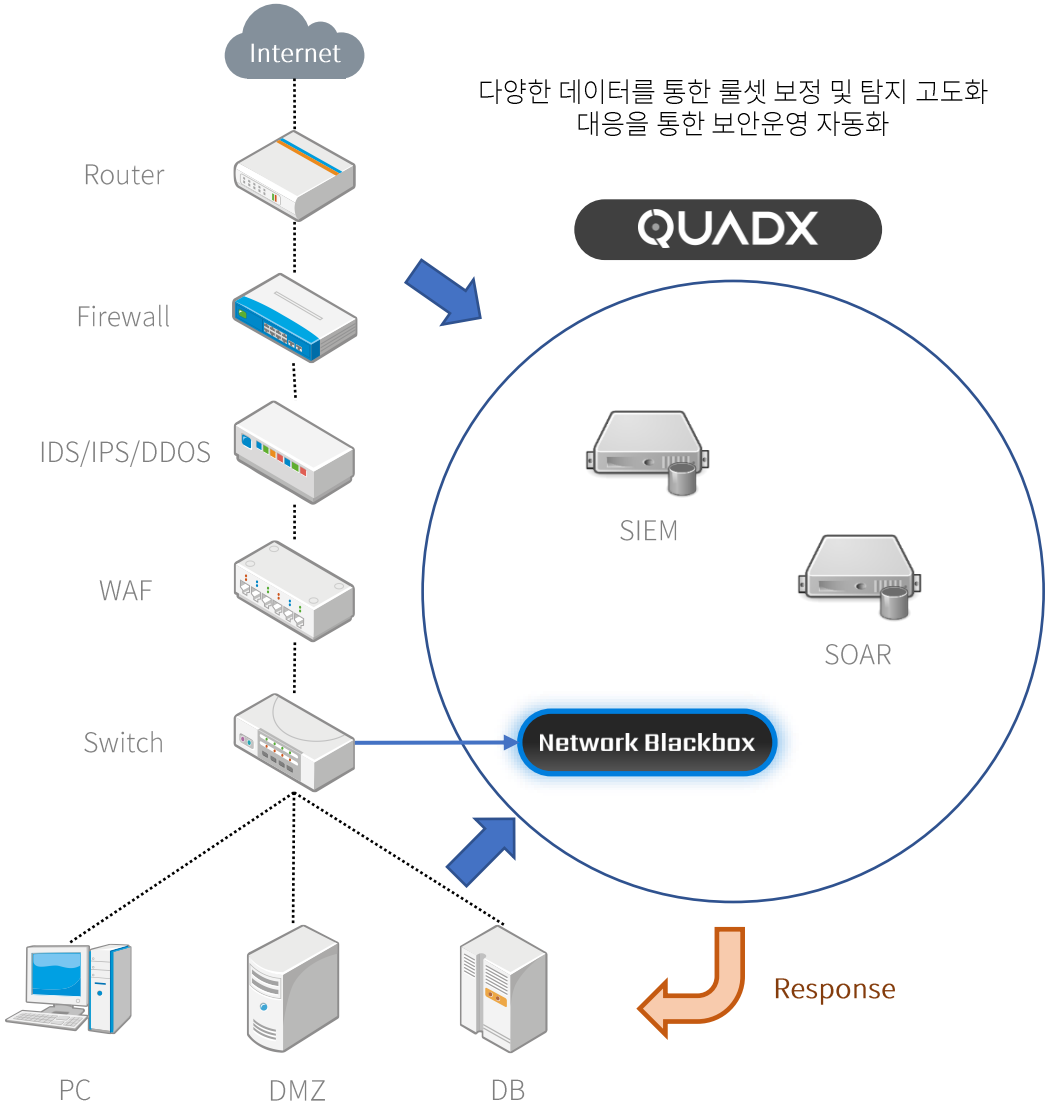


NDR의 개발 기획



오탐/과탐 분석 및 조정
알려지지 않은 위협행위 분석

- 모든 원본 패킷 저장 및 확인
- 중요 메타데이터를 제공하여 각 솔루션별 탐지 정확도 조정
- 자체 탐지 룰을 이용하여 상관분석 시나리오 강화



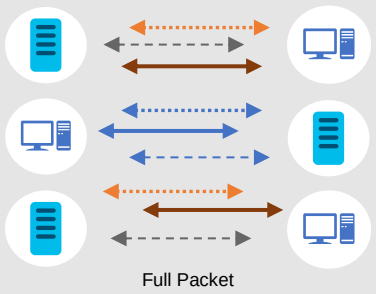
다양한 데이터를 통한 룰셋 보정 및 탐지 고도화
대응을 통한 보안운영 자동화

NDR의 요구 사항

NDR 필수기능 요건

Segment	Observations	AI Modeling	AI Anomalies	Detection	Hunting	Forensics	Respond	Other Cases
NDR	Network	Yes	YES	YES	YES	Yes	Yes	No
IPS	Network	No	No	Yes	No	Some	YES	No
NPMD	Network	No	Some	No	Yes	Some	No	Yes
SIEM	Logs and alerts	No	Some	Some	YES	No	Some	Yes
EDR	Endpoint	YES	Some	YES	YES	Some	Yes	Yes

풀패킷 데이터 수집 및 분석



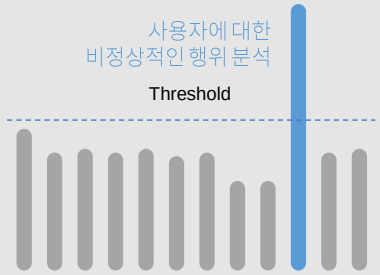
정상적인 동작에 대한 기준치 생성

~100 Security Events

Number of concurrent flows
Packet per second
Bits per second
New flows created
Number of SYNs sent
Time of day
Number of SYNs received
Rate of connection resets
Duration of the flow

