

Quad Miners

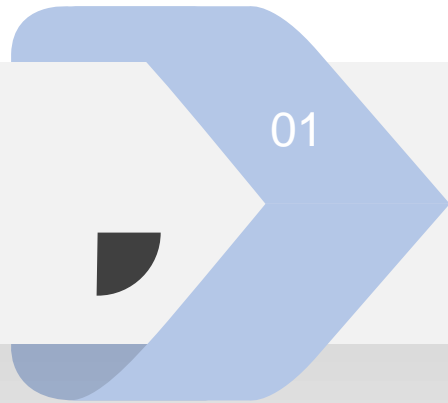
HUNT OR GET HUNTED

NDR을 활용한 네트워크 데이터 수집 및 AI

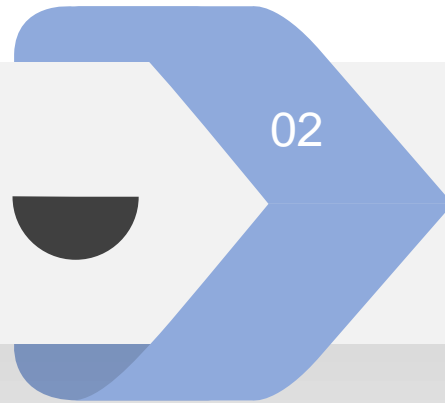
홍재완

Oct, 2024

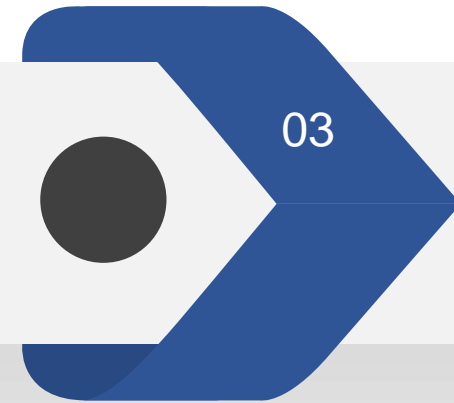




NDR 개발 기획



NDR의 요구사항



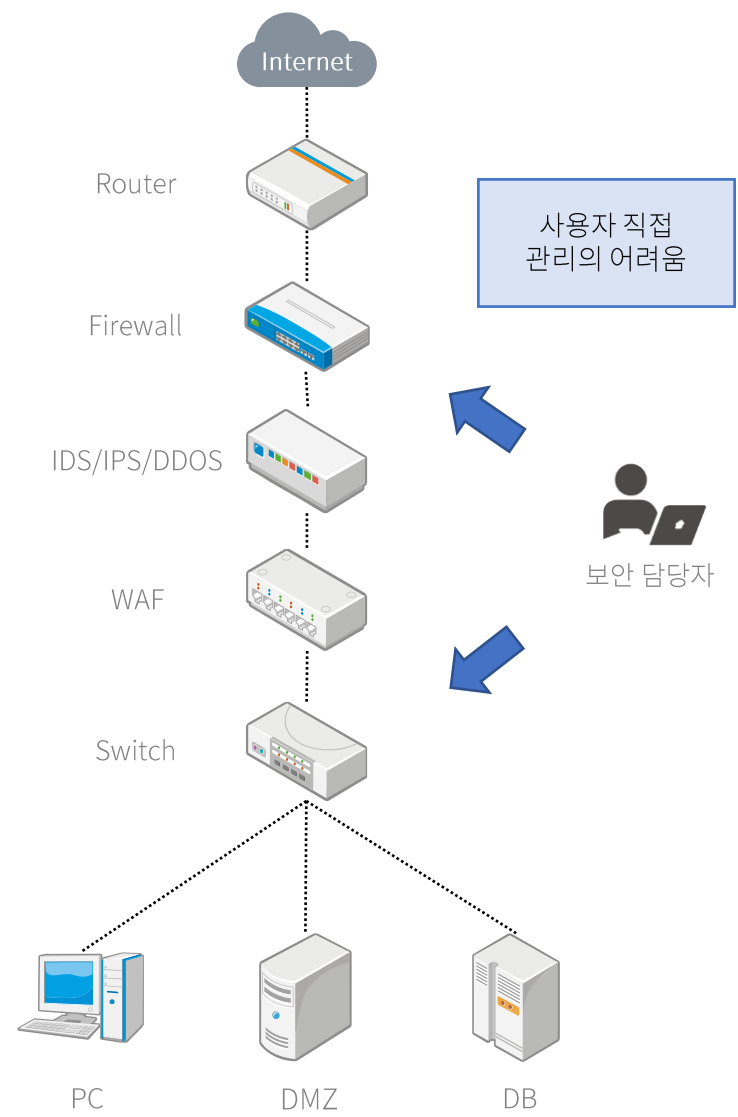
NDR & AI

Key Highlight

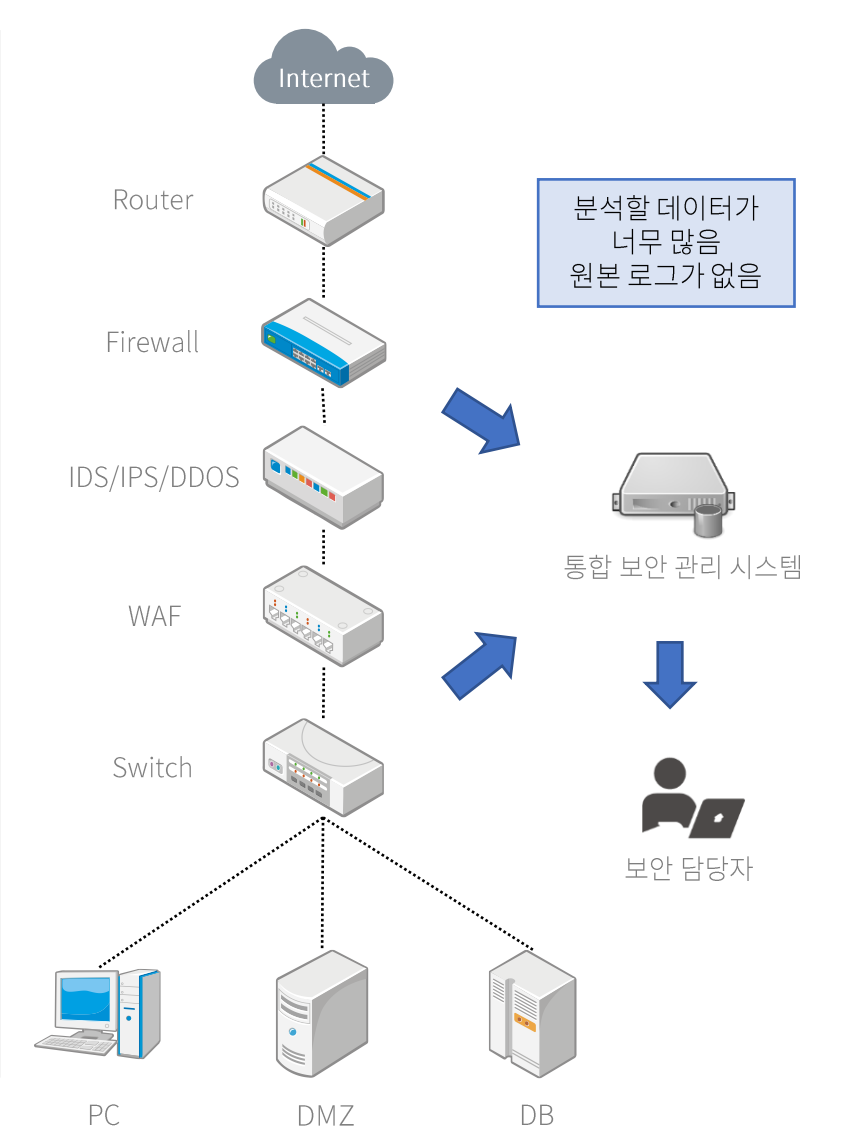
- Network Detection and Response
- Gartner, AI



