Data Leak Protection Strategy

EMASS AI

대외비 2024.03.10.

XCURENET

AGENDA

Ⅰ DLP* Analytics Trend

Ⅱ Pain Point

Ⅲ Why EMASS AI ?

Ⅳ EMASS AI 주요기능

Ⅴ Feasible Cases

Ⅵ Use Cases

* DLP : Data Loss Prevention

XCURENET

Chapter

I DLP Analytics Trend

“ DLP Analytics Trend ”

01

원격/하이브리드 작업
: 우발적・악의적
정보 유출

02

조직적 공모 행위로
인한 정보 유출
위험 증가

03

AI 데이터 분석
필요성 증가

04

빠르게
변화・증가하는 위험
: 규정 준수
요구사항 증가

01 원격/하이브리드 작업 : 우발적 · 악의적 정보 유출 가능성 증가

원격/하이브리드 작업 환경 도입으로 인해 직원들이 직접적인 통제 범위를 벗어나며 업무와 사생활이 혼합되는 경우가 많아집니다.

자신의 모바일 기기와 일반 사용 앱을 업무에 사용하는 경우가 증가합니다.

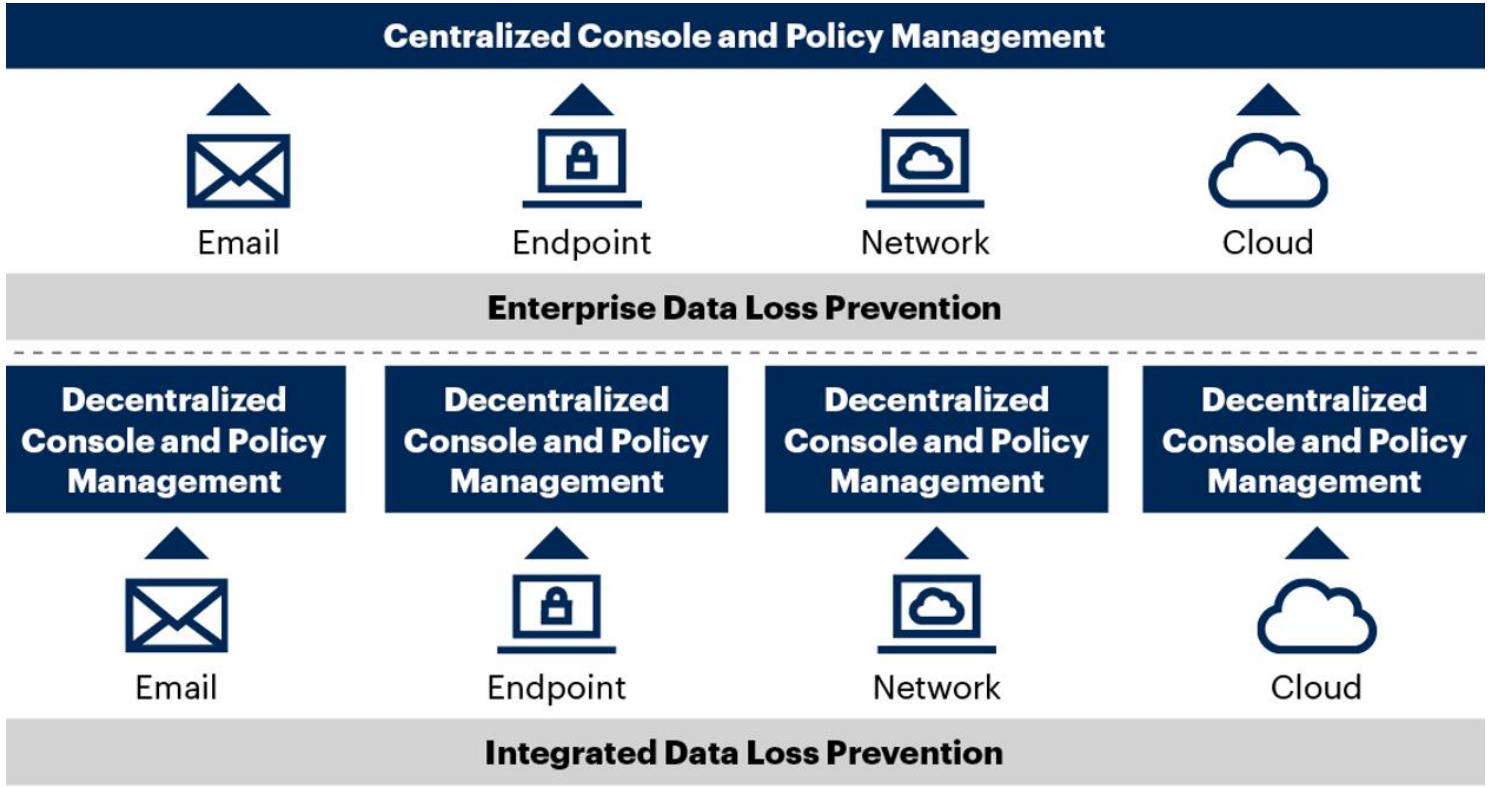
Global DLP Market

- ✓ 원격/하이브리드 작업 모델에서 중요한 데이터를 우발적 · 악의적으로 노출할 가능성이 증가합니다.
- ✓ 이에 따라 DLP 솔루션에 대한 필요성이 증가하고 솔루션은 최종 사용자 활동에 초점을 맞춰야 합니다.
- ✓ DLP 솔루션 분석은 최종 사용자에 집중될 것으로 예상됩니다.

02 조직적 공모 행위로 인한 정보 유출 위험 고려

전통적으로 개인적 일탈 문제로 간주되는 정보 유출에서 조직적 공모 행위 위험이 증가합니다.

향후 기업은 데이터 유출 위험 방지를 위해서 개인적 일탈 및 조직적 공모 위험 모두를 고려해야 합니다.



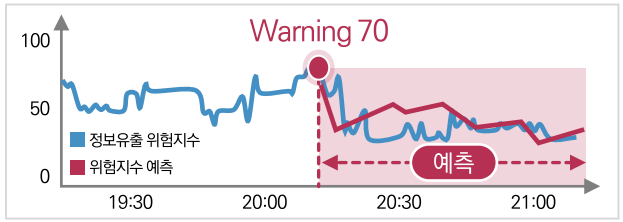
통합적 DLP 대응 필요

- ✓ 외부 공모자와 모의하여 지속적으로 이메일을 이용하여 특정 데이터를 추출하고 유출하기 위한 표적화된 정보유출 시도가 가능합니다.
- ✓ 이에 대응하여 사용자 기반으로 개인적 일탈 뿐만 아니라 조직적 공모에 의한 정보유출 위험도 고려하는 통합 DLP 대응이 필요합니다.

03 AI 데이터 분석 필요성 대두

인공지능(AI) 기술은 정보유출 방지를 위해서 패킷 정보 및 내용 분석에 사용될 수 있습니다.

최신 DLP 플랫폼은 인공 지능(AI) 기술을 사용하여 기능과 성능을 향상합니다.



위험도 분포 기반 이상치 원인 분석

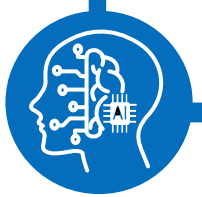
주요 원인

1. activeService — Top 10 원인분석
2. activeServiceRCount3
3. inode_used_pct
4. in_pps_max
5. mem_usage_#1
6. mem_usage_#2
7. cpu_runqueue
8. in_bps_avg
9. activeServiceRCount1
10. out_bps_avg

원인별 상세 분석

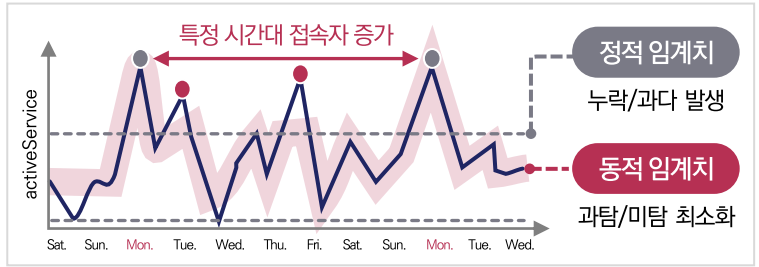
정보유출 위험지수
내용 기반 이상감지
사용자별 이상감지
…

서비스 위험지수		원인 분석	동적 임계치
서비스	시계열 예측	주요 인자 도출	정상 패턴 분석
성능	통합 스코어링	영역간 이벤트 상관 분석	동적 임계치 생성
로그			



AI 통합 모니터링

동적 임계치
요일/시간별 패턴에 따른 정상상태 학습



DLP 분야 AI 활용

✓ 다른 분야와 마찬가지로, DLP에서도 인공지능(AI)을 사용하여 새로운 기능을 추가하고 성능을 향상합니다.

✓ 인공지능(AI) 기술은 민감하고 위험성이 높은 데이터의 식별, 무단 데이터 사용 패턴 파악, 데이터 처리 정책 시행 자동화 기능을 수행하여 내부 정보를 지속적이고 효과적으로 보호할 수 있습니다.

04 빠르게 변화하고 증가하는 위험 : 규정 준수 요구사항 증가

변화하고 증가하는 위험에 따라 다양한 규정 준수 요구사항이 추가됩니다.

향후 추가될 수 있는 규정에 대한 유연한 대응이 필요합니다.

규정 준수를 위한 데이터 인식 및 유연한 사용

정책 변화에 따라 규정 준수를 받는 데이터를 효과적으로 인식하고 이에 따른 전체 데이터 처리 프로세스 재설계를 지원해야 합니다.

정책 변화에 따른 확장성 있는 아키텍처 지원

규정 강화 및 신규 규정 추가시 검토 및 적용 되어야 할 데이터의 수량은 기하 급수적으로 증가하며 이를 빠르고 무결하게 지원할 수 있는 아키텍처가 필요합니다.

장기적인 데이터 관리 및 거버넌스 지원

데이터 원천, 메타 데이터 관리 뿐만 아니라 데이터 생애주기 측면까지 관리되어야합니다.

규정 준수 요구사항 증가

- ✓ 정보침해 위험이 지속적으로 확대됨에 따라 민감한 데이터의 안전을 보장하는 규정 준수 요청이 더욱 강화될 것으로 예상됩니다.
- ✓ 향후 더 많은 규정 준수 표준이 등장할 것으로 예상할 수 있습니다.

Chapter

II Pain Point

XCURENET

Data Loss Prevention(DLP)에 대한 고민

1

복잡하고 다양한 분석에 필요한 **패킷** 및 **내용 데이터**를 어떻게 수집 적재할지?

2

방대한 **비정형 데이터** 대상으로 정보유출 위험 패킷과 내용을 인식하고 추출할지?

3

사용자 활동을 종합적으로 평가하여 **정보유출 위험도**를 **측정**할 수 있는가?

4

강화되고 **신설**되는 **규정 준수**에 유연하게 대응할 수 있는가?

Chapter

III Why EMASS AI ?

EMASS AI는

EMASS AI는 방대한 양의 정보를 수집, 처리하여 AI로 빠르게 분석하여 이해하기 쉽게 시각화 하는 '통합 DLP AI 플랫폼' 입니다.

EMASS AI

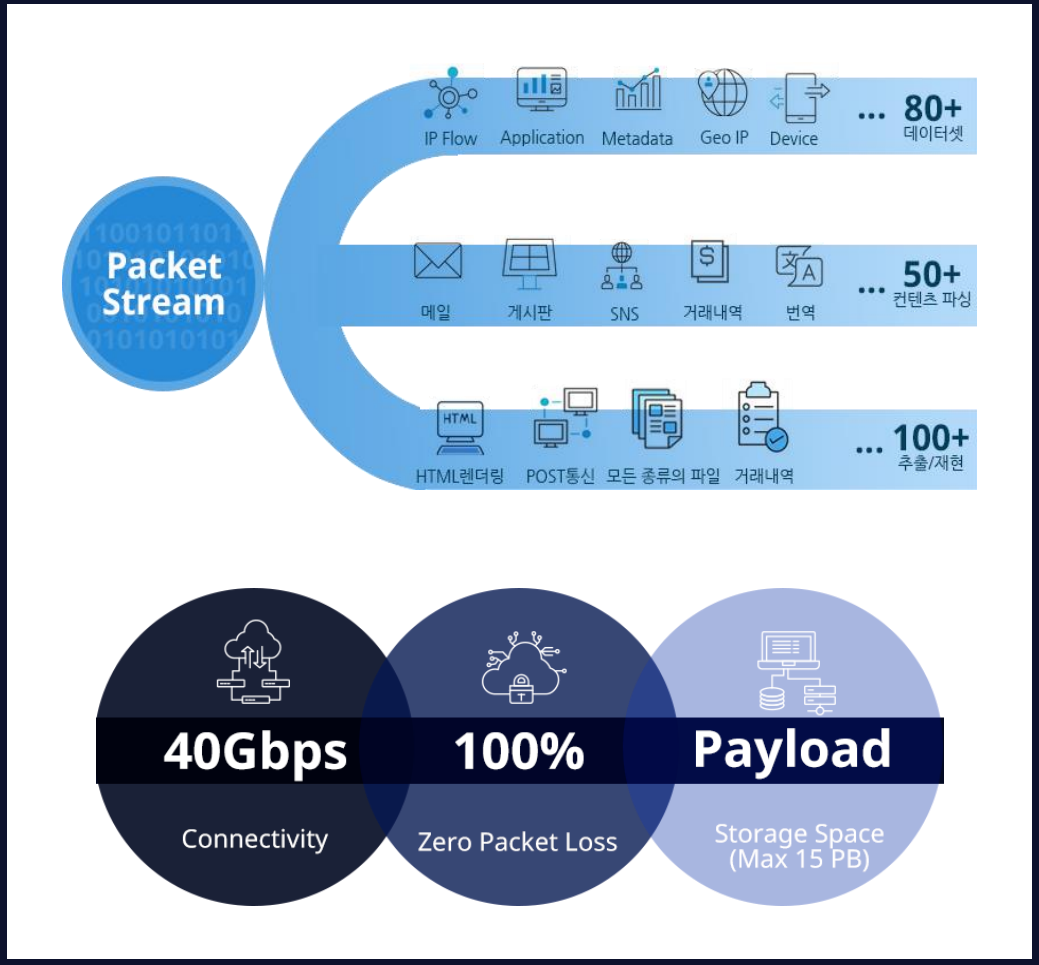
활용

Analytics Services

콘텐츠 기반 정보유출 | 이상행위 예측

OCR	데이터 분류	행동분석
Text Dection	이진 분류	정상 범주
Data Preparation	다중 분류	비정상 범주
	Deep Learning	비정상 범주

Private / Public On Premise



EMASS AI는 수집된 풀패킷 테이터와 콘텐츠를 대상으로 이상 징후를 탐지하고 정보유출 위험도를 자동으로 측정합니다.

1. 다양한 유형의 데이터와 다수의 데이터 소스로부터 수집이 가능합니다.
2. 풀패킷 데이터 수집 및 처리가 가능합니다.
3. 수집된 콘텐츠 대상으로 AI 를 통한 정보유출 위험도를 측정합니다.
4. 정보유출 위험도 패턴 도출을 통해 이상행위 수준을 감지합니다.
5. 패킷 데이터 및 콘텐츠 대상으로 파싱(Parsing) 자동화를 지원합니다.

EMASS AI는 사용자 및 활동 단위 시나리오 기반으로 이상 행위를 감지하고 경보할 수 있습니다.

1. 민감하고 위험성 높은 데이터를 식별합니다.
2. 무단 데이터 사용 및 전송 패턴을 파악합니다.
3. 데이터 처리 정책 시행 자동화 기능을 제공합니다.
4. 사용자 및 활동 단위 시나리오 기반 이상 행위를 감지합니다.
5. 정보유출 통합 모니터링 Dashboard를 제공합니다.