고객 환경에 맞는 기준 생성과
지도학습기반으로 학습 정확도 향상

이상징후 및 행위 변경 시 경보



Gartner

Emerging Technologies: Adoption Growth Insights for Network Detection and Response

Published 29 March 2022 - ID G00760392 - 16 min read

By Analyst(s): Nat Smith, Christian Canales

Initiatives: Emerging Technologies and Trends Impact on Products and Services

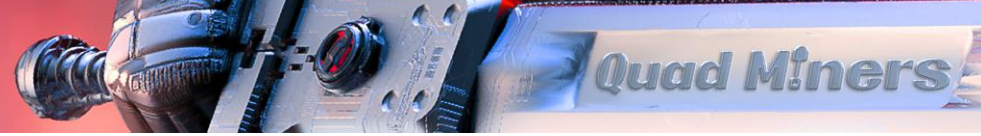
> The network detection and response market continues to grow quickly, and trends within the market are stabilizing. To maximize revenue, product leaders should focus on technical buyers and adjust roadmaps and go-to-market efforts to cover remote workers, SaaS applications and midsize organizations.

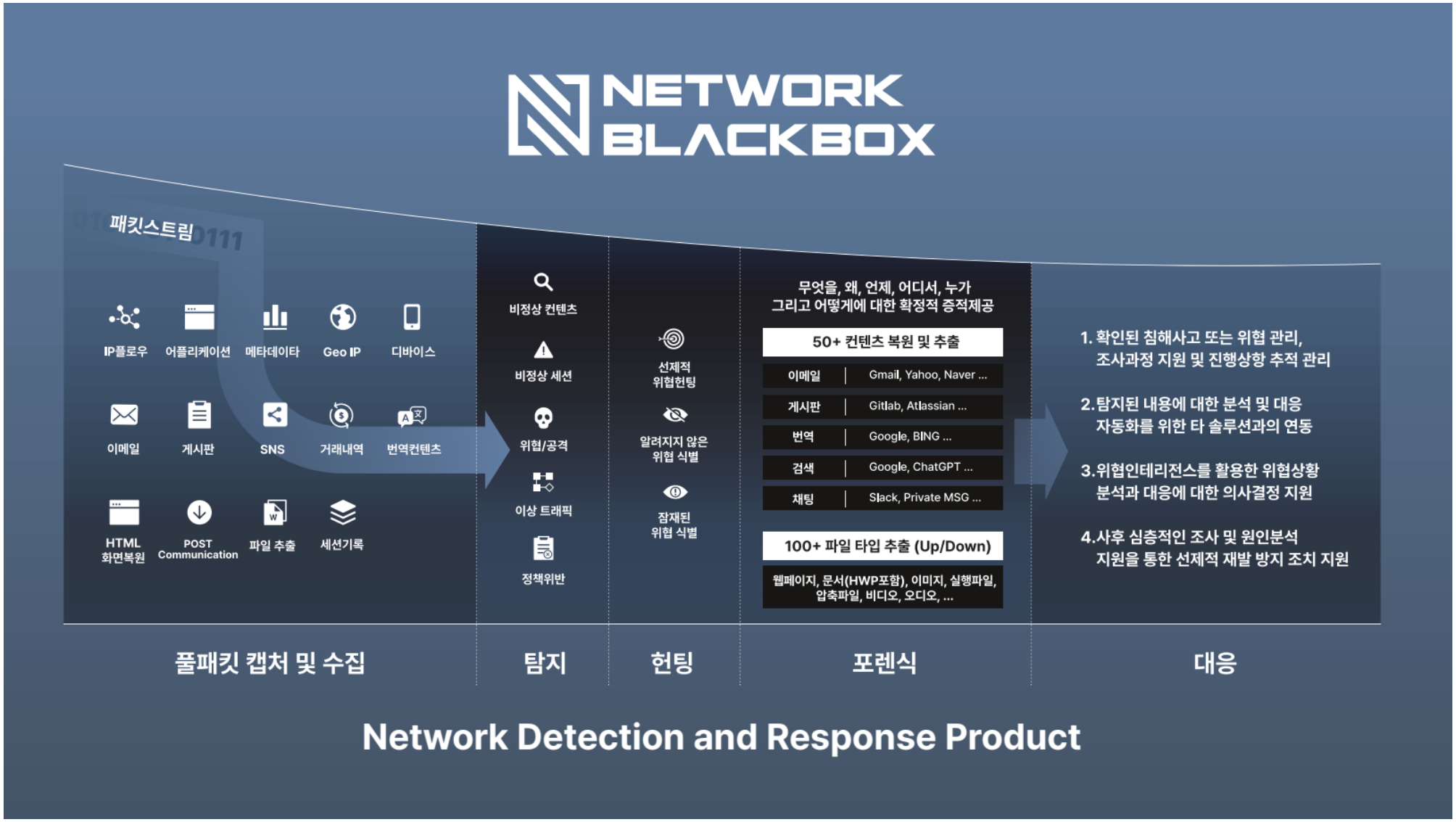
Overview

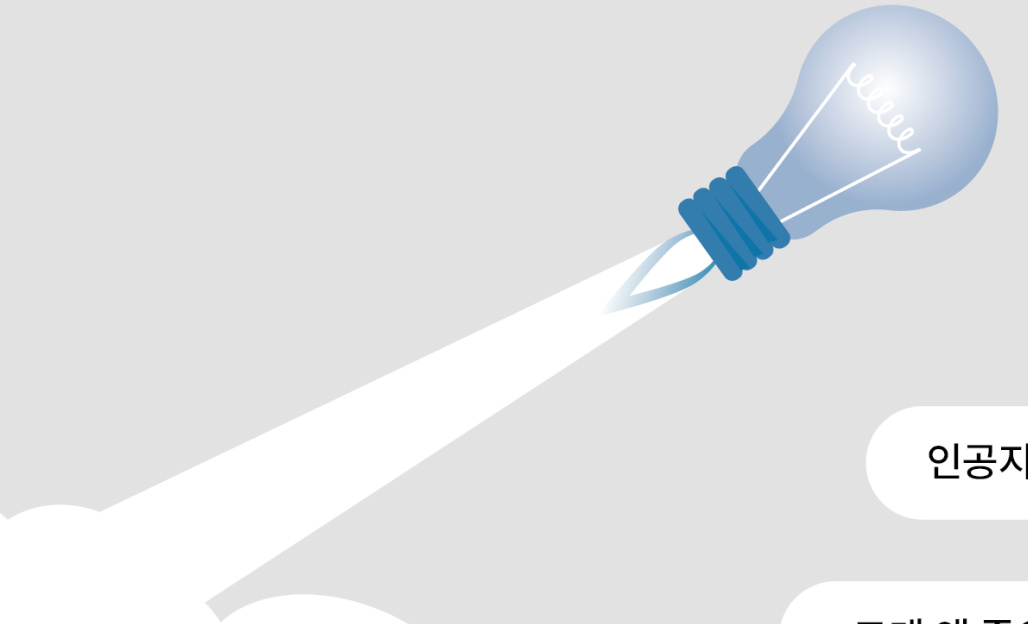
Key Findings

- MixMode (Network Traffic Analytics)
- Plixer (Plixer Scrutinizer)
- Quad Miners (Network Blackbox)
- Tencent (T-Sec NTA)
- Vectra (Cognito)
- Vehere (PacketWorker)
- VMware (Lastline Defender)

NDR의 요구 사항







새로운 기술 등장 시
우리의 흔한 반응

인공지능이 뭐예요?

우린 어떻게 해야 해요?

빅데이터는?

그게 왜 중요해요?

다들 어떻게 하고 있어요?

블록체인이 뭐예요?

사물인터넷이 뭐예요?

메타버스가 뭐예요?

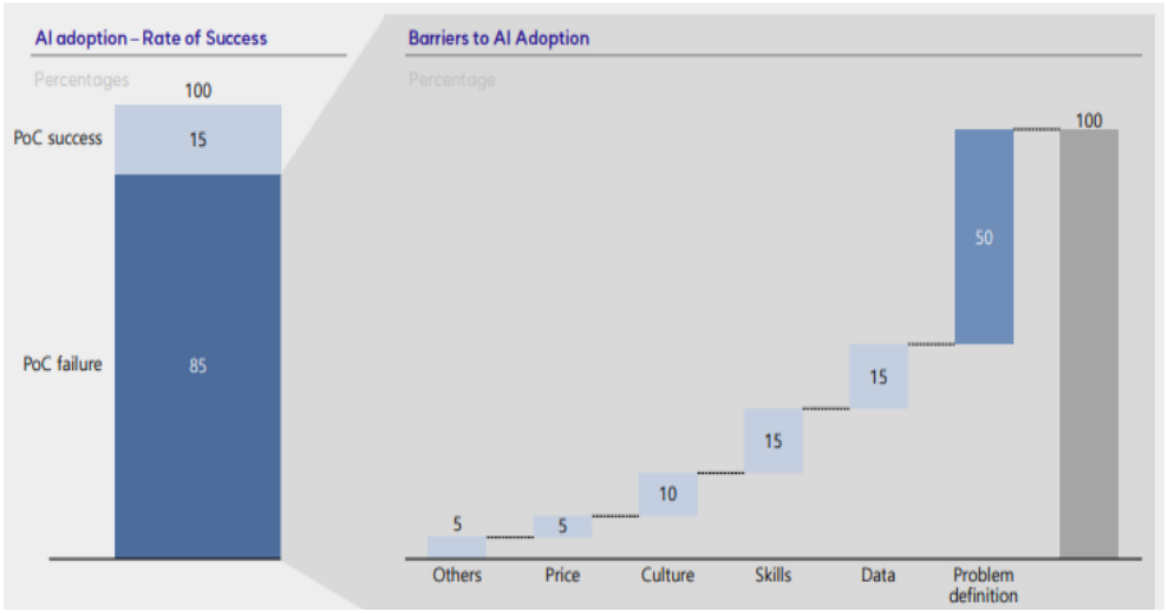
매년 수많은 디지털 AI 서비스가 야심차게 기획되어 추진되지만 지속 운영되는 서비스는 한정적이다.

고객들은 기술에 관심이 없다.
관심사는 오로지 문제해결 뿐

"고객 니즈에 대한 무지는 **쓸고퀄*** 서비스를 낳는다."

*'쓸데없이 고(高) 퀄리티'의 준말. 말 그대로 불필요한 상황이나 아무것도 아닌 상황에서 상당한 노력을 기울이거나 능력을 발휘하여 높은 퀄리티의 결과물을 내놓았을 때 쓰인다.