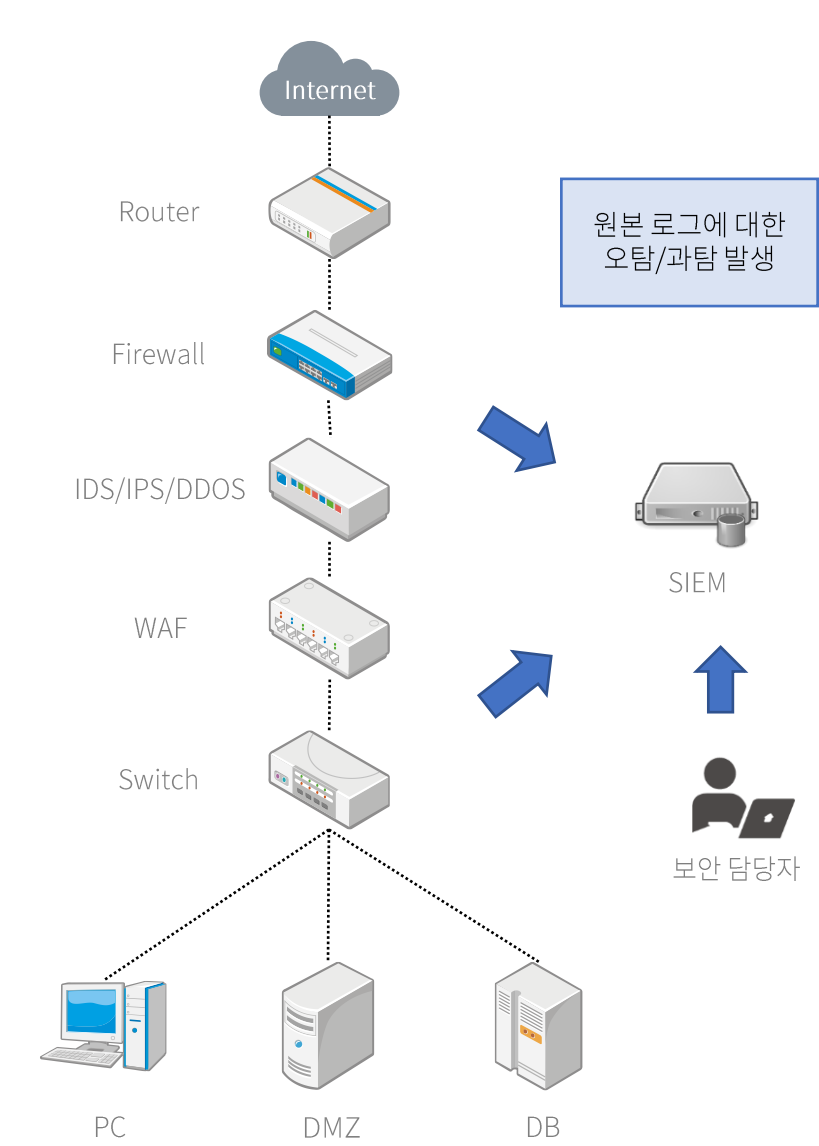
1. 직접 접근 분석 방식