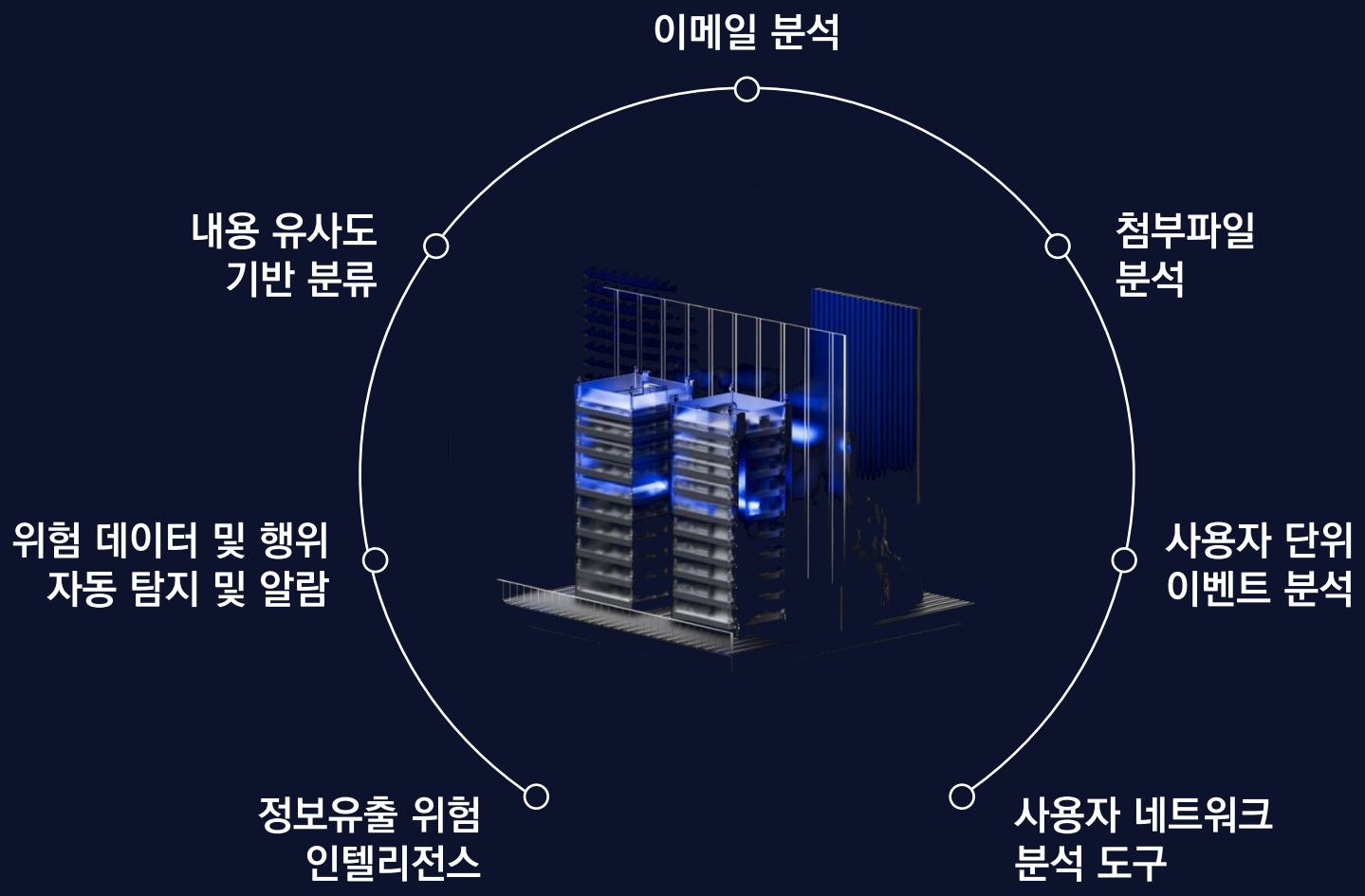
EMASS AI는
개인정보 · 민감정보 식별 및 무단 데이터 사용 파악을 지원하여 규정 변화에 유연하게 대응할 수 있습니다.

1. 규정 준수 대상이 되는 개인정보 및 민감정보를 식별합니다.
2. 정책에 따른 규정 준수 데이터 변화 및 시스템 영향도를 측정합니다.
3. 데이터 생애주기를 고려하는 거버넌스를 지원합니다.
4. 민감 데이터 관련 규정 표준을 준수합니다.

Chapter

Ⅳ EMASS AI 주요기능

이메일 분석에서 도출한 유출 위험에 대한 정보를 사용하여 이상징후를 찾아냅니다.
EMASS AI의 통합 모니터링을 통해 유출 발생 전 이를 식별하고 제거할 수 있습니다.



AI와 결합된 정보유출 방지 기능 제공

EMASS AI는『콘텐츠 단위 정보유출 위험 감지』,『사용자 행동분석』,『정보유출 모니터링』을 위해 AI와 결합된 기능을 제공합니다.

EMASS AI 기능 구조도

AI 위험도 평가

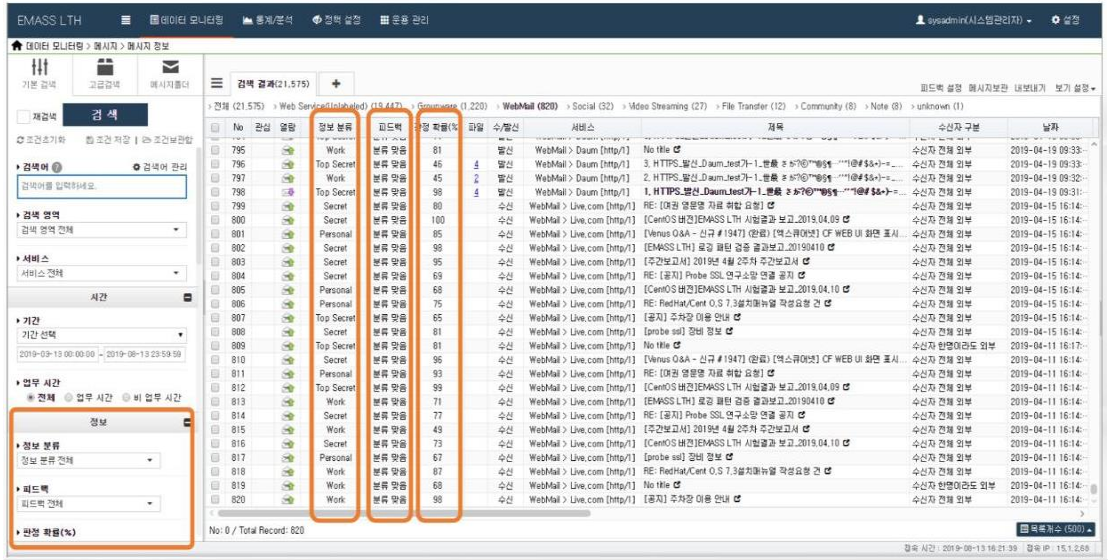
[콘텐츠 단위 유출 위험 감지]

유통되는 콘텐츠를 AI 기술로
지속적으로 검색하여
정보유출 위험을 완화하고
콘텐츠 단위 유출 위험을 평가합니다.

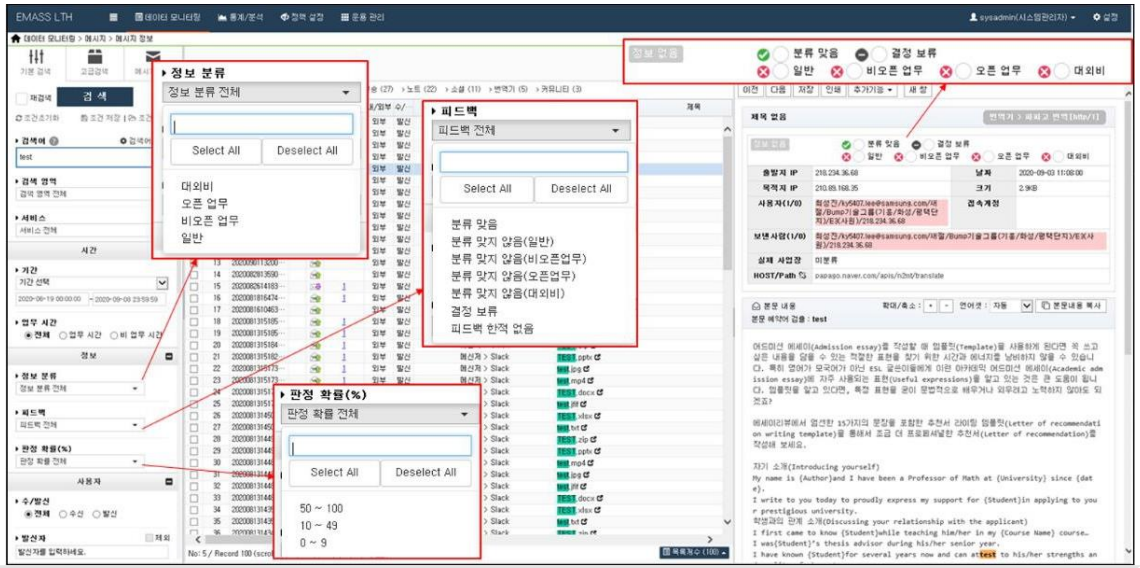
01 내용 기반 메일 위험도 분석

EMASS AI는 이메일 본문과 첨부파일, 사내 메신저를 대상으로 정보분류 · 피드백 · 판정확률와 함께 자동 판정된 데이터 검색 기능을 제공합니다. 자연어처리(NLP) 사용하여 키워드 단위 의미를 반영한 내용 기반 메일 위험도 분석 결과를 제공합니다.

메시지 정보 자동분류



사용자 피드백 기반 정확성 향상



키워드 단위 『의미』 반영 내용 기반 메일 위험도 분석

표제어 추출 (Lemmatization)	형태학적 분할 (Morphological segmentation)	품사 태그 지정 (Part-of-speech tagging)	어간추출 (Stemming)	문장 끊기 (Sentence breaking)

02 유사 메일 분석

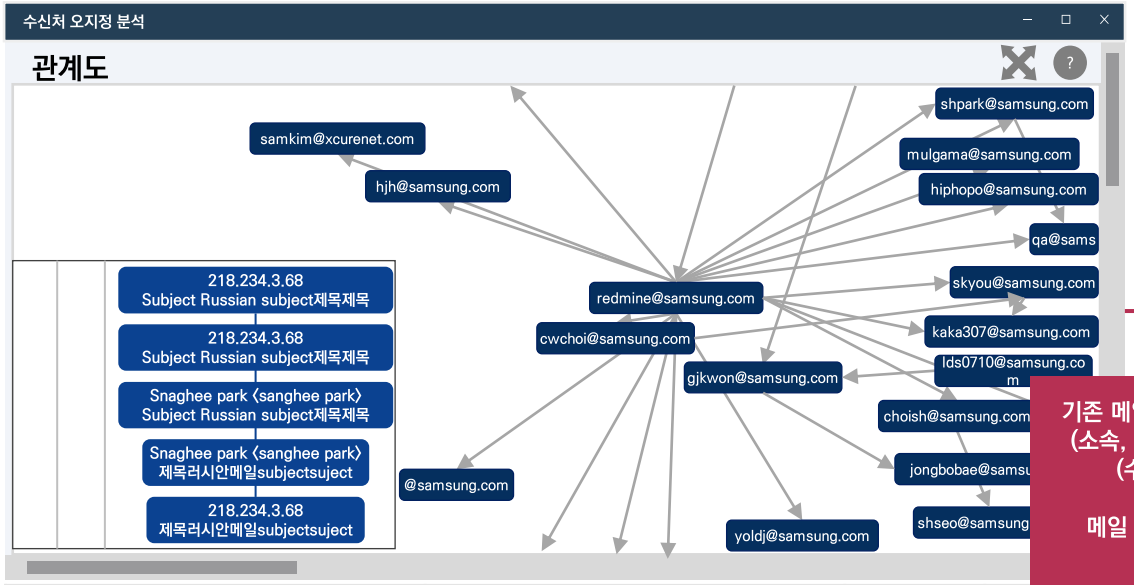
EMASS AI는 메일 본문 및 첨부파일 대상 유사 콘텐츠 검색 기능을 제공합니다. 위험도 높은 메일에 대해서 본문 및 첨부파일 기준 내용상 유사한 메일을 검색하여 상호간 위험도를 비교하고 위험 패턴을 발견할 수 있습니다.

메일 본문 및 첨부파일 내용 추출

본문 문자열 문서종류별 첨부파일	첨부파일 내용(그림 표 포함) 추출	고속 토크나이징	NbyN 문자열 매칭	문서 단위 유사도 측정

03 수신처 오지정 분석

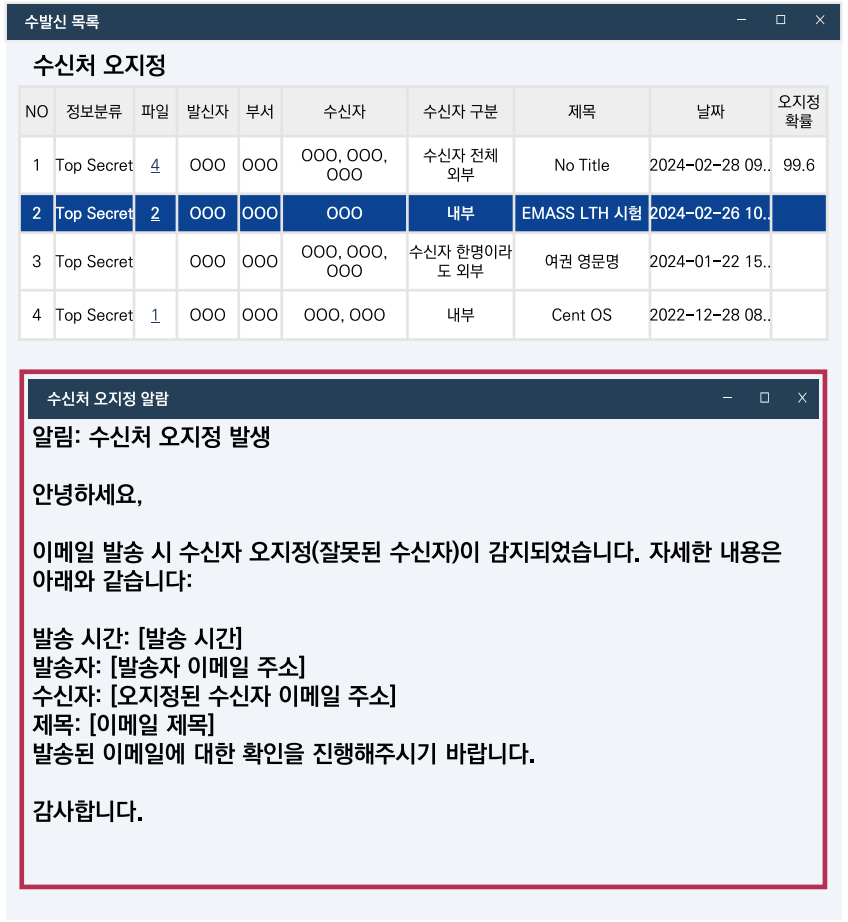
EMASS AI는 메일 수발신 네트워크 학습 모델을 기반으로 관계사 동명이인 수신처 오지정 메일 분석 기능을 제공합니다.
기존 수발신 패턴을 학습하여 패턴에 벗어나는 확률 낮은 수발신 목록을 추출하고 이를 관리자에게 자동 통보합니다.