잘못된 문제정의



머니투데이
https://news.mt.co.kr › mtview

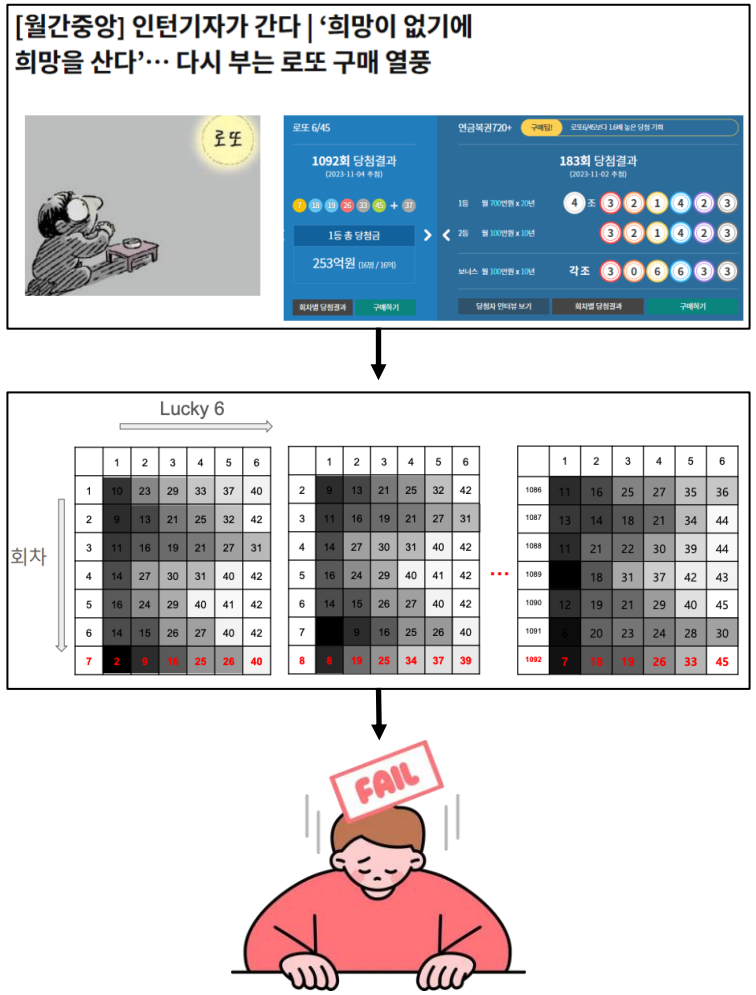
"수십억 대박" 황금빛 유혹 로또 예상업체, 믿을 수 있을까?

2015. 6. 12. — ... 로또 번호 예측 방법에 대해 "학술적 근거가 없다"고 말했다. 박유성 고려대 통계학과
"지금까지 나온 로또 번호를 조합하고 분석해서 장차 ...

통계학 전문가들은 이들 업체들이 주장하는 로또 번호 예측 방법에 대해 "학술적 근거가 없다"고 말했다. 박유성 고려대 통계학과 교수는 "지금까지 나온 로또 번호를 조합하고 분석해서 장차 나올 번호를 예측한다고 하는데 이는 확률의 기본을 무시한 발언"이라며 "모든 로또 조합은 독립변수이기 때문에 매번 확률이 '리셋'된다"고 말했다.

홍종선 성균관대 통계학과 교수는 "이들 업체 회원 가운데 1등 당첨이 된 사람이 많다고 하는 것은 사람들이 많이 찾는 복권 판매소에서 1등이 많이 배출됐다고 하는 것과 마찬가지"라며 "회원이 많고 표본집단이 커져 1등이 많이 나오는 것이지 당첨 확률 자체가 높아지는 것은 아니다"라고 말했다.