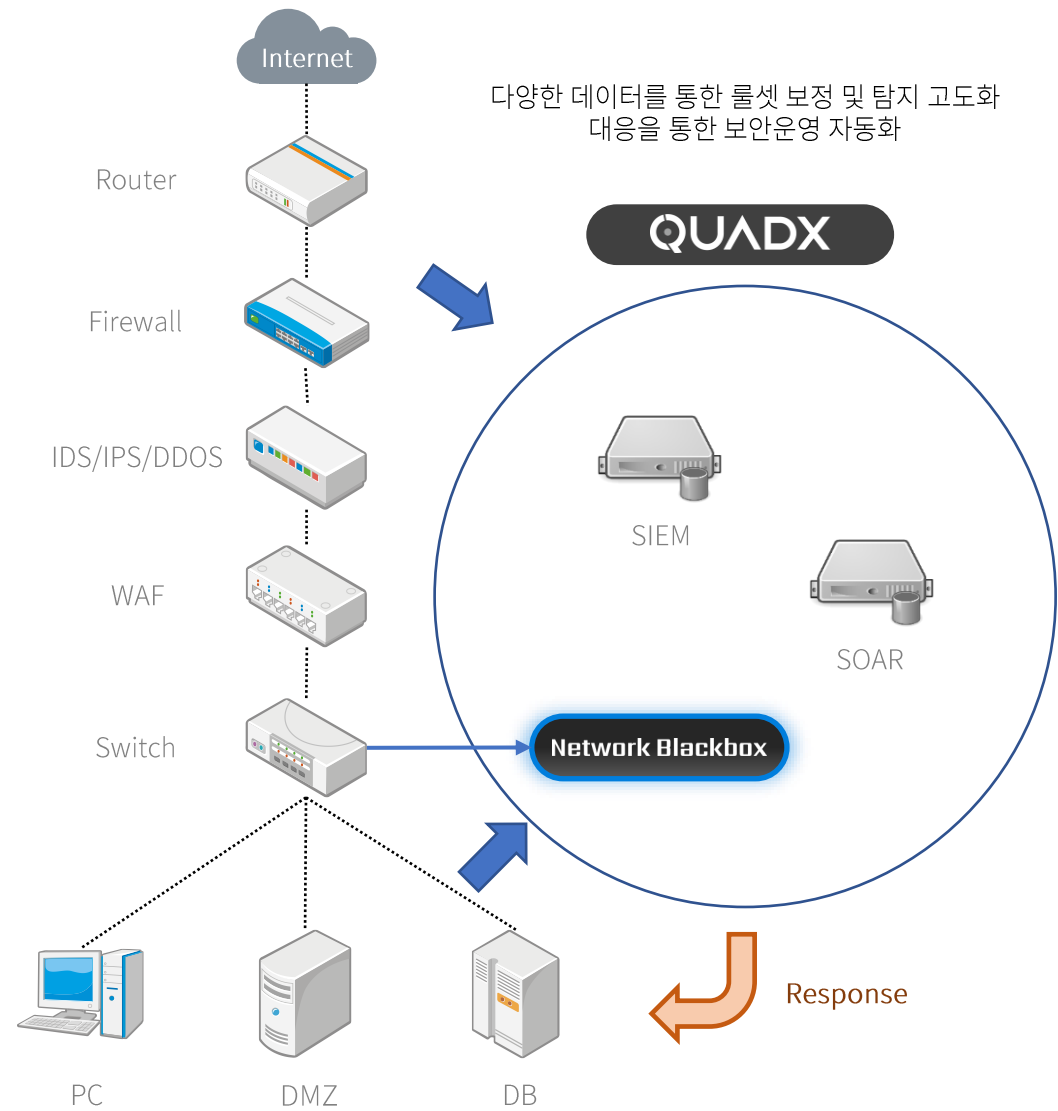
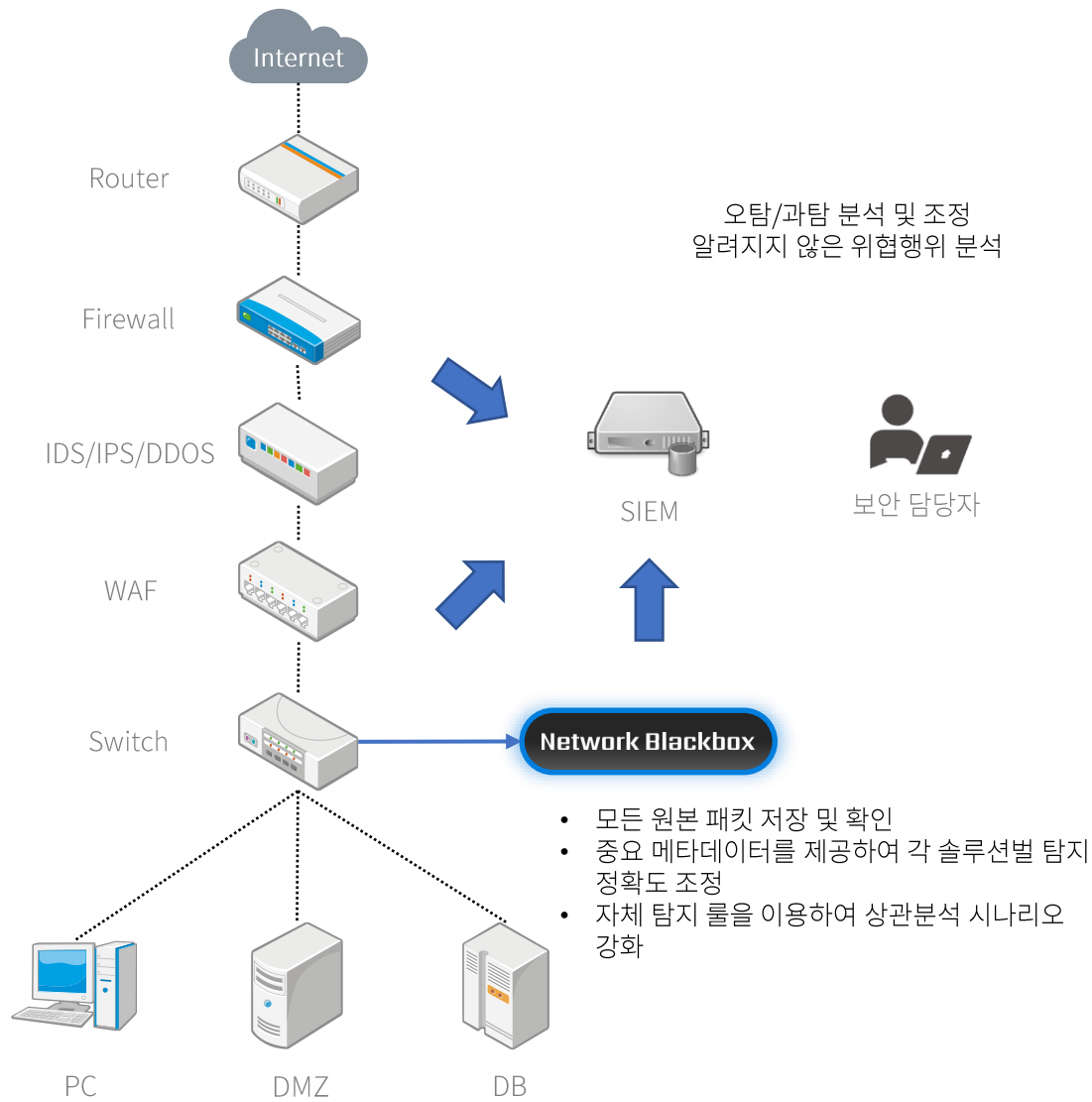