기존 메일 수발신 네트워크 분석
(소속, 개인, 직군 : 노드 정보)
(수발신 : 엣지 정보)

메일 수발신 확률 머신러닝
학습 모델

발신노드			수신노드			수신자 구분	오지정 확률
소속	직군	성명	소속	직군	성명		
OO	OO	OOO	OO	OO	OOO, OOO, OOO	수신자 전체 외부	95.6
OO	OO	OOO	OO	OO	OOO	내부	91.0
OO	OO	OOO	OO	OO	OOO, OOO, OOO	수신자 한명 이라도 외부	90.5
OO	OO	OOO	OO	OO	OOO, OOO	내부	85.5



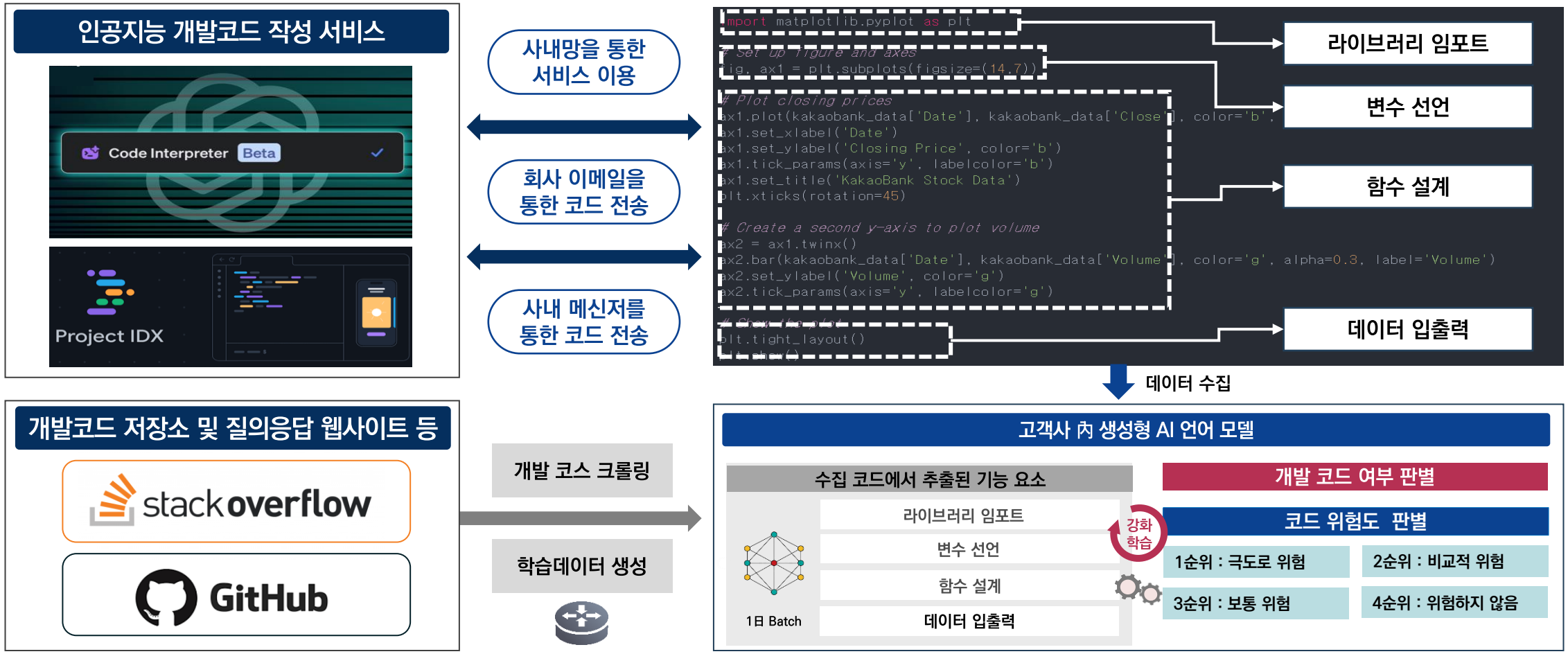
NO	정보분류	파일	발신자	부서	수신자	수신자 구분	제목	날짜	오지정 확률
1	Top Secret	4	OOO	OOO	OOO, OOO, OOO	수신자 전체 외부	No Title	2024-02-28 09..	99.6
2	Top Secret	2	OOO	OOO	OOO	내부	EMASS LTH 시험	2024-02-26 10..	
3	Top Secret		OOO	OOO	OOO, OOO, OOO	수신자 한명이라도 외부	여권 영문명	2024-01-22 15..	
4	Top Secret	1	OOO	OOO	OOO, OOO	내부	Cent OS	2022-12-28 08..	

04 관심 동향 분석

EMASS AI는 사내망을 통한 외부 검색어 로깅 및 분석을 통해 검색 키워드 추이 등 관심 동향 정보를 제공합니다. 또한 특정 서비스 이용 통계, 부서별 검색 키워드 동향 분석 기능을 가능합니다.

05 소스코드 유출 탐지

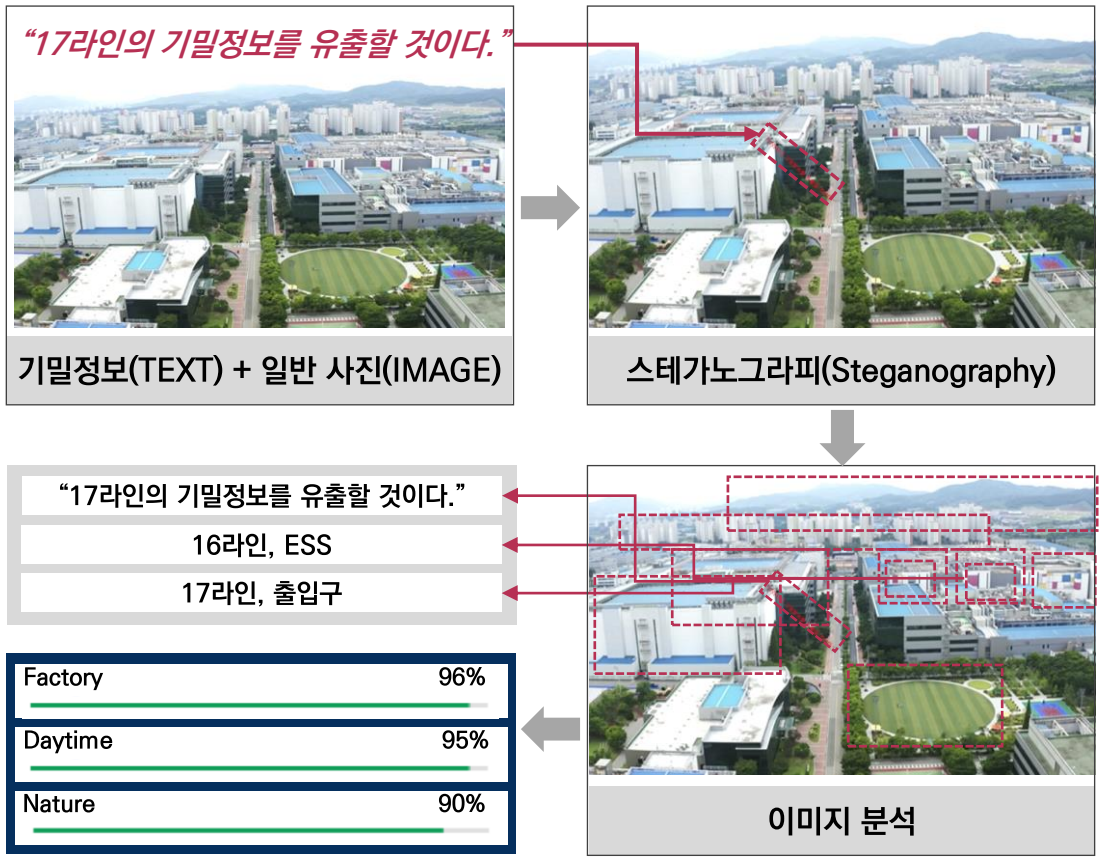
사내망을 인공지능 개발코드 작성 서비스 이용을 통한 개발 소스코드 유출을 탐지하기 위해 개발 코드 기반으로 학습데이터를 구축하고 개발 코드 및 해당 코드의 위험도를 판별할 수 있는 고객사 내에 설치할 수 있는 생성형 언어모델을 제공합니다.



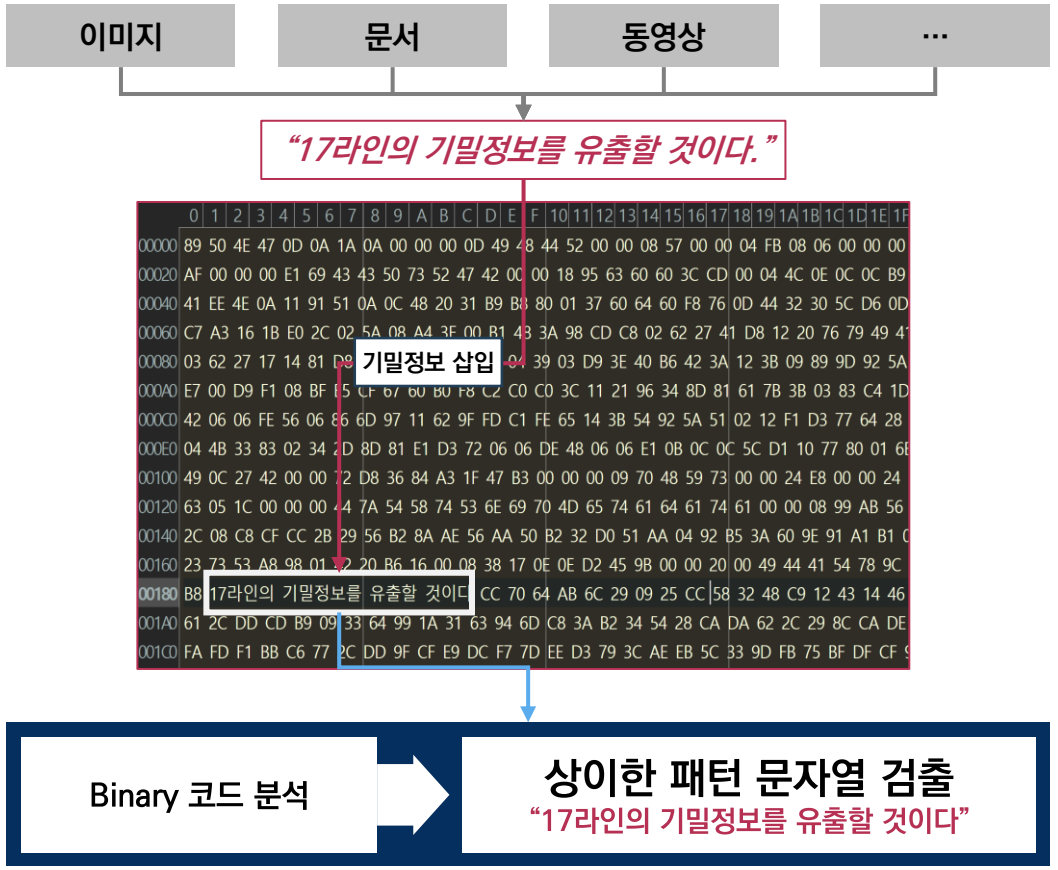
06 스테가노그라피 탐지

스테가노그라피 중, 이미지 상에 텍스트를 숨기는 경우는 이미지 분석 기반 의미 추출을 통해 텍스트 및 이미지 등 기밀정보 포함 여부를 검증하고 및 기밀정보를 추출할 수 있고, 각종 파일 binary 코드에 기밀정보를 숨기는 경우는 Binary 코드 분석을 통한 상이한 패턴 데이터를 추출하는 방식으로 대응할 수 있습니다.

이미지 내 기밀정보를 숨기는 경우



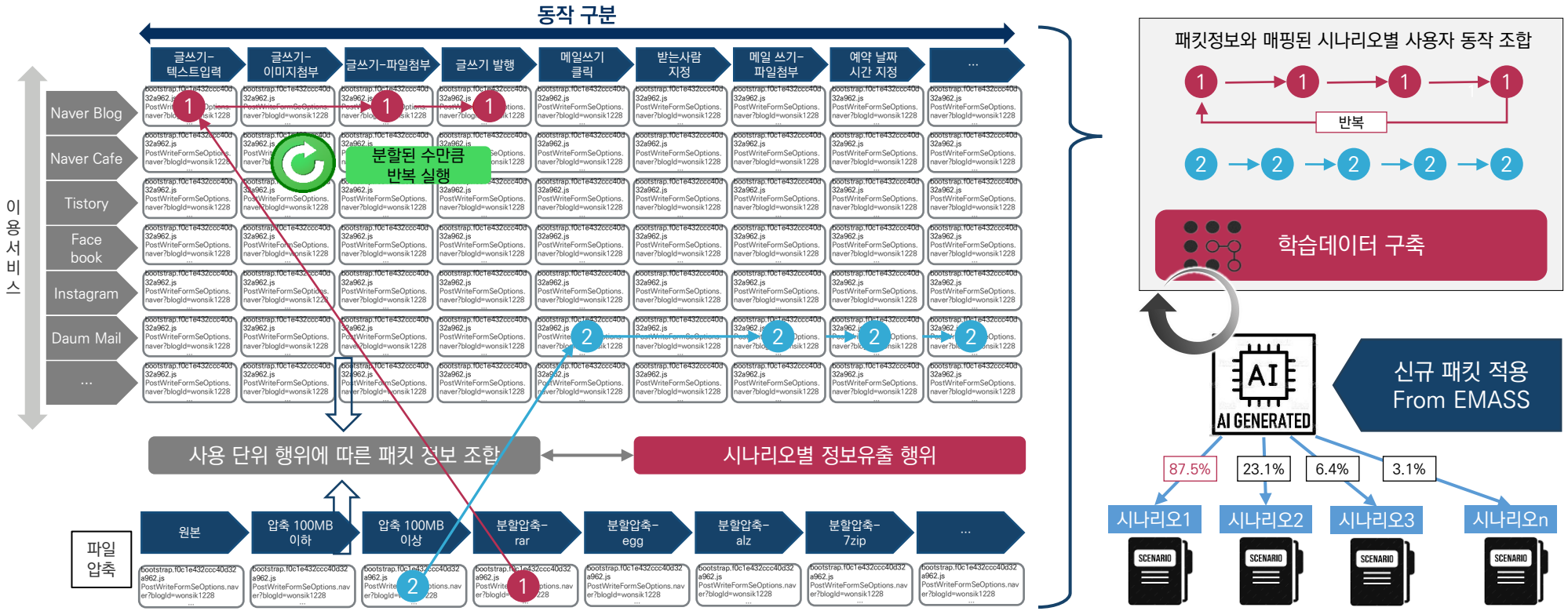
파일 Binary 코드에 기밀정보를 숨기는 경우



07 시나리오 기반 이상 징후 탐지

이상 징후 탐지를 위한 시나리오를 위해서 패킷 정보를 사용하여 『이용서비스-이용동작』을 구분하고 매핑하여 수집되는 데이터 패턴을 학습데이터로 구축합니다. 신규 유입되는 패킷 정보들을 사전정의된 시나리오별 적용 확률 등으로 표시됩니다.

- [시나리오 1] 내부설계도(대외비) 대용량 파일을 분할압축하여 네이버 블로그 글 쓰기 수정 하고 파일 첨부 기능 을 이용하여 반복 유출
- [시나리오 2] 내년사업계획(대외비) 파일을 압축하여 예약메일 내년 1월 1일 발송 설정하고 발송, 발송완료이전 재택근무시 예약메일함에서 개인PC로 유출



07 시나리오 기반 이상 징후 탐지

정보유출 대상 및 위험 유형 도출을 통한 이상징후 알람을 전송하고 상세정보를 확인하여 요인을 확인할 수 있습니다.