CNN Regression을 이용한 LOTTO 번호 예측



RNN을 이용한 사이트에서 각 사용자별 발생한 트래픽을 기반으로 학습을 통한 비정상 세션 탐지

네트워크 패킷 캡쳐 및 데이터 수집

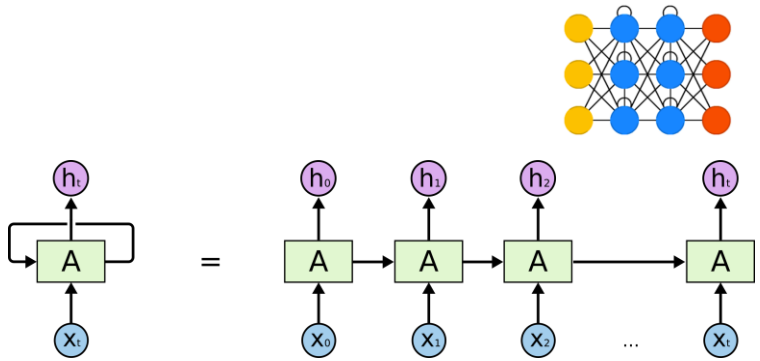
NETWORK TRAFFIC

내부 사용자

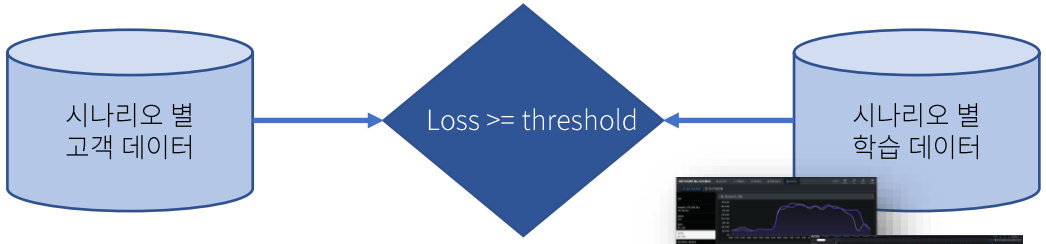
시나리오 별 데이터 전처리

- 전체 네트워크 행위 분석
- 어플리케이션 별 행위 분석
- 첨부파일 별 행위 분석
- 이메일/SNS 별 행위 분석

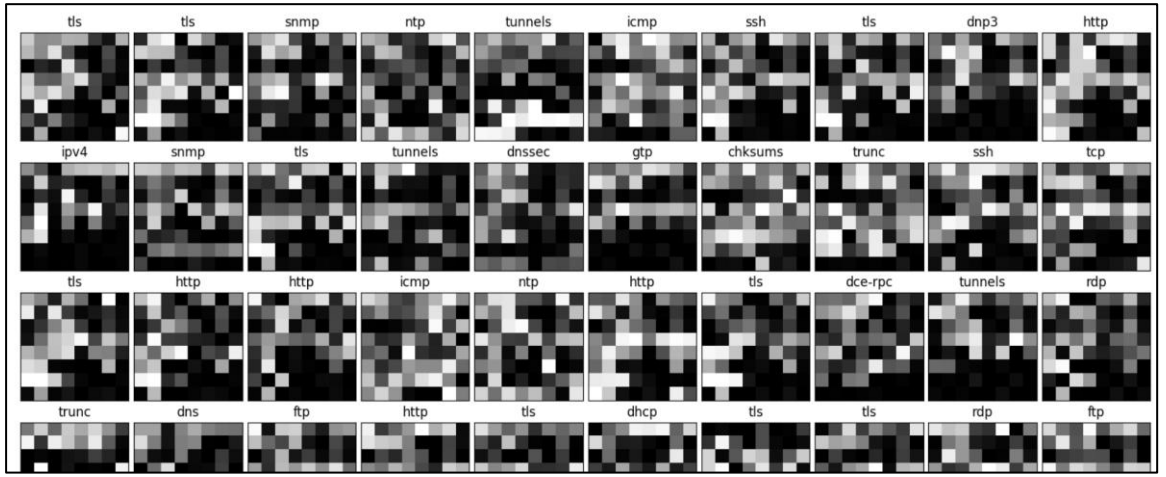
RNN

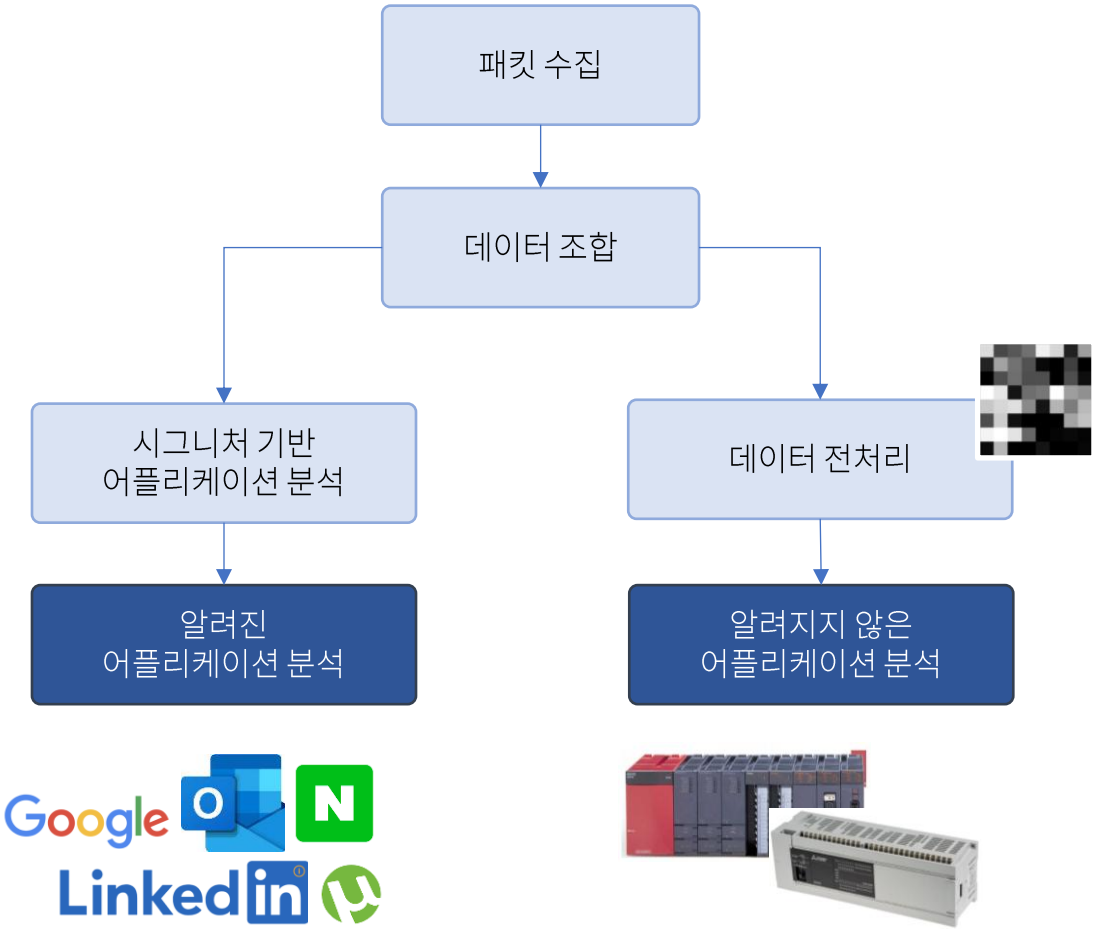