2. 로그 수집 분석 방식



3. 시나리오 분석 방식

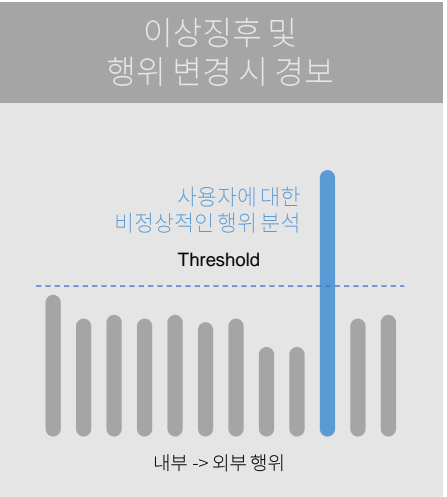
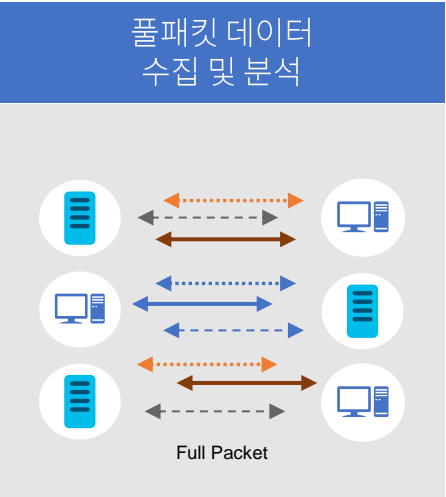






NDR 필수기능 요건

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



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

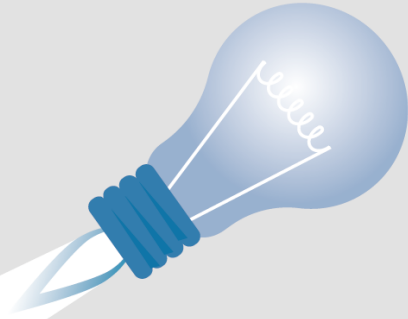
Key Findings

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





새로운 기술 등장 시 우리의 혼한 반응



인공지능이 뭐예요?

우린 어떻게 해야 해요?

빅데이터는?

그게 왜 중요해요?

다들 어떻게 하고 있어요?

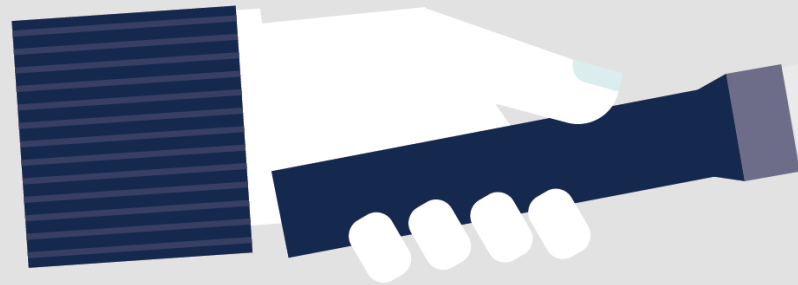
블록체인이 뭐예요?

사물인터넷이 뭐예요?

메타버스가 뭐예요?



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



고객이 불편함을 느끼는 것이 뭐지?

AI

X

NIA가 국비 지원해준다는데
김과장 빨리 과제하나 기획해봐!



요즘 ChatGPT가 대세라는데
뭐 할 수 있는 거 없어?

X



X

너도 나도 메타버스 사업 한다는데
우리도 뭐 해야 하지 않겠어?



고객들은 기술에 관심이 없다. 관심사는 오로지 문제해결 뿐

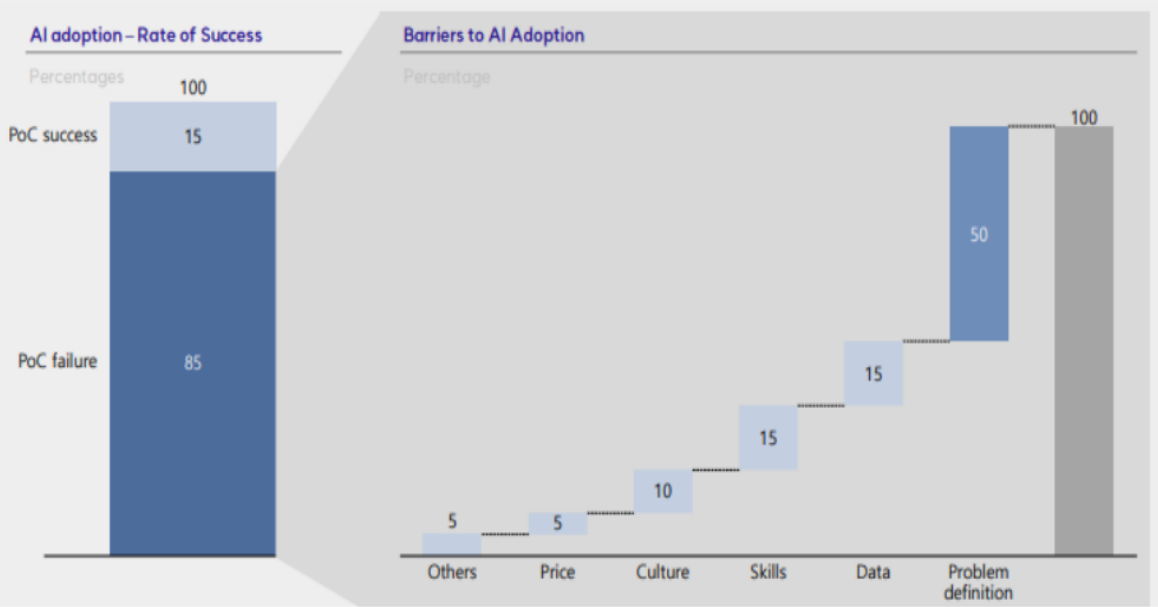
“고객 니즈에 대한 무지는 쓸고퀄* 서비스를 낳는다.”