정보유출 대상 및 위험 유형 도출

정보유출 대상 Category

메일 본문	첨부파일	이미지
수신자	예약메일	분할압축

위험유의유형

이상징후 자동 검출

정보유출 시나리오

1. 내부 설계도(대외비) 대용량 파일을 분할 압축하여 네이버 블로그 글쓰기 수정에서 파일 첨부 기능을 통해 반복 유출

2. 내년사업계획(대외비) 파일을 압축하여 예약메일 내년 1월 1일로 발송 설정하고 발송

관리도 Or 추세도 이상

이상징후 알람

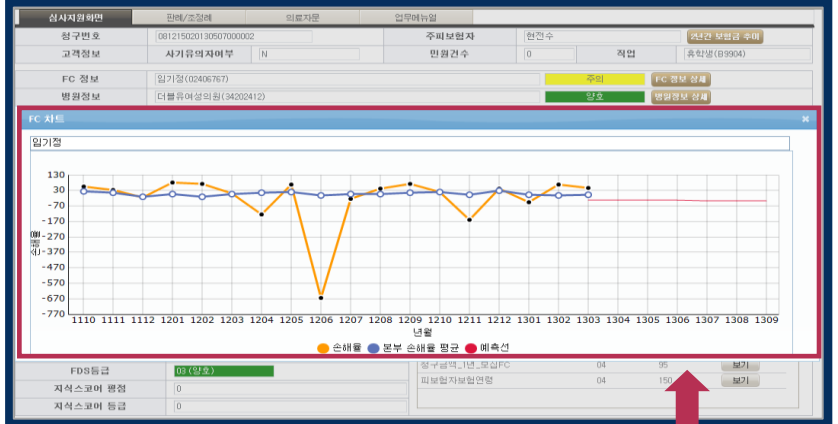
시나리오에 따른 Alarm List 생성

혐의그룹	메시지 분류	민감도
발신자 : OOO, 수신자 : XXX	대외비	0.92
발신자 : OOO, 수신자 : XXX	대외비	0.84
발신자 : OOO, 수신자 : XXX	업무성	0.55
발신자 : OOO, 수신자 : XXX	업무성	0.52
발신자 : OOO, 수신자 : XXX	개인	0.33

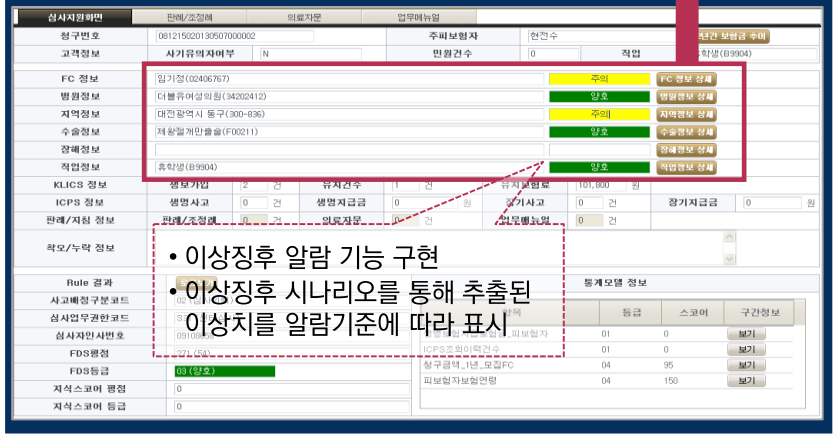
개별 유출 위험도 적용

주의	3.0 시그마 이상	0.5 이상
경계	3.5 시그마 이상	0.7 이상
심각	4 시그마 이상	0.9 이상

이상징후 알람 및 상세정보 표시



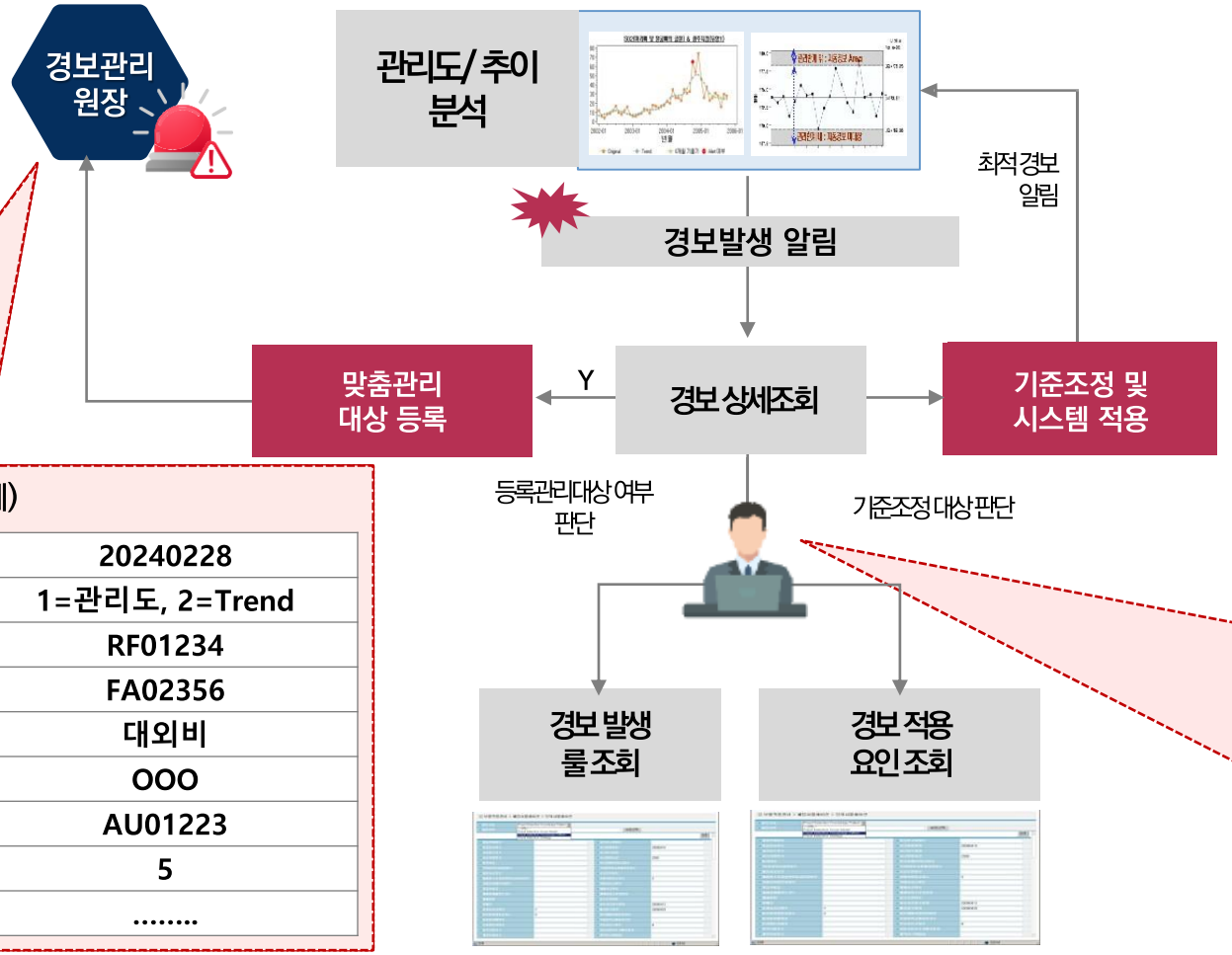
- 이상징후에 대한 상세 정보를 확인하기 위해 필요 Factor 선택 시 상세 정보 확인



- 이상징후 알람 기능 구현
- 이상징후 시나리오를 통해 추출된 이상치를 알람기준에 따라 표시

07 시나리오 기반 이상 징후 탐지

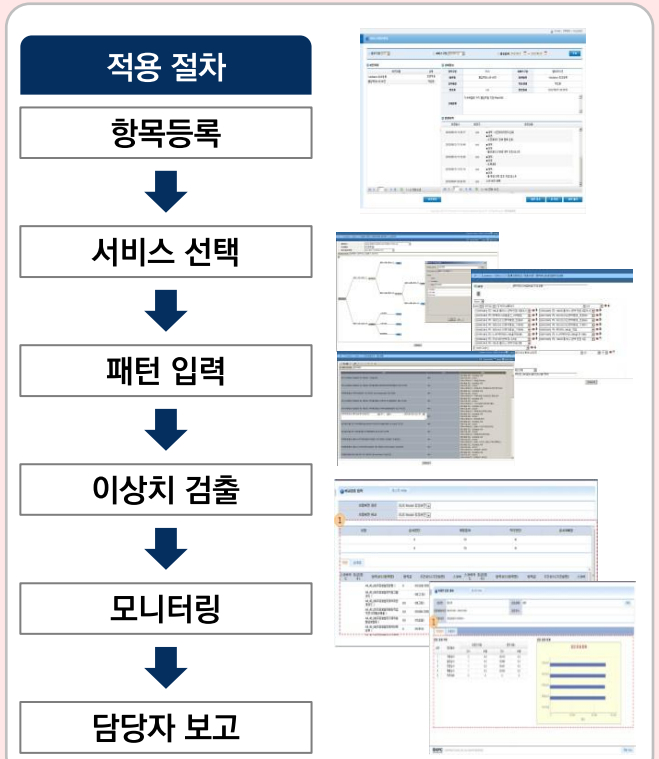
이상 징후 탐지를 위한 경보 관리원장 운영 및 기준 조정과 맞춤관리 대상등록을 통해 패턴을 도출 및 관리할 수 있고 이상징후 발생 시 담당자에게 자동으로 알람을 발송합니다.



- 맞춤관리 대상 등록(예)

경보일자	20240228
경보유형	1=관리도, 2=Trend
경보룰ID	RF01234
경보 팩터	FA02356
확인 결과	대외비
발신자명	OOO
사고번호	AU01223
위험등급	5
.....	.....

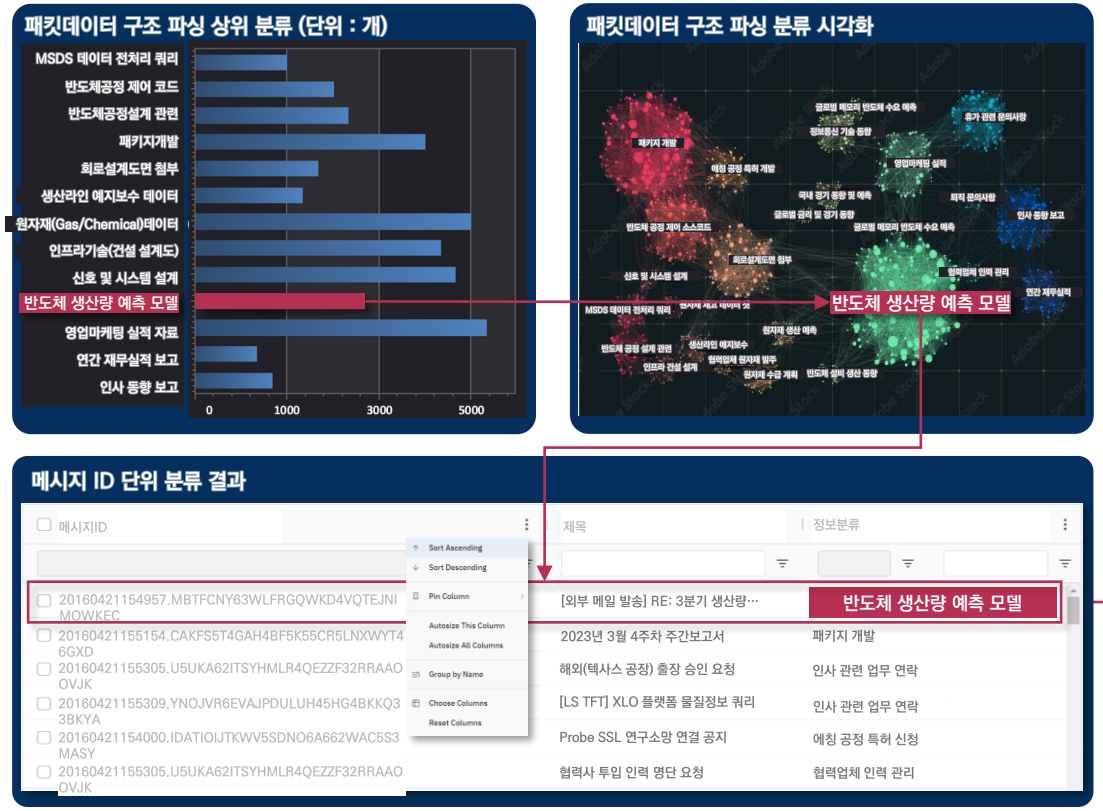
- 이상징후 대상 결과 및 분석 결과를 통한 패턴을 도출/적용 관리
- 이상징후 발생시 담당자에게 주기적으로 보고(자동 알림)



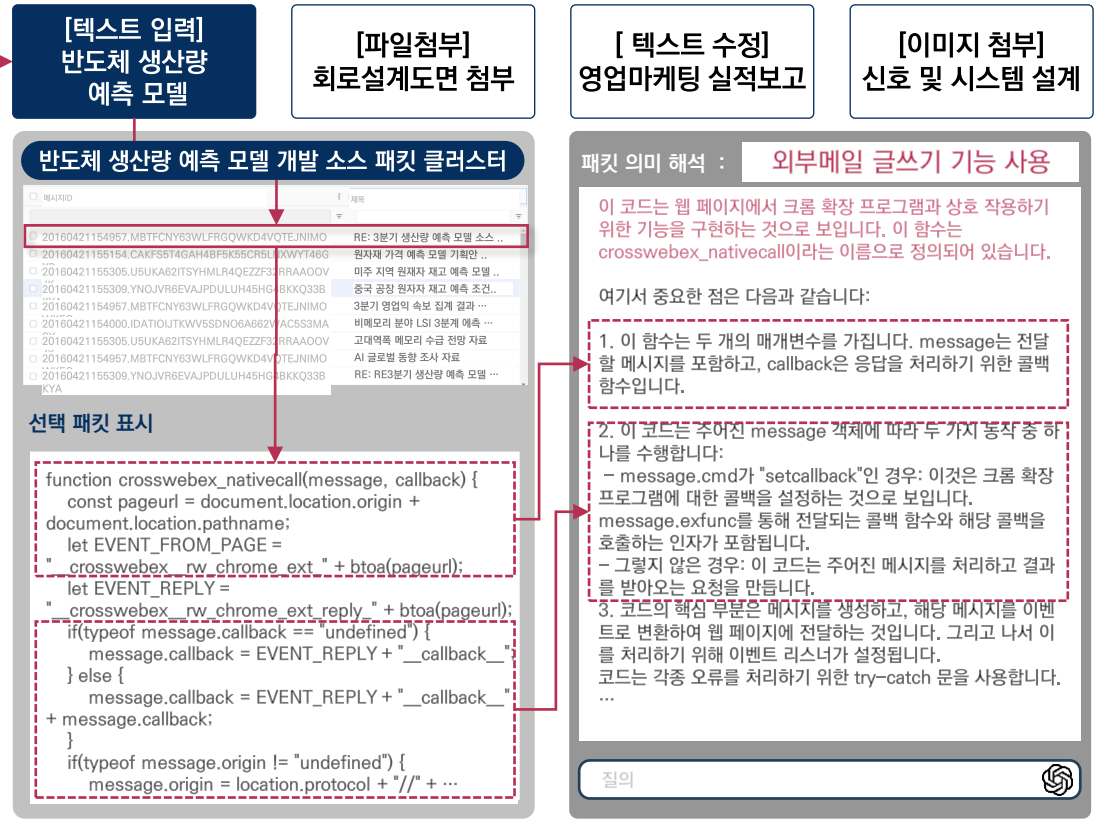
08 미분류 데이터 의미 해석

패킷데이터 구조 파싱 기반으로 미분류 데이터를 클러스터링 합니다. LLM을 사용한 미분류 패킷 데이터 의미 해석 서비스를 제공하고 사용자가 질의를 통해 의미 해석을 구체화할 수 있도록 지원합니다.

미분류 데이터 클러스터링



미분류 데이터 해석 서비스



08 미분류 데이터 최소화를 통한 분석 범위 확장

사전 정의된 구조 기반 클러스터링을 통해 패킷에 분류를 부여합니다. 기분류 패킷과 미분류 패킷의 임베딩 유사성 검색을 통해 일정수준 이상 유사성 이상 라벨링 벡터과 가장 유사한 미분류 패킷에 해당 분류를 부여합니다.

패킷 정보

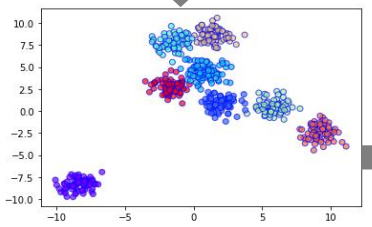
…kr3.samsung.net/mail/rest/v1/mails/read?folderID=2&mailSeq=23914&style=true&form=list&reduceTitlePrefixType=CONTINUOUS…

ANTLR Parser Generator

사전 정의된 패킷 구조 정보

오분류 · 미분류 구조 추가

패킷데이터 파싱 결과 클러스터링



패킷 데이터 구조(Abstract Syntax Tree) 파싱 결과

❶ GlobalScope
symbols = [x, y, a, b]

❷ FunctionSymbol
name = "a"
symbols = []

❸ LocalScope
symbols = [x]

❹ LocalScope
symbols = [y]

❺ FunctionSymbol
name = "b"
symbols = [z]

❻ LocalScope
symbols = []

파싱 패킷 데이터 라벨링 정보

라벨링 파싱 패킷 데이터 임베딩

라벨링 패킷 데이터	임베딩						
1. 대외비 : 개발 코드	0.6	0.9	0.1	0.4	−0.7	−0.3	−0.2
2. 일반 : 사적 여행 정보	0.5	0.8	−0.1	0.2	−0.6	−0.5	−0.1
3. 업무 : 출입승인 요청	0.7	−0.1	0.4	0.3	−0.4	−0.1	−0.3
4. 업무 : 사업계획서 승인	−0.8	−0.4	−0.5	0.1	−0.9	0.3	0.8

유사성 검색 → 유사 의미 코드

라벨링 패킷 데이터	임베딩						
1. 텍스트 입력	0.6	−0.2	0.8	0.9	−0.1	−0.9	−0.7
2. 파일 첨부	0.7	0.3	0.9	−0.7	0.1	−0.5	−0.4
3. 받는 사람 지정	0.5	−0.4	0.7	0.8	0.9	−0.7	−0.6
4. 외부 서비스 접속	0.8	−0.1	0.8	−0.9	0.8	−0.5	−0.9

유사성 검색 → 파일 첨부 동작

미분류 패킷 데이터

벡터 기반 『개발코드』 유사성 검색

-0.1345	0.4309	-0.4449	-0.9373	-0.7451	-0.7896
-0.3206	0.827	0.9597	0.531	0.8922	-0.7498
-0.7746	-0.2094	0.9845	0.3102	0.222	0.4571
-0.792	0.8161	-0.0699	-0.9747	0.6475	0.6098
-0.0239	-0.2011	-0.0158	0.8175	0.9314	-0.0475
-0.9637	-0.157	-0.7026	-0.2104	-0.493	-0.1543
-0.6619	0.05	-0.3819	0.3724	-0.8769	0.2528
-0.3071	-0.4611	0.7577	-0.766	-0.9066	0.2564

벡터 기반 『파일첨부』 유사성 검색

0.7442	0.3967	-0.8062	-0.4207	-0.3519	-0.3605
0.9863	-0.0222	-0.5552	-0.1508	0.4029	-0.3038
0.666	0.2314	-0.2159	0.4779	-0.4028	-0.9953
-0.9264	-0.7497	0.8007	-0.1029	-0.6804	0.2332
0.8809	-0.433	0.9178	-0.7938	-0.2062	-0.4352
0.3674	0.8398	0.0748	-0.2974	0.0074	-0.4981
0.896	0.6811	-0.0143	-0.8229	-0.6632	0.4546
0.0089	-0.0471	-0.9631	0.9462	-0.1989	-0.7988

내용	개발 코드 작성	동작	파일 첨부	미분류 데이터 최소화

사용자 행위 이해

[사용자 단위 정보 유출 탐지]

최종 사용자 행위를
종합적으로 분석하여
사용자 단위 위험 가능성을 탐지하여
정보 유출 위험을
사전에 대비합니다.