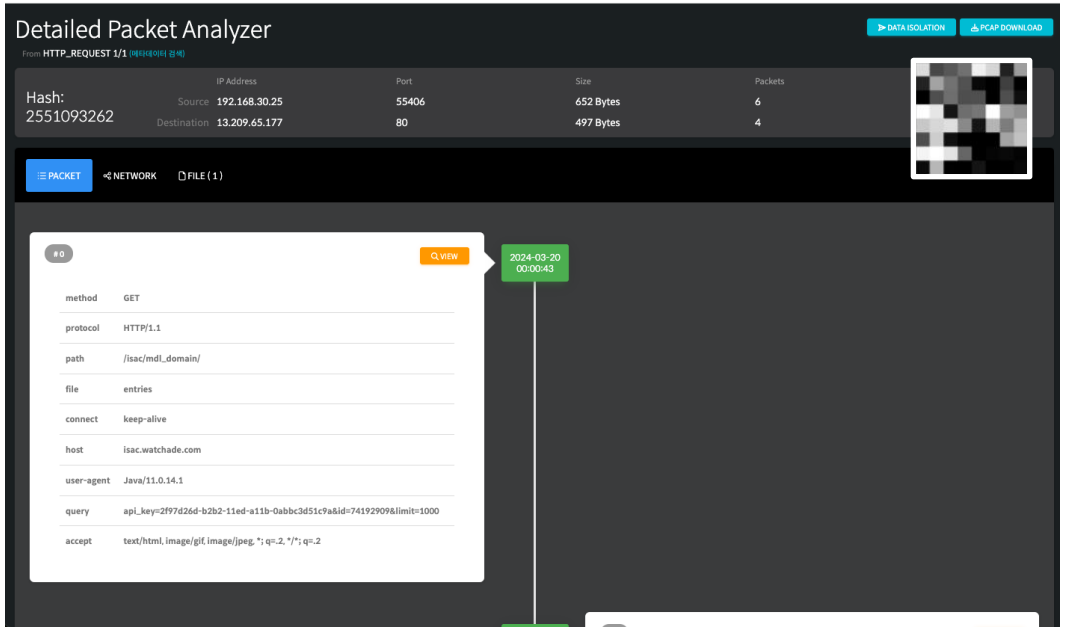
Detect



딥러닝을 이용한 효과적인 DPI(Deep Packet Inspection) 분석 방법



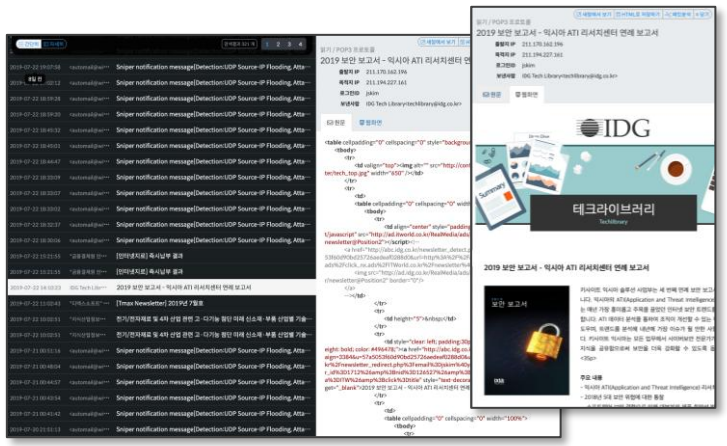




LLM을 통한 정보의 축약

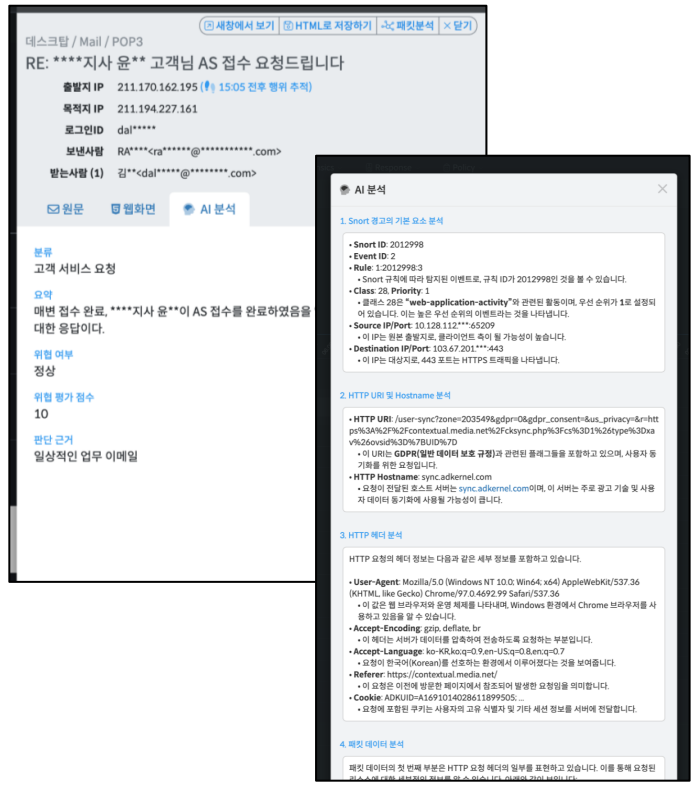
TEXT → LLM → TEXT

Network Blackbox

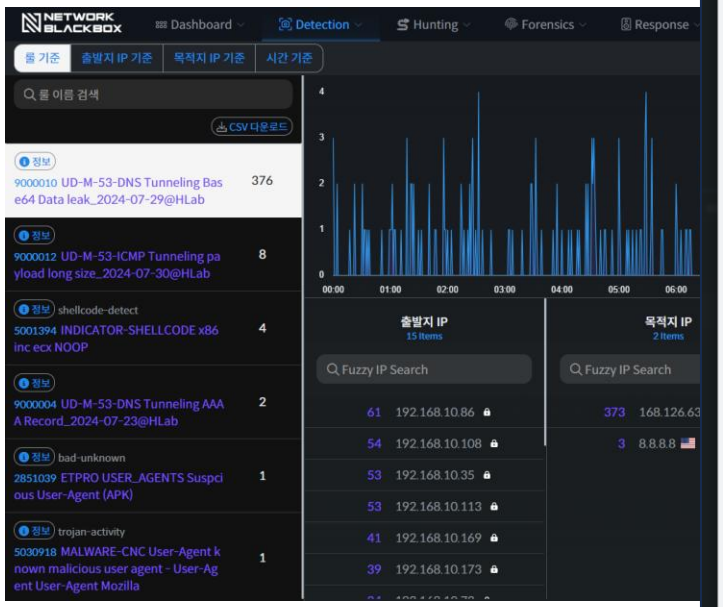


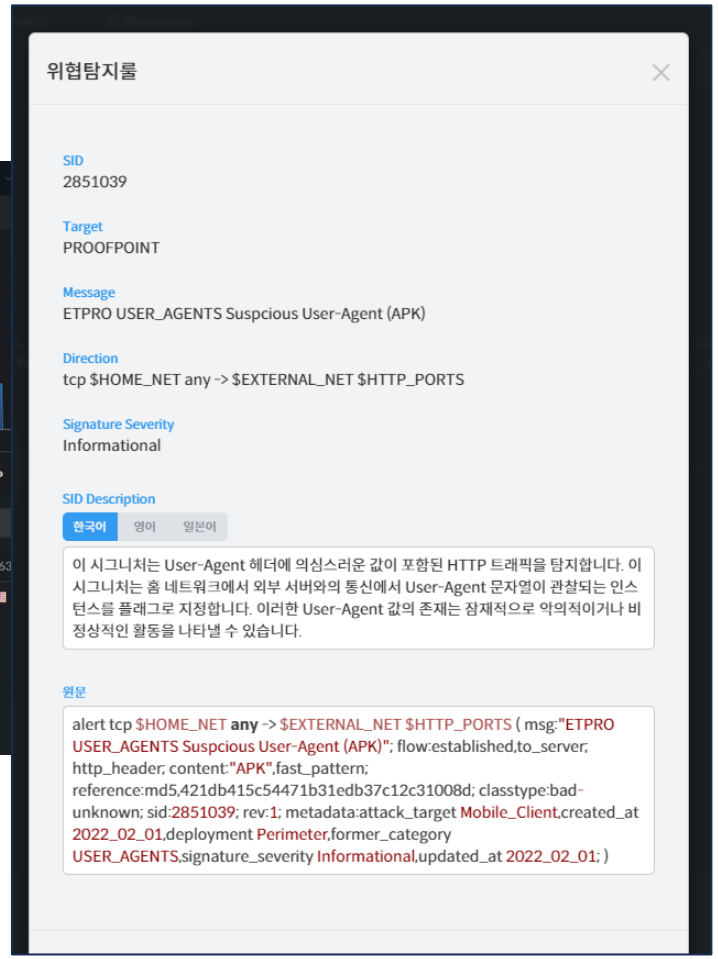
Local → Google BERT

API → OpenAI

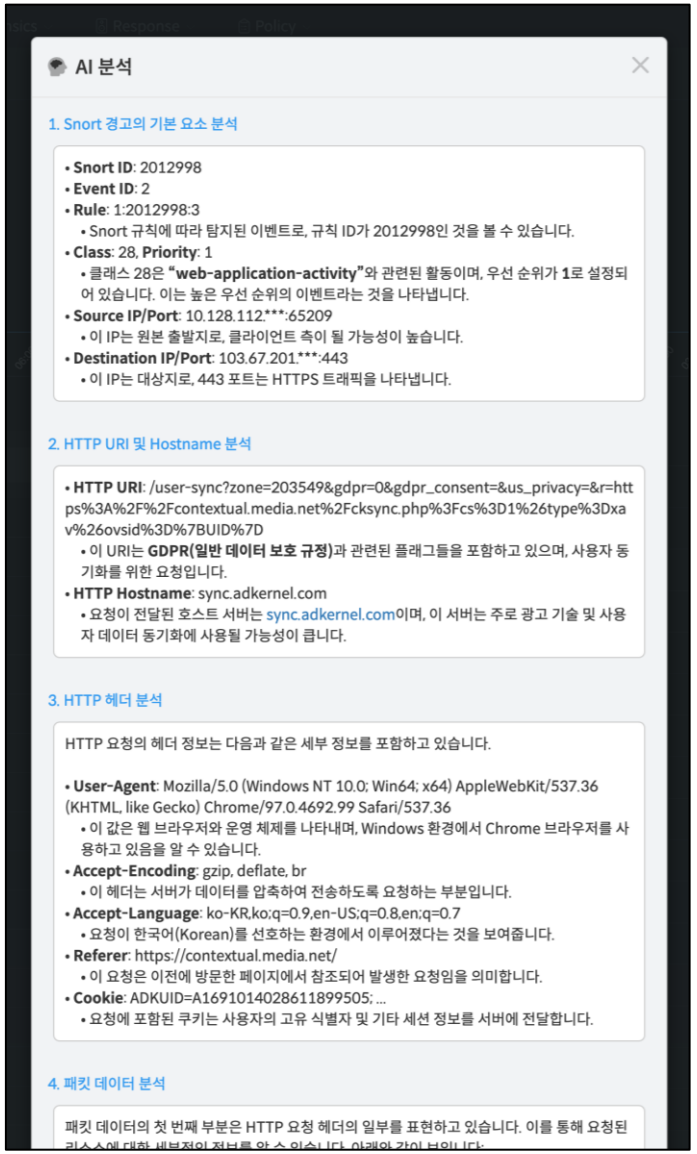