*'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



CNN Regression을 이용한 LOTTO 번호 예측



Lucky 6

	1	2	3	4	5	6
1	10	23	29	33	37	40
2	9	13	21	25	32	42
3	11	16	19	21	27	31
4	14	27	30	31	40	42
5	16	24	29	40	41	42
6	14	15	26	27	40	42
7	2	9	18	25	28	40

	1	2	3	4	5	6
2	9	13	21	25	32	42
3	11	16	19	21	27	31
4	14	27	30	31	40	42
5	16	24	29	40	41	42
6	14	15	26	27	40	42
7	9	16	25	28	40	
8	8	12	25	34	37	39

	1	2	3	4	5	6
1086	11	16	25	27	35	36
1087	13	14	18	21	34	44
1088	11	21	22	30	39	44
1089		18	31	37	42	43
1090	12	19	21	29	40	45
1091		20	23	24	28	30
1092	7	12	13	26	33	45



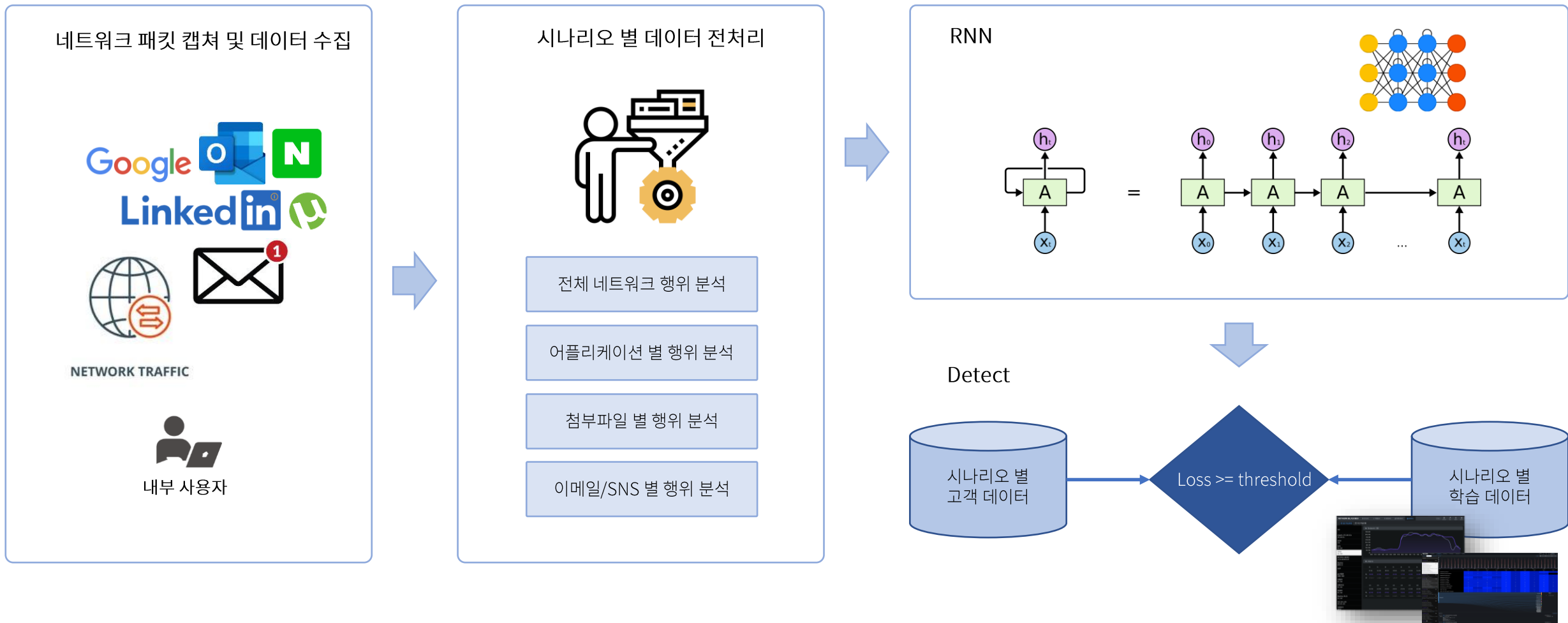
머니투데이
<https://news.mt.co.kr> · mtview

"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 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.