01 사용자 행동 종합분석

시계열 반영 사용자 행동 분석을 통해 비정상적인 사용자 행동 패턴을 발견하고, 잠재적인 정보유출을 조기에 감지하여 추가적인 피해를 방지합니다.

사용자 단위 종합 메시지 분석

✔ 메시지 단위 횡단면(Cross-Sectional) 분석

기존 EMASS 메시지 분석 프레임

▪ **금일 수집** 메시지
- **금일 수집**된 데이터 정보가 읽지 않은 ..

▪ 개인정보 메시지
- **금일 수집**된 데이터 정보 중, 개인정보...

▪ 예약어 메시지
- **금일 수집**된 데이터 정보 중, 사전에 등록..

▪ 사용자 조건 필터
- **금일 수집**된 데이터 정보 중, 운용자가 ..

[기존]
이메일 본문 내용 텍스트

[신규]
이메일 첨부 파일 추출 데이터

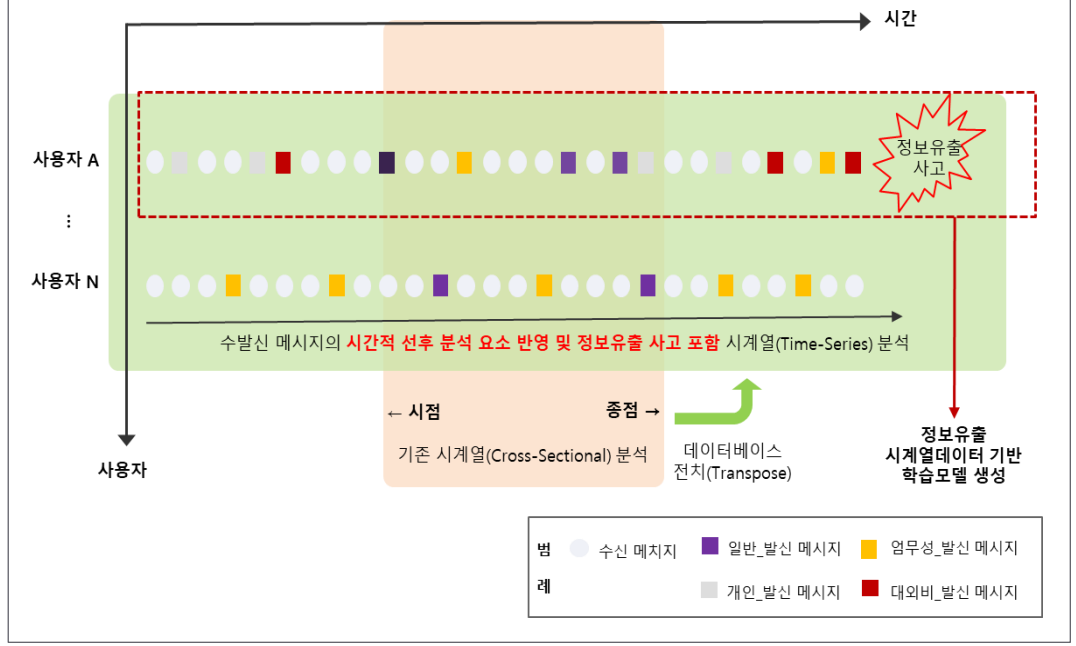
[신규]
웹 서비스 사용 패킷 분석
(기존 미분류 웹서비스 포함)

[신규]
사용자 네트워크 분석 → 혐의점수

시계열 반영 사용자 행동 분석

✔ 사용자 단위 종단면(Time-Series) 분석

사용자 단위 시계열 데이터 기반 정보유출 학습모델 생성 개요

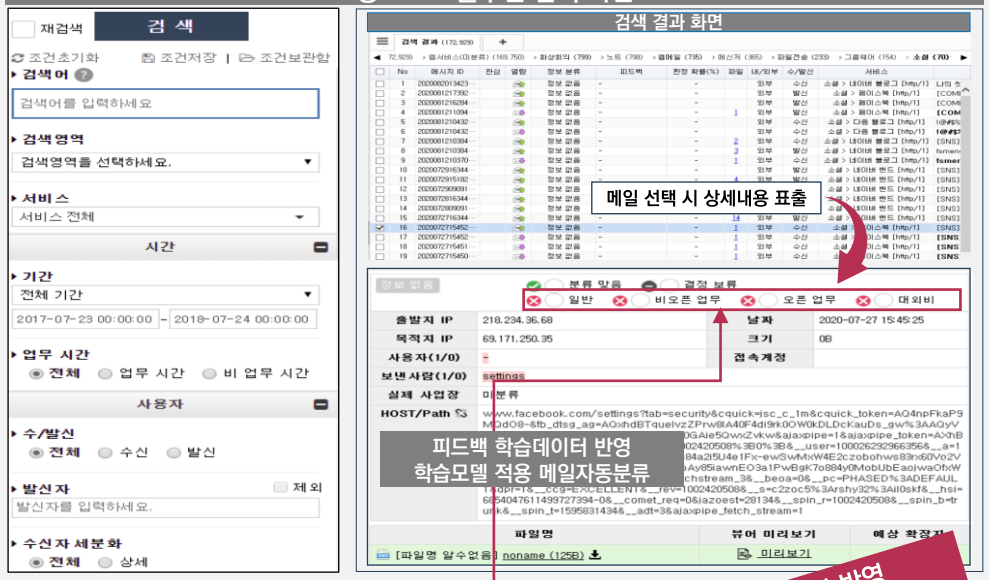


01 사용자 행동 종합분석

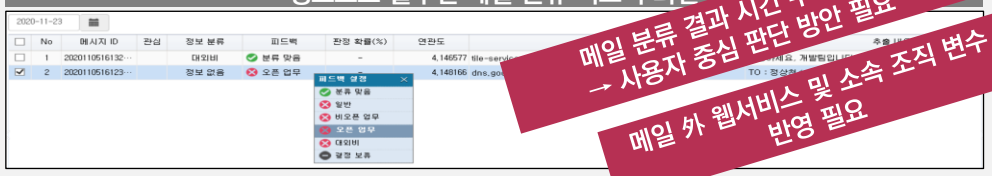
시간의 흐름에 따른 이메일 본문, 첨부파일, 웹서비스를 종합적으로 반영한 종단면 분석으로 전환을 통해 사용자 단위 정보유출 가능성을 탐색합니다.

AS-IS 메일 단위로 머신러닝 분류를 적용하는 개별 메일 중심 분석

정보보호 솔루션 검색 화면



정보보호 솔루션 메일 분류 피드백 화면

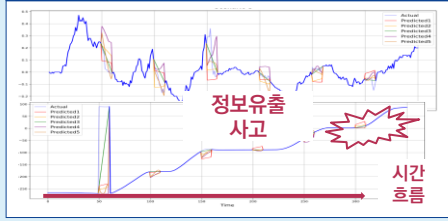


메일 분류 결과 시간 누적 반영
→ 사용자 중심 판단 방안 필요

메일 外 웹서비스 및 소속 조직 변수 반영 필요

TO-BE 메일, 웹서비스, 소속 조직 변수 시간누적적으로 반영 → 사용자 중심 분석

메일 본문 · 첨부파일 내용 시계열 분석

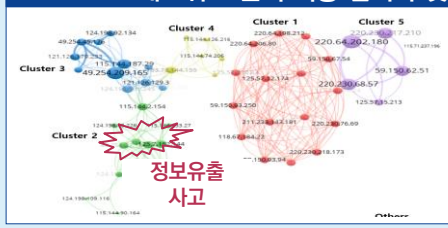


- 메일 본문 내용 분석 (기존)
- 메일 첨부파일 추출 (신규)
- 사용자 시계열 데이터 기반 혐의 점수 부여

웹서비스 사용 패킷 분석

- 웹서비스 별 『서비스-동작-패킷 맵』 구성
- 사용자 단위 패킷 조합 의도 추론

네트워크 분석 적용 혐의자 및 혐의그룹 도출



- 정보유출 사고자와 네트워크 거리 기반
- 정보유출 가능성 계산
- 조직 구조 반영 혐의 점수 부여

사용자 과거이력 반영
정보유출 혐의점수

시계열 데이터 (종단면) 적용
통해 사용자 중심→ 종합 분석
통해 혐의점수

과거 행위 데이터를 포함한
사용자 단위로 분석 가능

메일 내용, 첨부파일,
사용 생성형 AI 내용,
소속 조직(집단) 혐의 점수 반영
→ 종합적 판단 가능

조직 구조 반영
정보유출 혐의 점수

EMASS AI All companies 1 Apr – 1 May Client

사용자와 연결된 패킷 및 콘텐츠 단위 AI 분석을 통해 해당 사용자 단위의 위험도 평가 및 예측이 가능합니다.

Scam
Counterfeit
Tools
Settings
Graph

General risk score
75%

Logo usage risk score
82%

Domain risk score
60%

Registrar info

Registrar
domain.com

Registrar email
r01@domain.com

Registrar phone number
+00 (123) 456 78 00

Registrant organisation
Not indicated

Registrant person
Private person

Registration date
1 Dec 2010

Expiration date
1 Dec 2021

Hosting info

Hosting provider name
Provider

Hosting provider phone number
+00 (123) 456 78 00

Hosting provider email
valuehost@domain

Vpbank
EU

IP address
217.123.42.77

Admin info

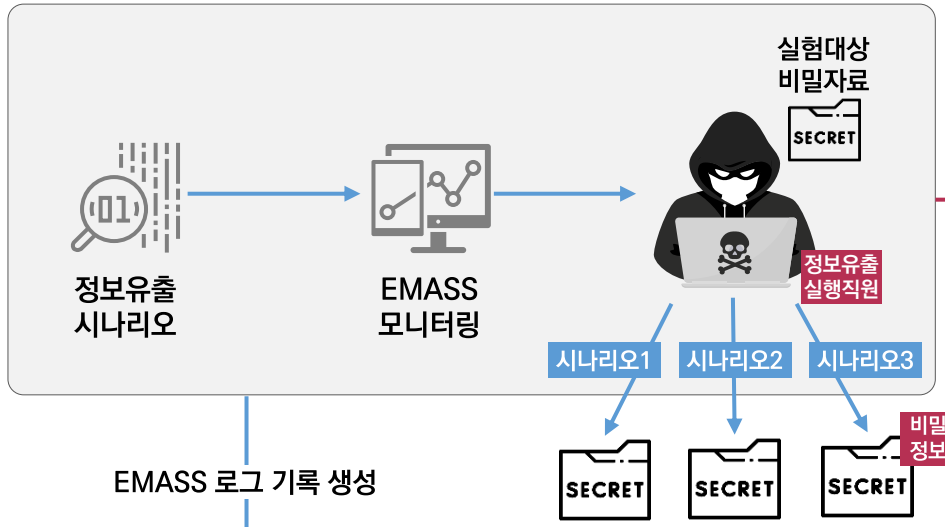
Admin phone number
+00 (123) 456 78 00

IP address
217.123.42.77

Admin email
example@gmail.com

02 사용자 의도 파악을 위한 패킷 분석

각 서비스별 '서비스-동작-패킷 맵'을 구성하여 EMASS 패킷 검색 결과와 비교를 통해 누락된 정보를 확인하고 세부행위별로 정보유출 의도를 파악합니다.



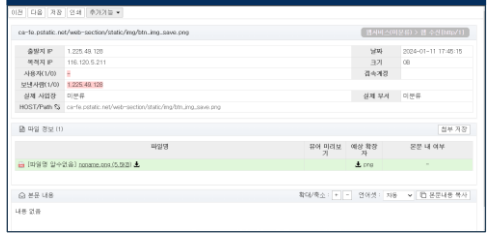
정보유출시 단위행위 및 해당 패킷 정보

웹서비스 : 동작 – 패킷 정보 기록

동작구분	구분	Name	Status	Type	Initiator	Size	Time
글쓰기	Doc	postwrite	200	document	VM228 LayoutBottomCommon-165671165 https .js:1	5.2 kB	132 ms
글쓰기	JS	common.js	200	script	VM451 js:140	(disk cache)	2 ms
글쓰기	JS	util.js	200	script	VM451 js:140	(disk cache)	2 ms
글쓰기	JS	bootstrap.f0c1e432ccc40d32a962.js	200	script	postwrite:2	(disk cache)	1 ms
글쓰기	JS	react.1535fb943a1015ce41f2.js	200	script	postwrite:2	(disk cache)	2 ms
글쓰기	JS	vendor.2f37b2be31bcf76e836e.js	200	script	postwrite:2	(disk cache)	19 ms
글쓰기	JS	main.26c1b1f089e2311aebe2.js	200	script	postwrite:2	(disk cache)	7 ms
글쓰기	JS	se-launcher.js?v=1.51.0-20231124173559	200	script	vendor.2f37b2b….js:2	(disk cache)	1 ms
글쓰기	JS	se-15.js?t=1700814959432	200	script	se-launcher.js?v=1.51.0-20231124173559:6	(disk cache)	0 ms
글쓰기	JS	se-74.js?t=1700814959432	200	script	se-launcher.js?v=1.51.0-20231124173559:6	(disk cache)	2 ms
…	…	…	…	…	…	…	…