LLM을 이용한 탐지로그 분석 및 패킷 분석
패킷에 대한 이해도가 낮은 담당자도 쉽게 분석할 수 있도록 정보제공





LLM

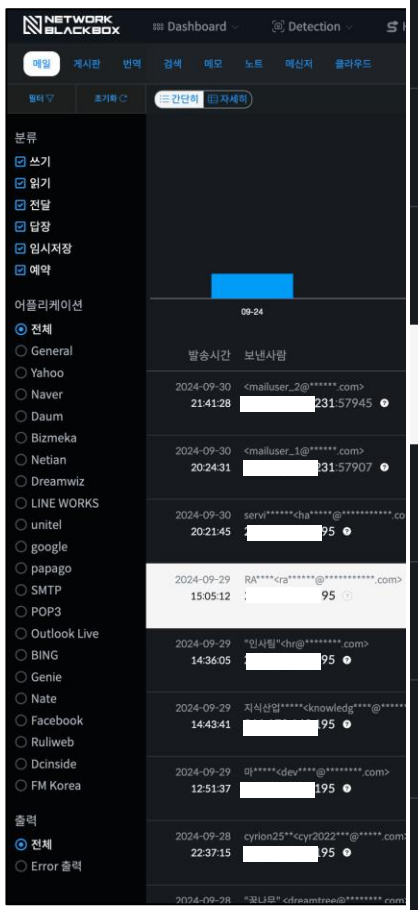


NDR & AI

LLM을 이용하여 이메일, 블로그, 첨부파일, 번역기 등 다양한 텍스트 기반의 데이터들을 요약, 분류하여 보안 담당자가 알아야 할 내용들을 정리

공통 카테고리	주문 및 물류 관리
	재무/회계 관리
	고객 서비스 지원
	프로모션 및 마케팅
	….
이커머스 (Model C)	공통 카테고리 조정
	카테고리 추가
국방 (Model M)	공통 카테고리 조정
	카테고리 추가
금융 (Model F)	공통 카테고리 조정
	카테고리 추가