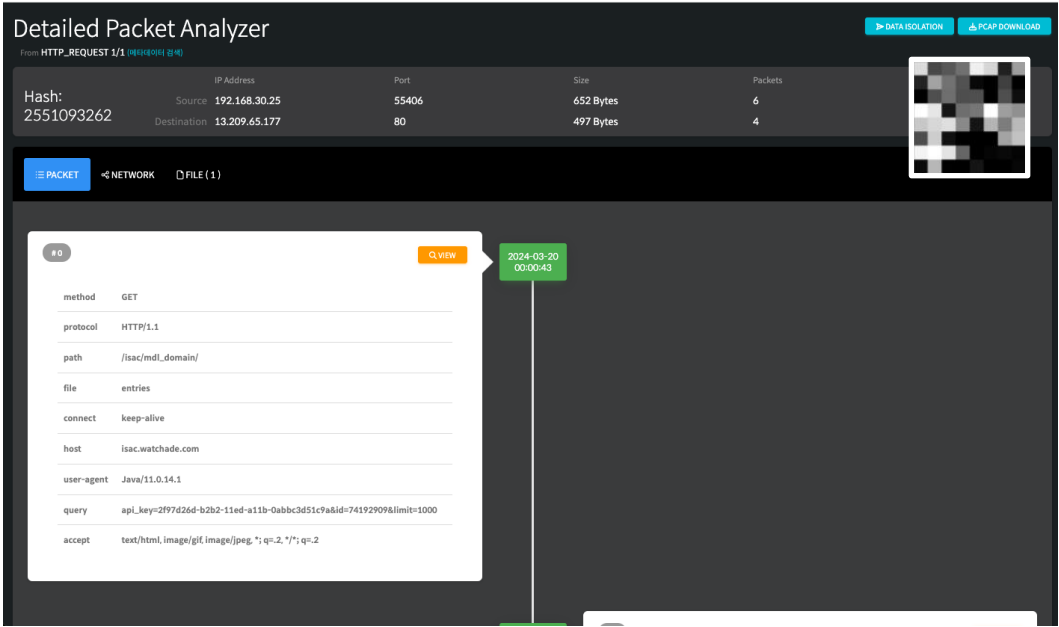
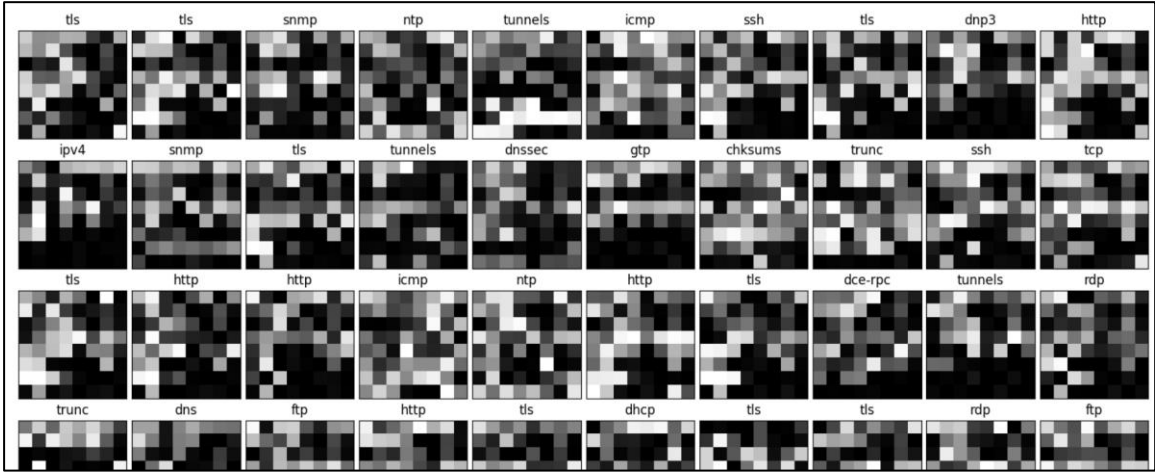
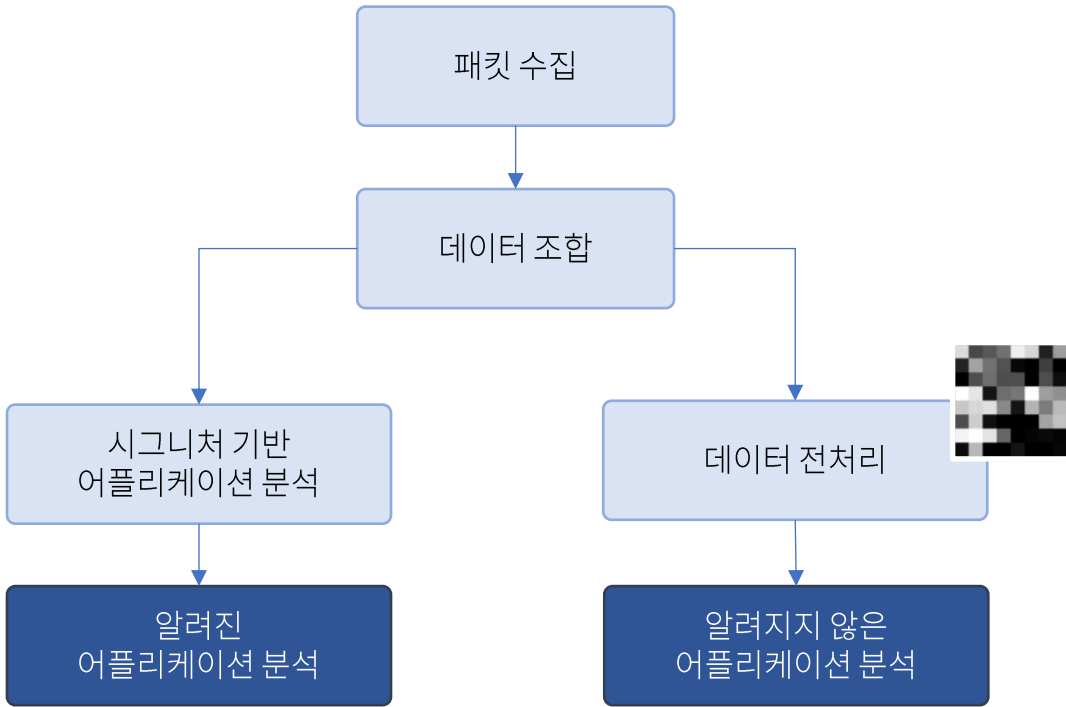
홍중선 성균관대 통계학과 교수는 "이들 업체 회원 가운데 1등 당첨이 된 사람이 많다고 하는 것은 사람들이 많이 찾는 복권 판매소에서 1등이 많이 배출됐다고 하는 것과 마찬가지로"라며 "회원이 많고 표본집단이 커져 1등이 많이 나오는 것이지 당첨 확률 자체가 높아지는 것은 아니다"라고 말했다.