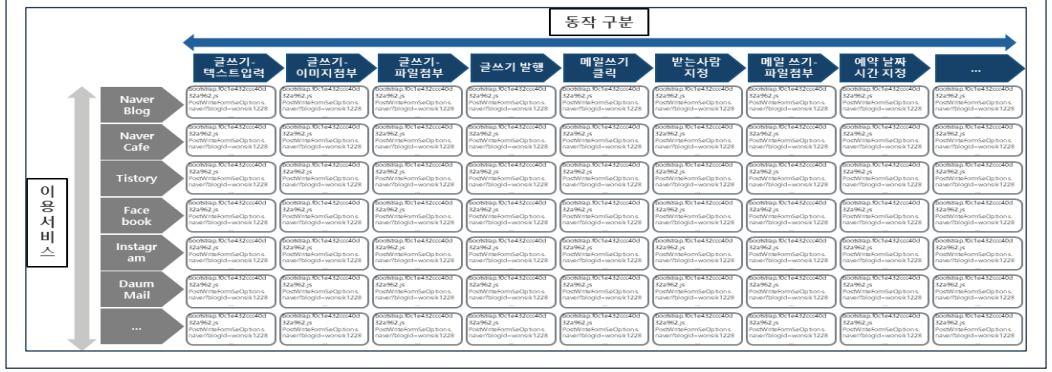
EMASS 로그 기록 생성

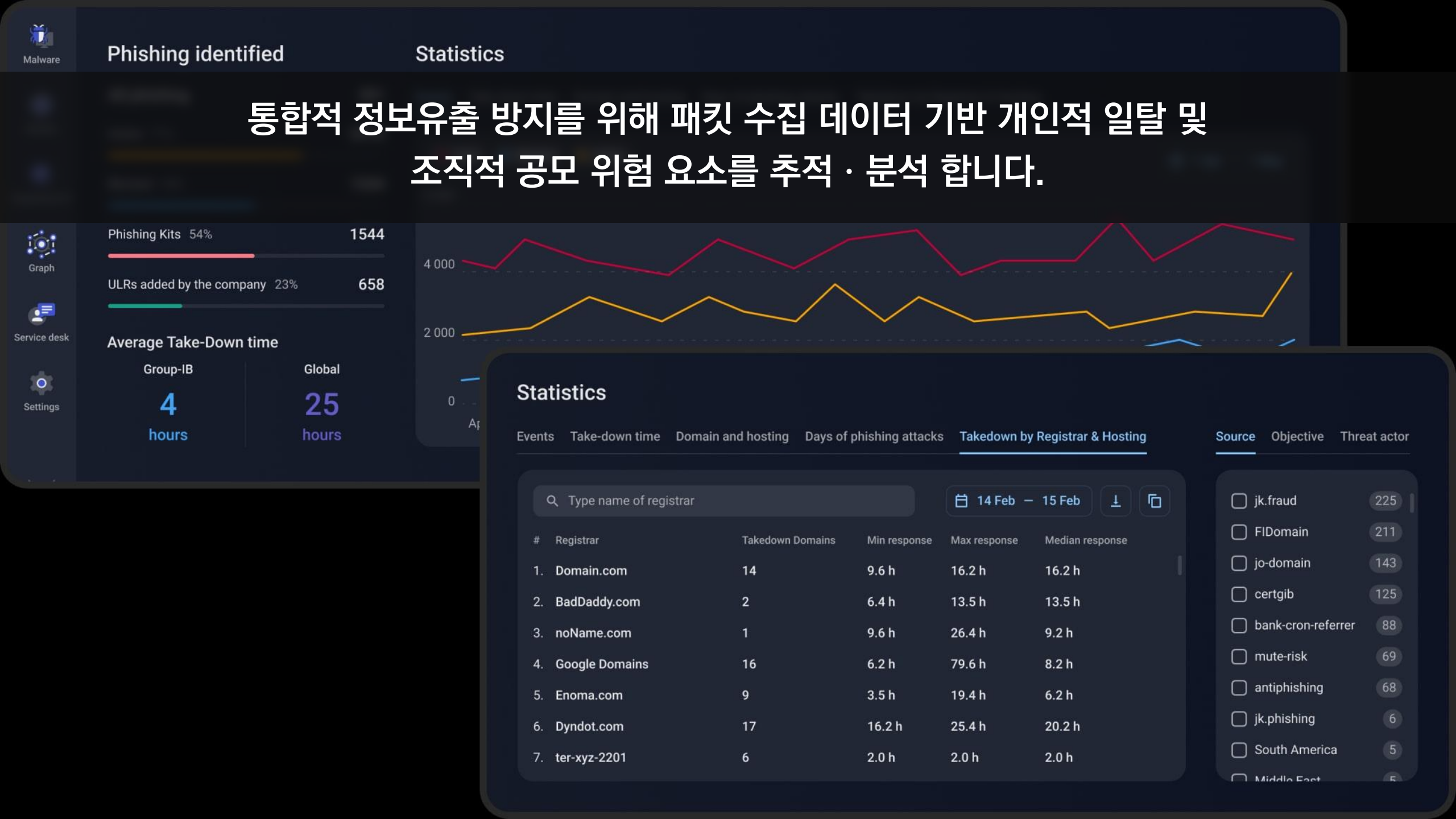
EMASS AI 검색 서비스



정보 비교
→ 누락정보 인식 · 세부 행위별 구분

서비스-동작-패킷 맵(map)



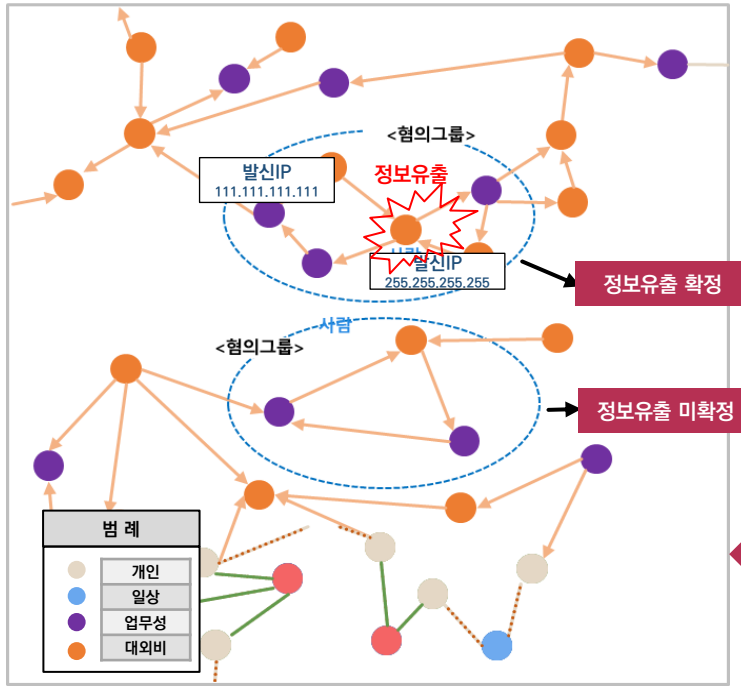

Malware
Phishing identified
Statistics
통합적 정보유출 방지를 위해 패킷 수집 데이터 기반 개인적 일탈 및
조직적 공모 위험 요소를 추적 · 분석 합니다.
Graph
Service desk
Settings
Phishing Kits 54% 1544
ULRs added by the company 23% 658
Average Take-Down time
Group-IB
4
hours
Global
25
hours
4 000
2 000
0
Statistics
Events
Take-down time
Domain and hosting
Days of phishing attacks
Takedown by Registrar & Hosting
Source
Objective
Threat actor
Type name of registrar
14 Feb – 15 Feb
Registrar Takedown Domains Min response Max response Median response
1. Domain.com 14 9.6 h 16.2 h 16.2 h
2. BadDaddy.com 2 6.4 h 13.5 h 13.5 h
3. noName.com 1 9.6 h 26.4 h 9.2 h
4. Google Domains 16 6.2 h 79.6 h 8.2 h
5. Enoma.com 9 3.5 h 19.4 h 6.2 h
6. Dyndot.com 17 16.2 h 25.4 h 20.2 h
7. ter-xyz-2201 6 2.0 h 2.0 h 2.0 h
jk.fraud 225
FIDomain 211
jo-domain 143
certgib 125
bank-cron-referrer 88
mute-risk 69
antiphishing 68
jk.phishing 6
South America 5

03 사용자 행동 네트워크 분석

특정인에게 메시지 수신이 집중되는 경우 메시지 발신자들 간에 연결관계가 존재함을 가정하여 네트워크를 구성하고, 정보유출 사고자와의 연결관계 및 패턴을 기반으로 집단적으로 이루어지는 행위를 반영하여 혐의점수 부여

네트워크 분석 적용 혐의자 및 그룹 도출

사례별 정보유출 결과 학습데이터 구축



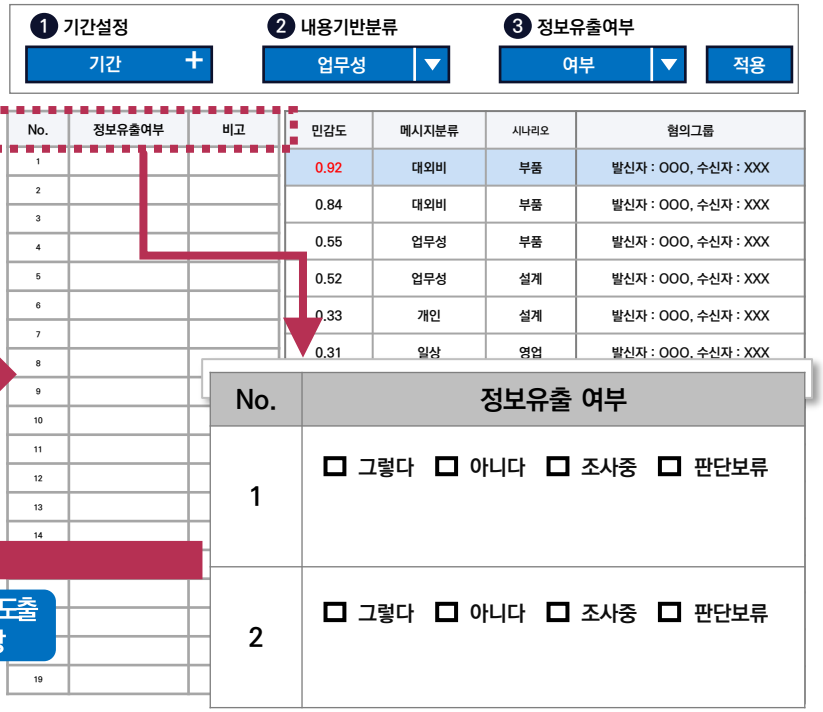
학습 데이터

피드백 데이터

혐의자 및 그룹 도출 정확도 향상

학습데이터 및 모델 구현 → 혐의자 및 그룹 도출

피드백 제공을 통한 성능향상



EMASS AI

Client

사용자 관련정보를 네트워크로 연결하여 사용자 행동 분석을 통해 이상징후를 탐지합니다.

Compromises

Malware

Attacks

Suspicious IP

Graph

Service desk

Settings

Expiry · Domain · Start — End · Domain

Registrar date 13 Dec 2018 · Exp date 3 Feb 2023

Domain name	Registrar
berbank.com	reg-ripn
IP-address	**E-mail**	**Owner**
195.208.0.4 195.208.0.5 +3	card@tours-cin.org	AS56724

Registrar date 25 Oct 2019 · Exp date 22 Feb 2022

Domain name	Registrar
cin.kp	r01-reg-ripn
IP-address	**E-mail**	**Owner**
195.208.0.4 292.168.3.4 +9	admin@pneer.net	AS43783

Registrar date 12 Dec 2019 · Exp date 2 Feb 2022 — Malicious

Domain name	Registrar
neerco.net	reg-ripn
IP-address	**E-mail**	**Owner**
234.221.98.01 234.221.98.03 +3	ad@ci-nema.net	AS4482

Registrar date 5 May 2020 · Exp date 5 May 2023 — Malicious

01 AI OCR을 통한 첨부파일 내용 추출

첨부파일 內 단순 텍스트 내용 및 해당 내용의 위치값, 표, 도형 등 다양한 데이터를 추출하여 모델 분류 정확도를 제고합니다.

정보보호 업무시스템 연계 및 프로세스 처리 기능 제공

다양한 압축 파일 처리

대응 파일 형태 : PPT, EXCEL, HWP/DOC/PDF에 따른 개별적 첨부파일 추출 모델 적용

첨부파일 중 압축파일(ZIP, ALZ 등)이 포함된 경우 자동 압축 해제 및 텍스트 변환

표 형식 텍스트 변환

1

PPT, EXCEL, HWP/DOC/PDF 등 첨부파일 別

각각 개별적인 첨부파일 추출 모델

2

첨부파일 내용 단락, 제목, 내용, 캡션, 표 등 정보 추출

그림(사진) 파일 저장

3

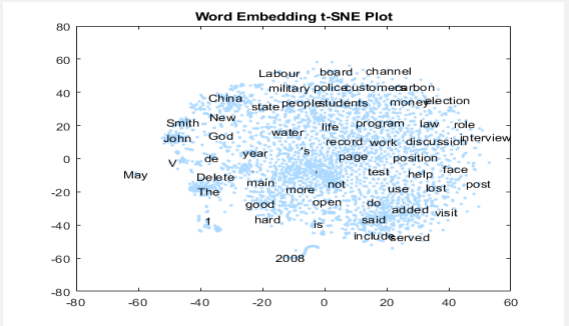
각 정보의 x,y 좌표값 지정 및 파싱

4

KEY	값
이름	홍길동
주소	서울특별시
유형	대외비
연락처	010-0000-0000

신규 DB 구축 및 추출한 문자열 좌표값(x,y) 정보 DB 저장

첨부파일 변환 결과 ML 분류 모델 반영



첨부파일 변환 결과 텍스트 및 다양한 표 형식 벡터화

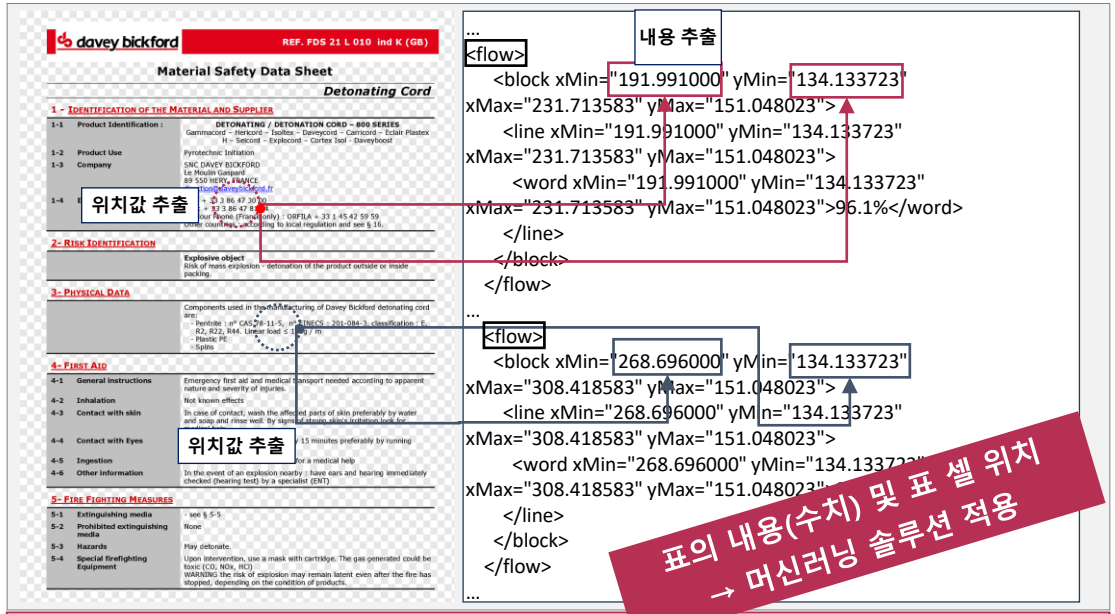
정보보호 ML 분류모델

메일 본문 뿐만 아니라 다양한 첨부파일 텍스트 변환 결과 및 다양한 표 대상 머신러닝 모델 적용을 통한 분류 정확도 제고

01 AI OCR을 통한 첨부파일 내용 추출

이메일 첨부파일 內 텍스트 내용과 해당 텍스트, 도형, 표 등의 위치값을 파악하여 머신러닝 솔루션을 적용하며, 첨부파일을 유형화한 후, 첨부파일 유형에 따라 차별화된 내용추출 기능을 제공합니다.