LLM



분류 / 제목

재무 및 회계 - 평가지수: 10
Desktop - 메일 - SMTP - SMTP - SMTP 메일 파싱
[**카드] 20**년 **월 **일 이메일 명세서 입니다

마케팅 및 홍보 - 평가지수: 10
Desktop - 메일 - SMTP - SMTP - SMTP 메일 파싱
(광고) [***몰] 배송 안내

고객 서비스 요청 - 평가지수: 10
데스크탑 - Mail - POP3 - POP3 - Unknown
[****] 최**님 주문하신 내역을 확인해주세요.

고객 서비스 요청 - 평가지수: 10
데스크탑 - Mail - POP3 - POP3 - Unknown
RE: ****지사 윤** 고객님 AS 접수 요청드립니다

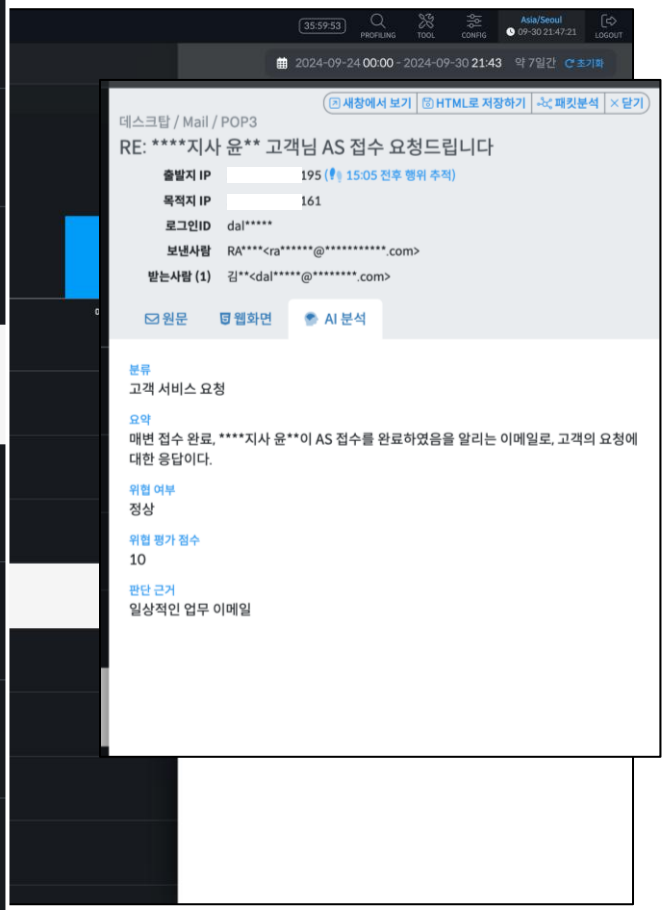
데이터 유출 - 평가지수: 90
데스크탑 - Mail - POP3 - POP3 - Unknown
*** 이력서

비업무활동 - 평가지수: 10
데스크탑 - Mail - POP3 - POP3 - Unknown
인공지능 기반 첨단 4차 산업 혁명 기업 리포트

재무 및 회계 - 평가지수: 10
데스크탑 - Mail - POP3 - POP3 - Unknown
20**년 *월 ** email 명세서입니다.(010-34**-****)

내부 업무 보고 및 정보 공유 - 평가지수: 10
데스크탑 - Mail - POP3 - POP3 - Unknown
*** 귀속 연말정산 안내문 보내드립니다.

내부 업무 보고 및 정보 공유 - 평가지수: 10



Quad Miners ISEC 2024 부스 운영 및 강연 안내

주요 제품 Portfolio

Quad Miners

첨단산업을 지키는 사이버보안,
방산기술보안 및 AI 보안분야 전문기업

NETWORK BLACKBOX

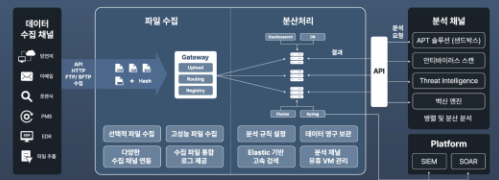
Network Detection and Response Product

QUADX v2.0

eXtended Detection and Response Product

APTRCENTER
POWERED BY NETWORK BLACKBOX

파일 통합 검역소, 파일데이터 흐름 가시화, 파일형 APT 공격 통합 분석/ 대응 체계 기능 제공



APT 공격 대응 기대효과

Visibility | Analytics | Orchestration | Automation

부스 위치 (P05)

Day 2 10/17(목)
13:00 ~ 13:40 @Track C
홍재완 대표이사 | Quad Miners CDO

Day 1 10/16(수)
11:30 ~ 12:00 @오디토리움
김용호 전무 | Quad Miners CTO

발표 Session

Quad Miners Keynote Session

보안운영 자동화의 과거, 현재 그리고 가까운 미래

김용호 전무 | Quad Miners CTO

Day 1 10/16(수) 11:30 ~ 12:00 @오디토리움

Quad Miners Breakout Session

NDR을 활용한 네트워크 데이터 수집 및 AI

홍재완 대표이사 | Quad Miners CDO

Day 2 10/17(목) 13:00 ~ 13:40 @Track C

HUNT OR GET HUNTED

Revolutionizing cyber warfare with **Network Blackbox**

Quad Miners