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



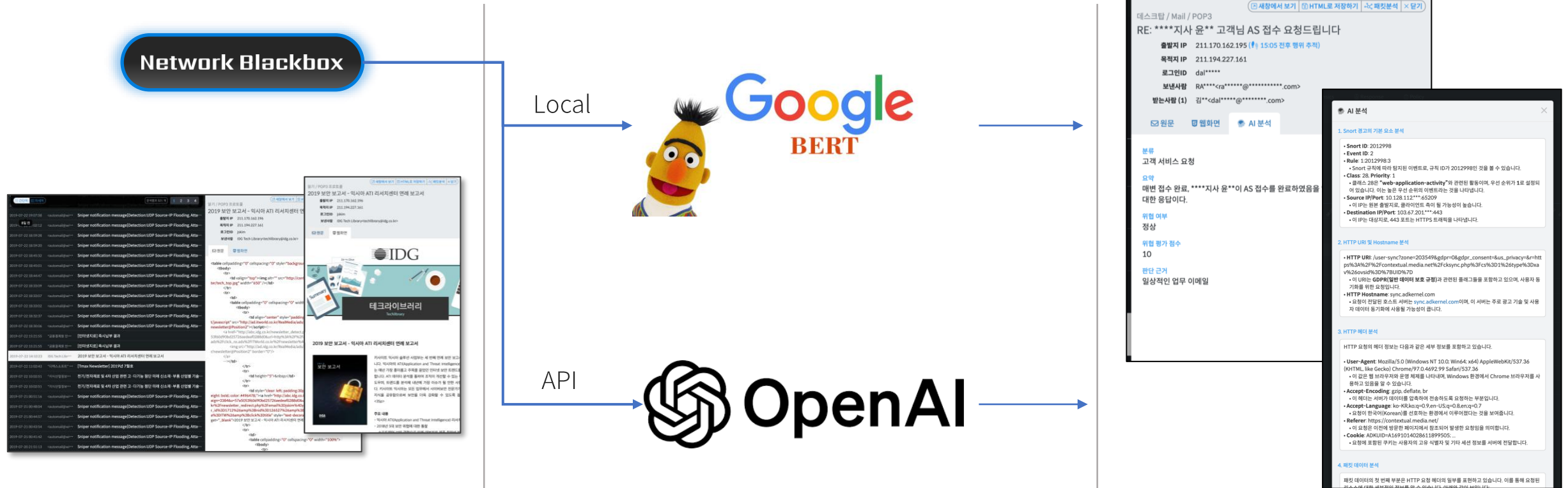


딥러닝을 이용한 효과적인 DPI(Deep Packet Inspection)
분석 방법



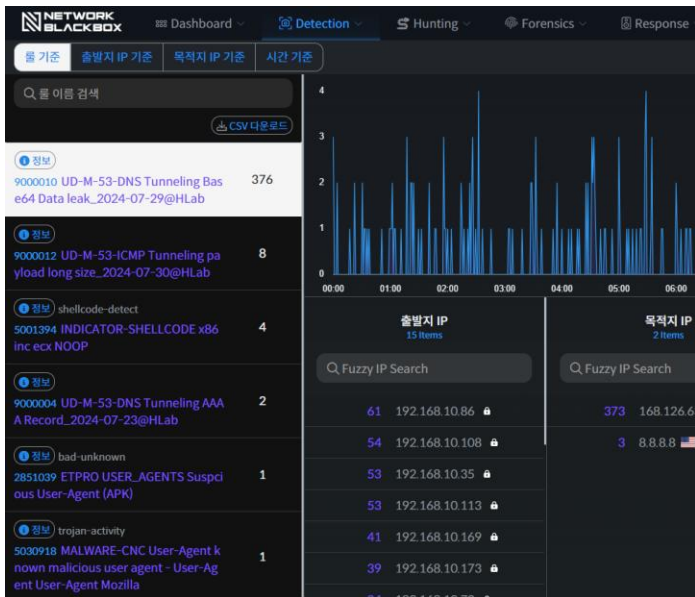

```
graph LR; A((TEXT)) --> B((LLM)); B --> C((TEXT))
```

A diagram illustrating the flow of information in a Large Language Model (LLM) system. It consists of three circular nodes connected by arrows. The first node on the left is light blue and labeled "TEXT". An arrow points from this node to a central dark blue node labeled "LLM". Another arrow points from the "LLM" node to a third light blue node on the right labeled "TEXT".





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



위협탐지물

SID
2851039

Target
PROOFPOINT

Message
ETPRO USER_AGENTS Suspicious User-Agent (APK)

Direction
tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS

Signature Severity
Informational

SID Description

한국어 영어 일본어

이 시그니처는 User-Agent 헤더에 의심스러운 값이 포함된 HTTP 트래픽을 탐지합니다. 이 시그니처는 홈 네트워크에서 외부 서버와의 통신에서 User-Agent 문자열이 관찰되는 인스턴스를 플레그로 지정합니다. 이러한 User-Agent 값의 존재는 잠재적으로 악의적이거나 비정상적인 활동을 나타낼 수 있습니다.