표 내용 및 표 셀 위치 등 정보를 추출



- 첨부파일 중, 파워포인트(pptx) 파일의 표(table)에 포함되는 내용과 내용이 위치하는 셀 및 내용 위치 표시
- 내용과 위치값을 모두 머신러닝 솔루션에 적용 → 내용 및 위치값 정보로 문서 내용 정확히 재현 가능 → **사람이 표를 보고 판단하는 것과 같은 논리**로 **대외비 여부 판단** 가능

※표 재현 이슈 엑셀과 같은 스프레드 시트 파일(전체 27.7% 차지)에서 결정적

첨부파일 분석 범위

순위	확장자	순위	확장자	순위	확장자	순위	확장자
1	xlsx	18	sql	35	properties	52	tcd
2	jpg	19	wmv	36	xlsb	53	uts
3	null	20	egg	37	tar	54	pptm
4	docx	21	xlsm	38	gul	55	z01
5	pdf	22	mht	39	java	56	psd
6	ko	23	mp4	40	ppt	57	c
7	p7s	24	so	41	eml	58	fsdb
8	xls	25	gif	42	jpeg	59	diff
9	json	26	m4a	43	tif	60	avi
10	pptx	27	dll	44	bmp	61	apk
11	zip	28	7z	45	dxp	62	a00
12	png	29	html	46	dwg	63	pc
13	xml	30	bin	47	f22	64	csv-1512448295175
14	htm	31	log	48	pfx	65	ear
15	doc	32	gz	49	h	66	csv-1512448295180
16	txt	33	123	50	request	67	alz
17	p7m	34	hwp	51	cs	68	3

머신러닝 솔루션 적용 첨부파일 유형

보고서	pdf, hwp, docx, doc	발표문서	pptx, ppt	압축파일	zip, egg, 7z, tar, alz
자료정리	xls, xlsx	데이터파일	json, txt, csv, xml	코드	java, sql

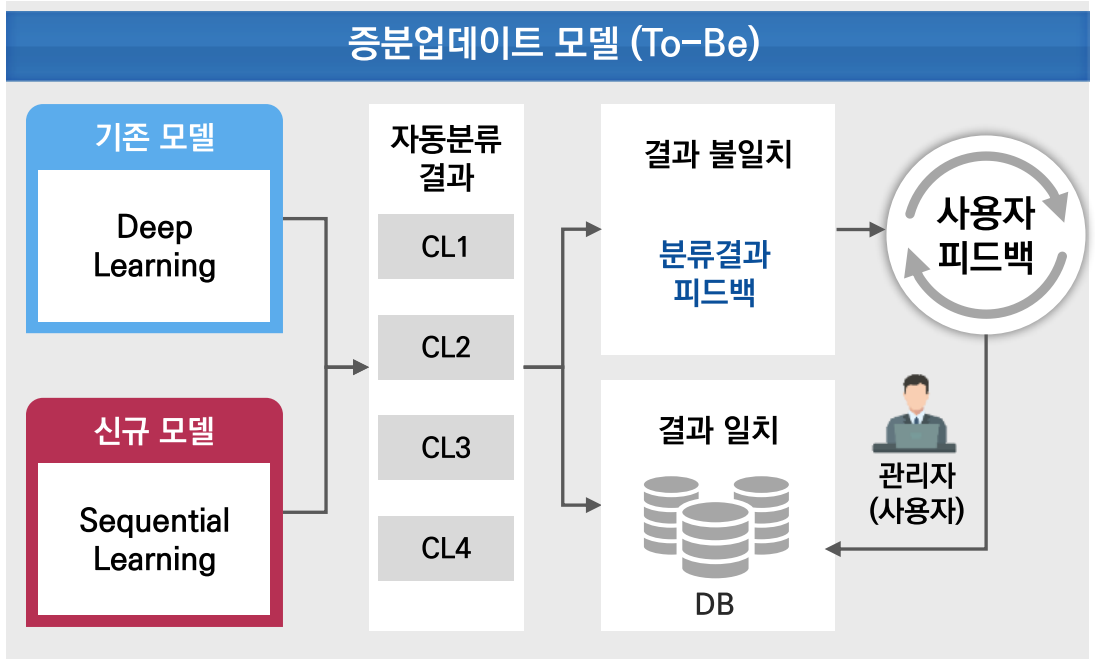
02 EMASS AI 딥러닝 피드백 자동화

EMASS AI 는 콘텐츠 분류 모델의 성능 향상을 위한 효과적 피드백 데이터 구축을 위해 『다중모델 결과 불일치 피드백』 모델과 『다중모델 상호 피드백』 모델을 제안합니다.

다중모델 결과 불일치 피드백

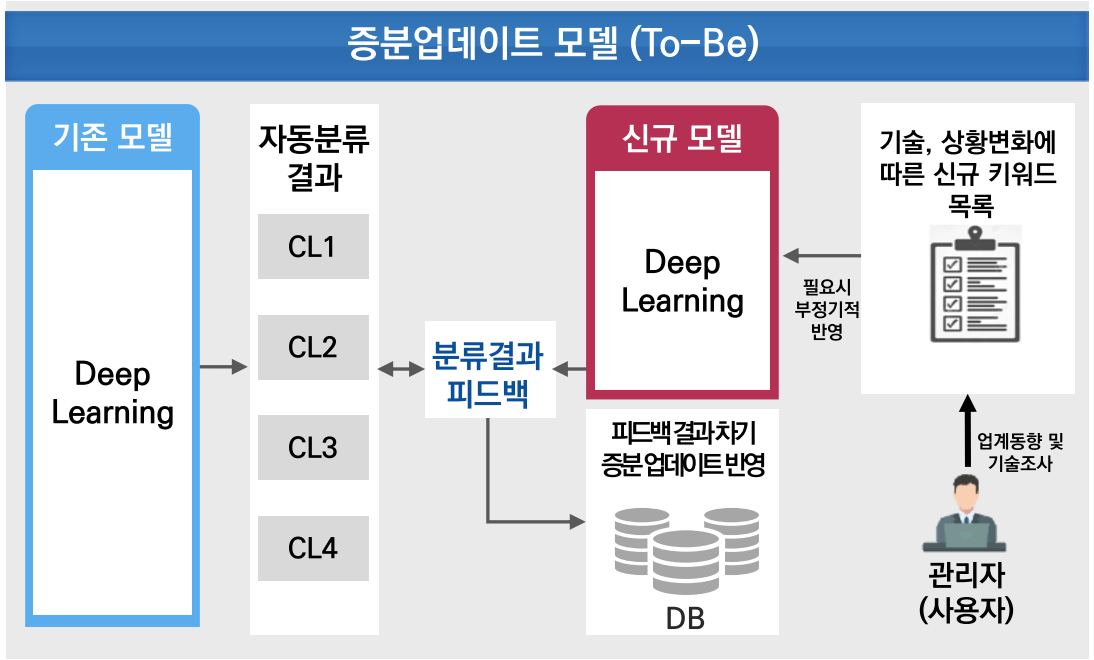
복수의 모델의 일치하는 결과에만 사용자 피드백

→ 사용자 피드백 부담 감소



다중모델 상호 피드백

기존 분류 모델의 결과를 신규 도입 모델이 사용자 대신하여 피드백하여 사용자 개입 최소화



정보유출 주요 관제 지표

[모니터링 대시보드 제공]

주요 관제지표, 이상징후 발생 징후,
실시간 관리현황, 최근 이벤트 상세
정보 제공을 통해
정보유출 모니터링을 실시합니다.

01 정보유출 모니터링 대시보드

주요 관제 지표를 기준으로 이상징후 탐지 추이 및 실시간 관리현황 등 관측 가능한 정보유출 대시보드를 제공합니다.

01 주요 관제 지표

주요 이상징후 관제 지표 신속한 탐지

02 이상징후 탐지 추이

직전 7일 또는 30일간의 이상징후 발생 추이

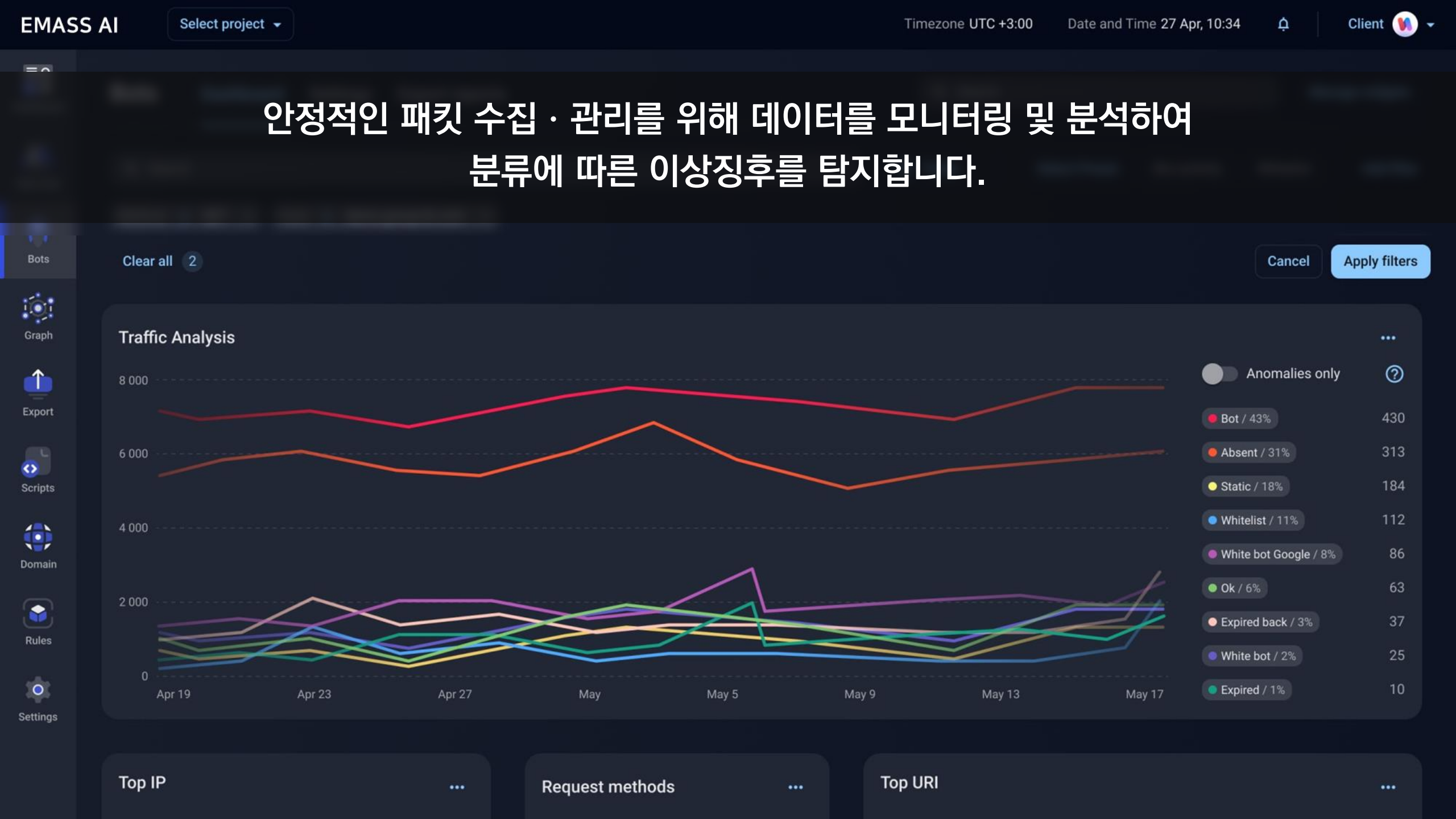
03 실시간 관리 현황

실시간 수집, 탐지 및 대응의 적정성 표시

04 최근 이벤트 상세

최근 탐지된 이벤트 상세 리스트
(시나리오별 이벤트 개수 및 감지 동향)

안정적인 패킷 수집 · 관리를 위해 데이터를 모니터링 및 분석하여
분류에 따른 이상징후를 탐지합니다.



02 정보유출 모니터링을 위해 다양한 시각화 도구 제공

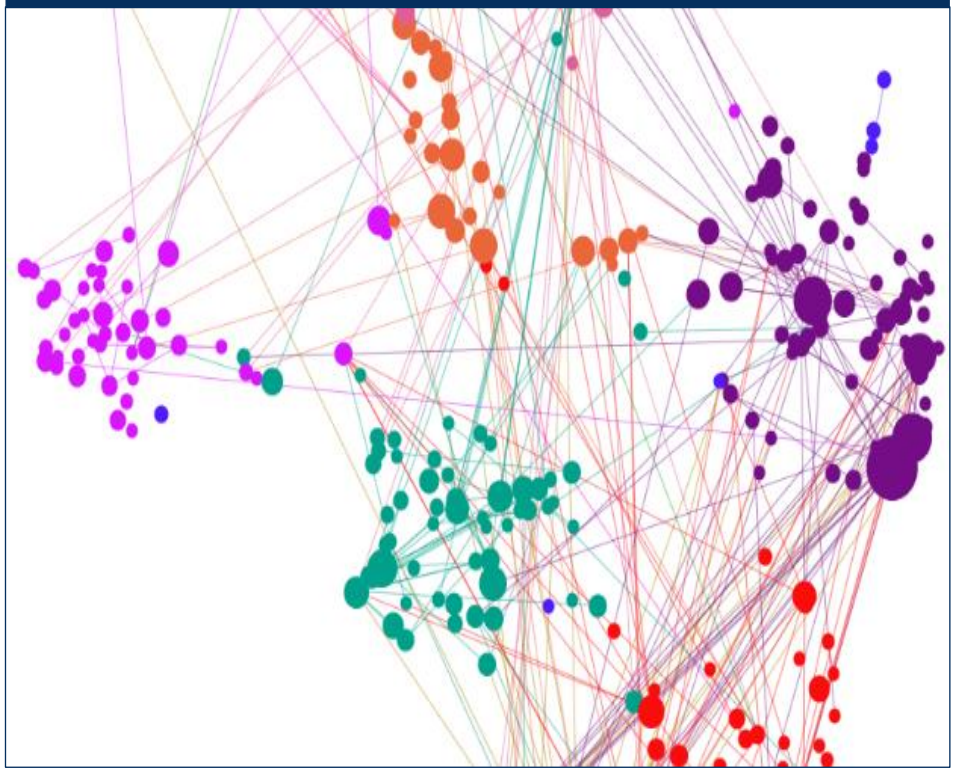
주제별 클러스터 기반의 메일 수발신 네트워크 통해서 정보유출 이상징후 탐색 기능을 제공합니다.

주제 분석을 통한 메일 수발신 네트워크 분석

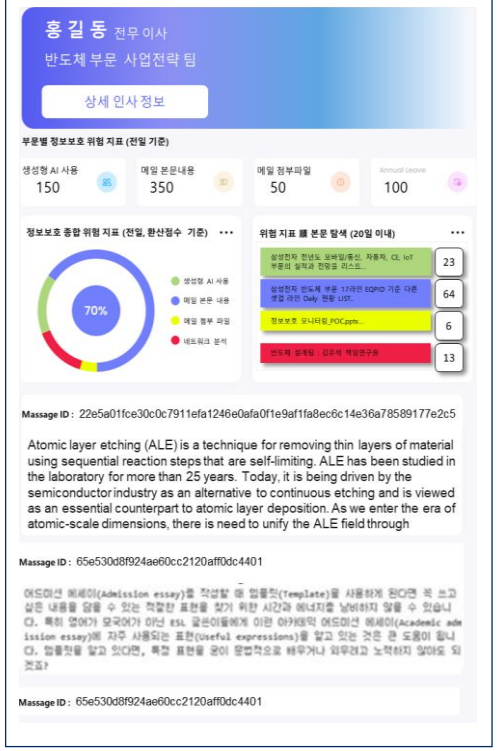
주제 분석(Topic Modeling) 결과

TOPIC	KEYWORDS
Wafer Preparation	Wafer cleaning, polishing, slicing, wafer flat, notch, orientation, surface preparation
Photolithography	Photoresist, photomask, exposure, ultraviolet (UV) light, pattern transfer, reticle, stepper, alignment
Etching	Chemical etching, dry etching, wet etching, plasma etching, photoresist removal, selective etching, isotropic etching
Deposition	Chemical Vapor Deposition (CVD), Physical Vapor Deposition (PVD), atomic layer deposition (ALD), thin film, sputtering, epitaxy.
Lithography	Optical lithography, deep ultraviolet (DUV), extreme ultraviolet (EUV), resolution enhancement techniques (RET), mask aligner.
Ion Implantation	Doping, ion beam, dopant atoms, ionized species, implantation energy, ion dose, annealing.

주제 분석에 따른 메일 수발신 네트워크



특정 네트워크 노드 상세 정보



이메일 정보유출 분석

[이메일 매개 위험 감소]

이메일 메타정보 및
내용 기반의 정보유출 탐지 기술로
우발적 · 의도적 이메일 매개
정보유출 위험을 예방합니다.