원문

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS ( msg:"ETPRO USER_AGENTS Suspicious User-Agent (APK)"; flow:established,to_server; http_header, content:"APK",fast_pattern; reference:md5,421db415c54471b31edb37c12c31008d; classtype:bad-unknown; sid:2851039; rev:1; metadata:attack_target Mobile_Client,created_at 2022_02_01,deployment Perimeter,former_category USER_AGENTS,signature_severity Informational,updated_at 2022_02_01; )
```

LLM

AI 분석

1. Snort 경고의 기본 요소 분석

- Snort ID:** 2012998
- Event ID:** 2
- Rule:** 1:2012998:3
 - Snort 규칙에 따라 탐지된 이벤트로, 규칙 ID가 2012998인 것을 볼 수 있습니다.
- Class:** 28, **Priority:** 1
 - 클래스 28은 "web-application-activity"와 관련된 활동이며, 우선 순위가 1로 설정되어 있습니다. 이는 높은 우선 순위의 이벤트라는 것을 나타냅니다.
- Source IP/Port:** 10.128.112***:65209
 - 이 IP는 원본 출발지로, 클라이언트 측이 될 가능성이 높습니다.
- Destination IP/Port:** 103.67.201***:443
 - 이 IP는 대상지로, 443 포트는 HTTPS 트래픽을 나타냅니다.

2. HTTP URI 및 Hostname 분석

- HTTP URI:** /user-sync?zone=203549&gdpr=0&gdpr_consent=&us_privacy=&r=ht ps%3A%2F%2Fcontextual.media.net%2Fcsync.php%3Fcs%3D1%26type%3Dxa v%26ovsid%3D%7BUID%7D
 - 이 URI는 **GDPR(일반 데이터 보호 규정)**과 관련된 플래그들을 포함하고 있으며, 사용자 동기화를 위한 요청입니다.
- HTTP Hostname:** sync.adkernel.com
 - 요청이 전달된 호스트 서버는 **sync.adkernel.com**이며, 이 서버는 주로 광고 기술 및 사용자 데이터 동기화에 사용될 가능성이 큼니다.

3. HTTP 헤더 분석

HTTP 요청의 헤더 정보는 다음과 같은 세부 정보를 포함하고 있습니다.

- User-Agent:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.99 Safari/537.36
 - 이 값은 웹 브라우저와 운영 체제를 나타내며, Windows 환경에서 Chrome 브라우저를 사용하고 있음을 알 수 있습니다.
- Accept-Encoding:** gzip, deflate, br
 - 이 헤더는 서버가 데이터를 압축하여 전송하도록 요청하는 부분입니다.
- Accept-Language:** ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
 - 요청이 한국어(Korean)를 선호하는 환경에서 이루어졌다는 것을 보여줍니다.
- Referer:** https://contextual.media.net/
 - 이 요청은 이전에 방문한 페이지에서 참조되어 발생한 요청임을 의미합니다.
- Cookie:** ADKUID=A1691014028611899505;...
 - 요청에 포함된 쿠키는 사용자의 고유 식별자 및 기타 세션 정보를 서버에 전달합니다.

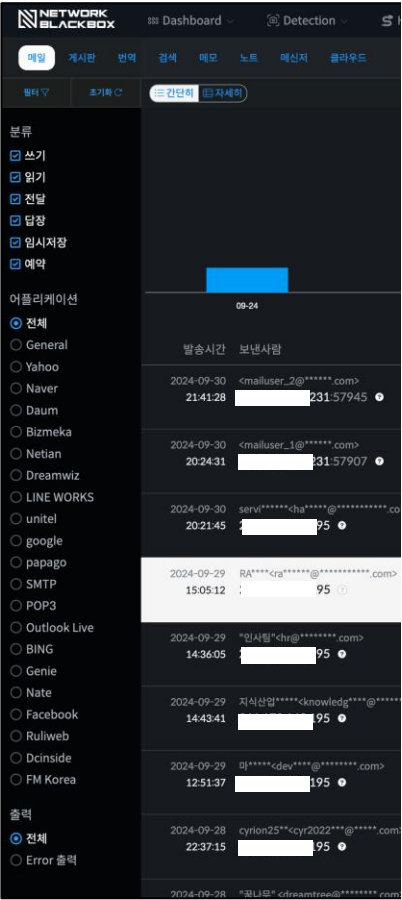
4. 패킷 데이터 분석

패킷 데이터의 첫 번째 부분은 HTTP 요청 헤더의 일부를 표현하고 있습니다. 이를 통해 요청된 리소스에 대한 세부적인 정보를 알 수 있습니다. 아래와 같이 보일 수 있습니다.



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



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** 고객님의 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

데스크탑 / Mail / POP3

RE: ****지사 윤** 고객님의 AS 접수 요청드립니다

출발지 IP 195 (15:05 전후 행위 추적)

목적지 IP 161

로그인ID dal*****

보낸사람 RA*****@*****.com>

받는사람 (1) 김**<dal*****@*****.com>

원문 웹화면 AI 분석

분류
고객 서비스 요청

요약
매번 접수 완료, ****지사 윤**이 AS 접수를 완료하였음을 알리는 이메일로, 고객의 요청에 대한 응답이다.

위험 여부
정상

위험 평가 점수
10

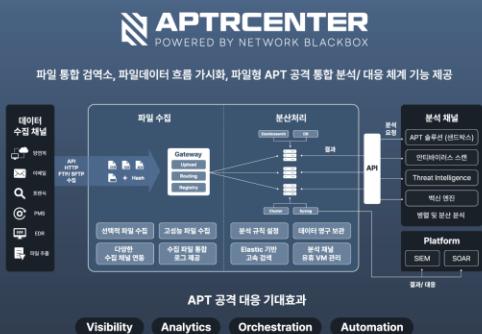
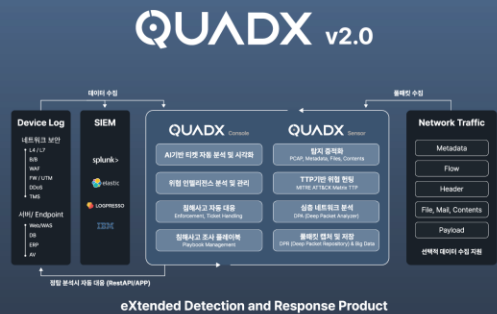
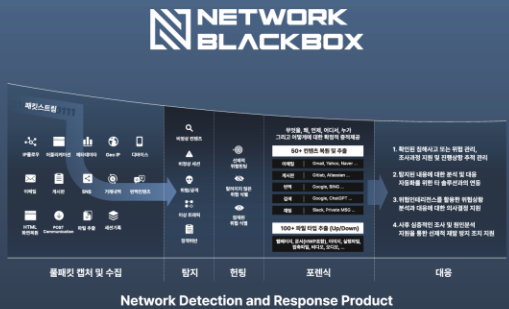
판단 근거
일반적인 업무 이메일



주요 제품 Portfolio

Quad Miners

첨단산업을 지키는 사이버보안,
방산기술보안 및 AI 보안분야 전문기업



부스 위치 (P05)



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

HUNTOR GET HUNTED

Revolutionizing cyber warfare with Network Blackbox



Quad Miners