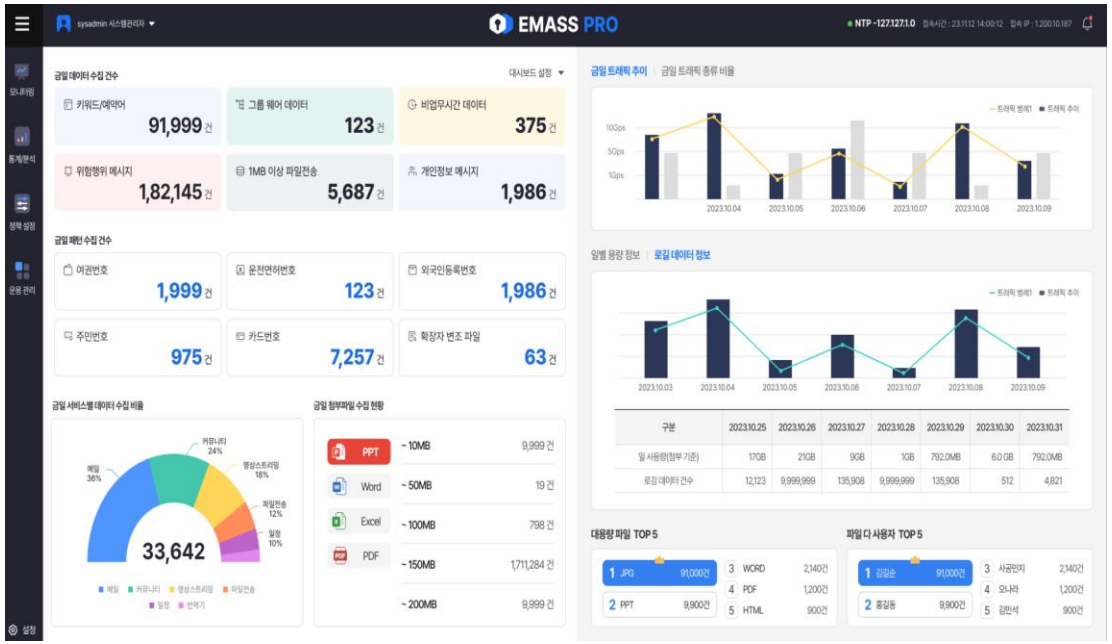
03 정보유출 모니터링을 위한 스코어보드

대외비 분류 등 분류 수준 기준 정보보호 클린지수, 각종 통계 정보를 표출하는 대시보드 및 사용자별 현황을 종합하는 스코어보드 등을 제공합니다.

정보유출 모니터링 종합 대시보드

화면 구성 내용

1. 정보보호 클린지수



사용자별 스코어보드

화면 구성 내용

1. 사용자별 정보보호 위험 지표

XCURENET

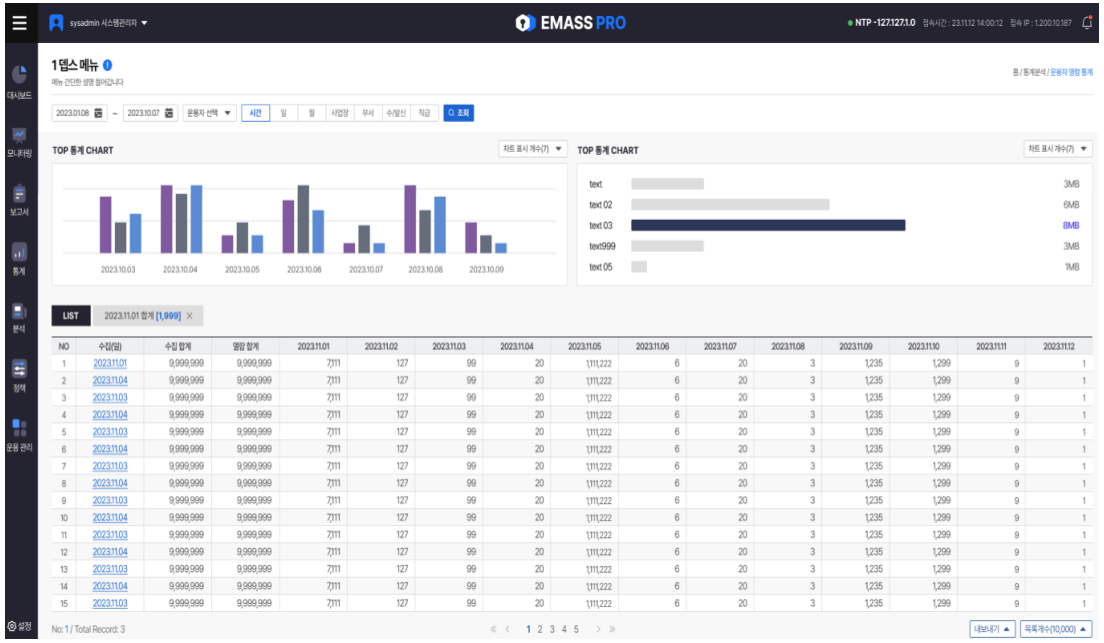
04 이메일 매개 정보 유출 분석 화면

모니터링 대시보드 메인화면, 통계 및 메시지 검색 화면 등 시나리오별 분석 화면을 제공합니다.

통계 분석 화면

화면 구성 내용

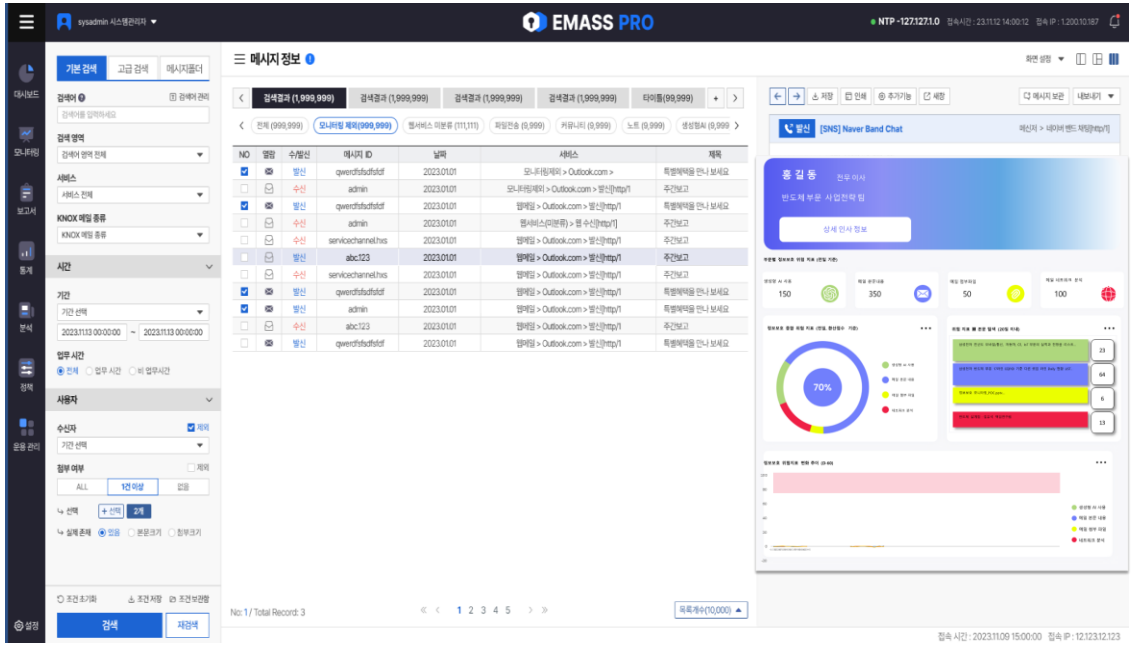
1. 상세 메뉴에서 통계 메뉴 확인 가능



메시지 검색 화면

화면 구성 내용

1. 메시지 검색 기능



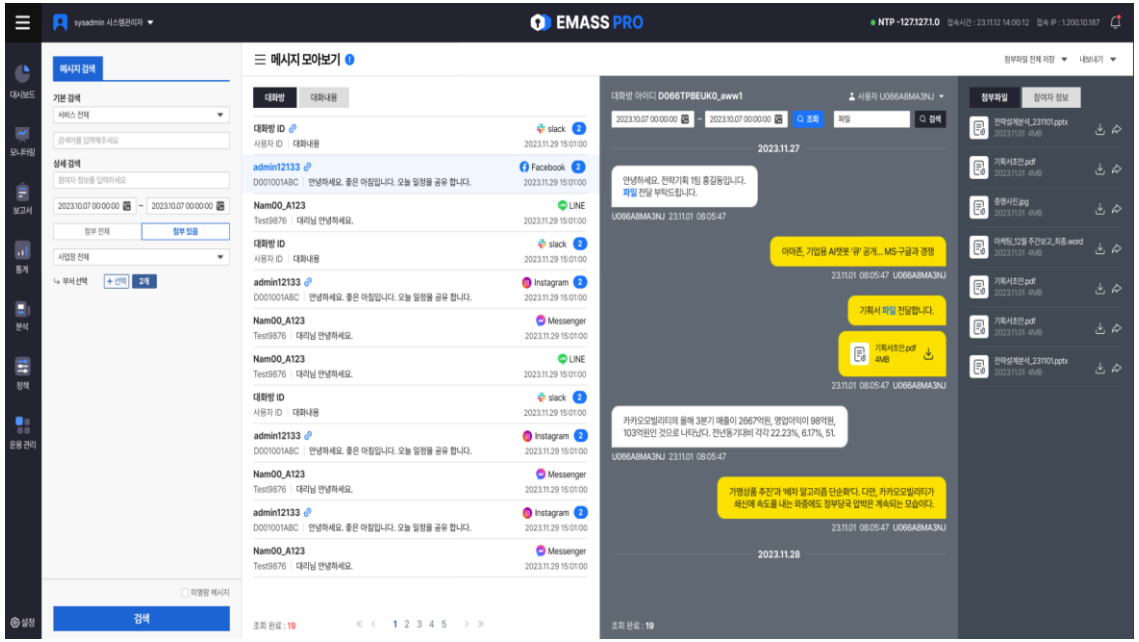
04 이메일 매개 정보 유출 분석 화면

모니터링 대시보드 메인화면, 통계 및 메시지 검색 화면 등 시나리오별 분석 화면을 제공합니다.

메신저 내용 분석

화면 구성 내용

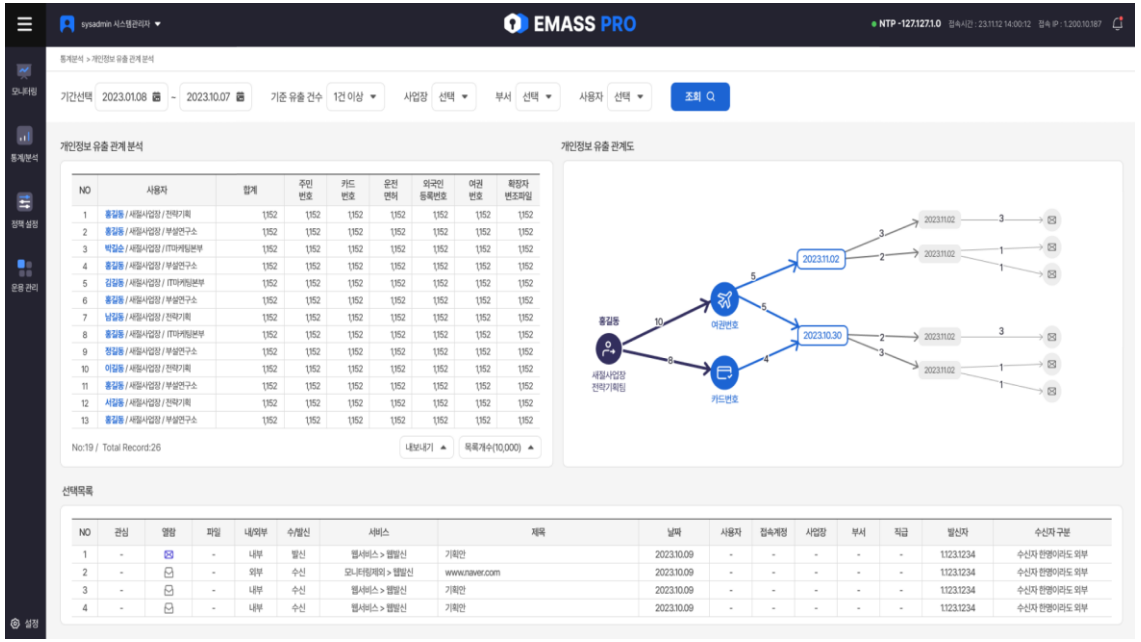
1. 메신저 내용 모아보기, 사용자별 메신저 내용 검색 등



정보유출 관계분석 화면

화면 구성 내용

1. 정보 유출 관계분석, 정보 유출 관계도 등으로 구성



EMASS AI

All projects

Timezone UTC +3:00 Date and Time 27 Apr, 10:34 Client

이메일 단위 수발신 네트워크를 통해 특정 이메일 혹은 연관된 이메일의 위험도를 평가할 수 있습니다.

Bots

Graph

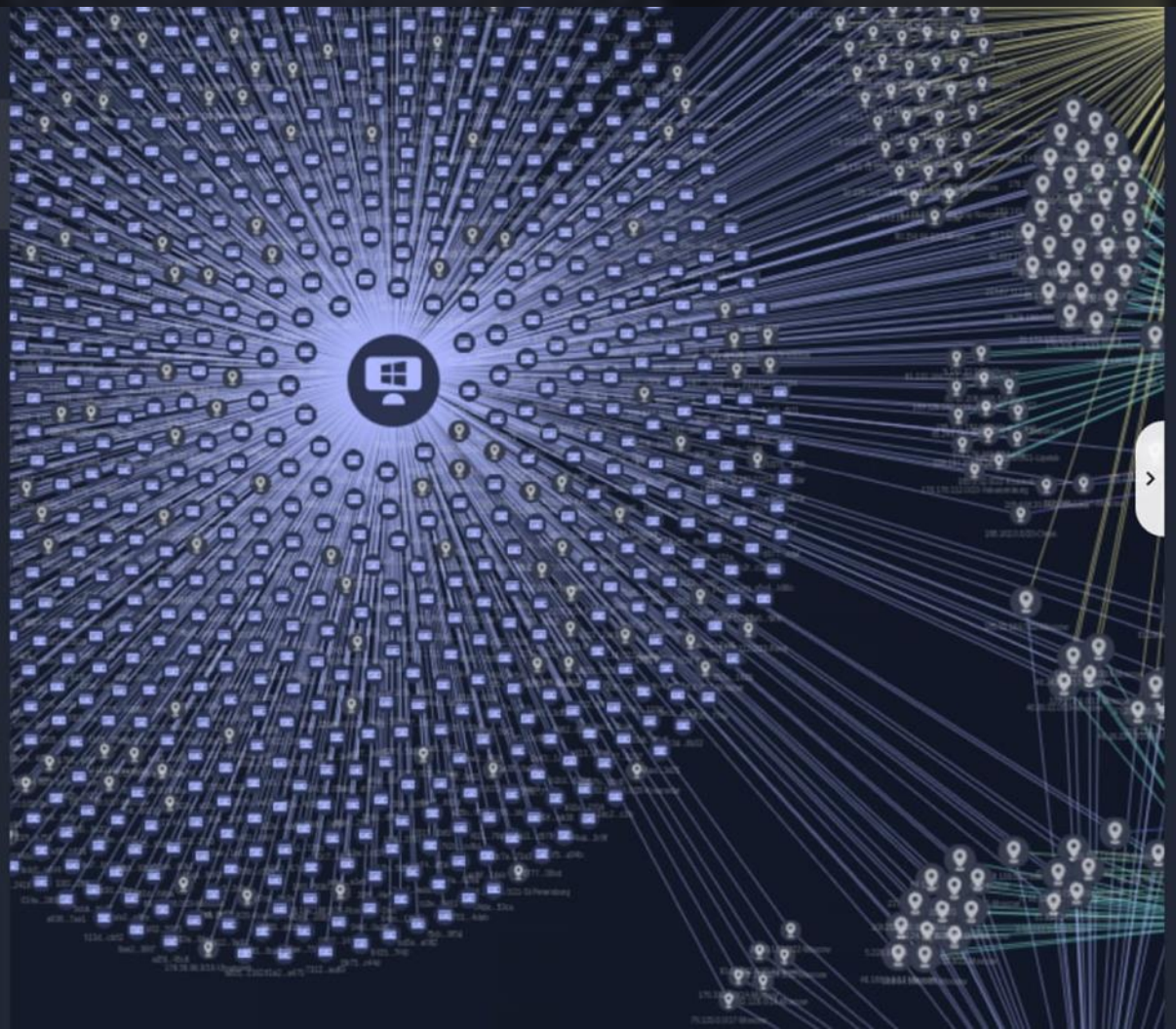
Export

Scripts

Domain

Rules

Settings



Found devices

Information about devices and user sessions from this device.

Unknown Device

7e403498f-394f-ow01-39dd-3490fkfj5708

Score 90

Device info | Identities 1 | IP-Addresses 8 | Browsers 2 | Sessions 2 | Events

Device fingerprint	28397694-7d59-45fd-99e3-e12229a4fkoe
Customers	Blue Hawk
Start Active time	26 Aug 2021, 19:24
End Active time	27 Aug 2021, 12:43
Operating System	Unknown
Platform	Unknown
CPU Cores	4
Channels	Web iOS Android
List	Block list

Device Windows

fbd83498f-394f-ow01-39dd-3490fkfj74bc

Score 25

Device info | Identities 1 | IP-Addresses 8 | Browsers 2 | Sessions 2 | Events

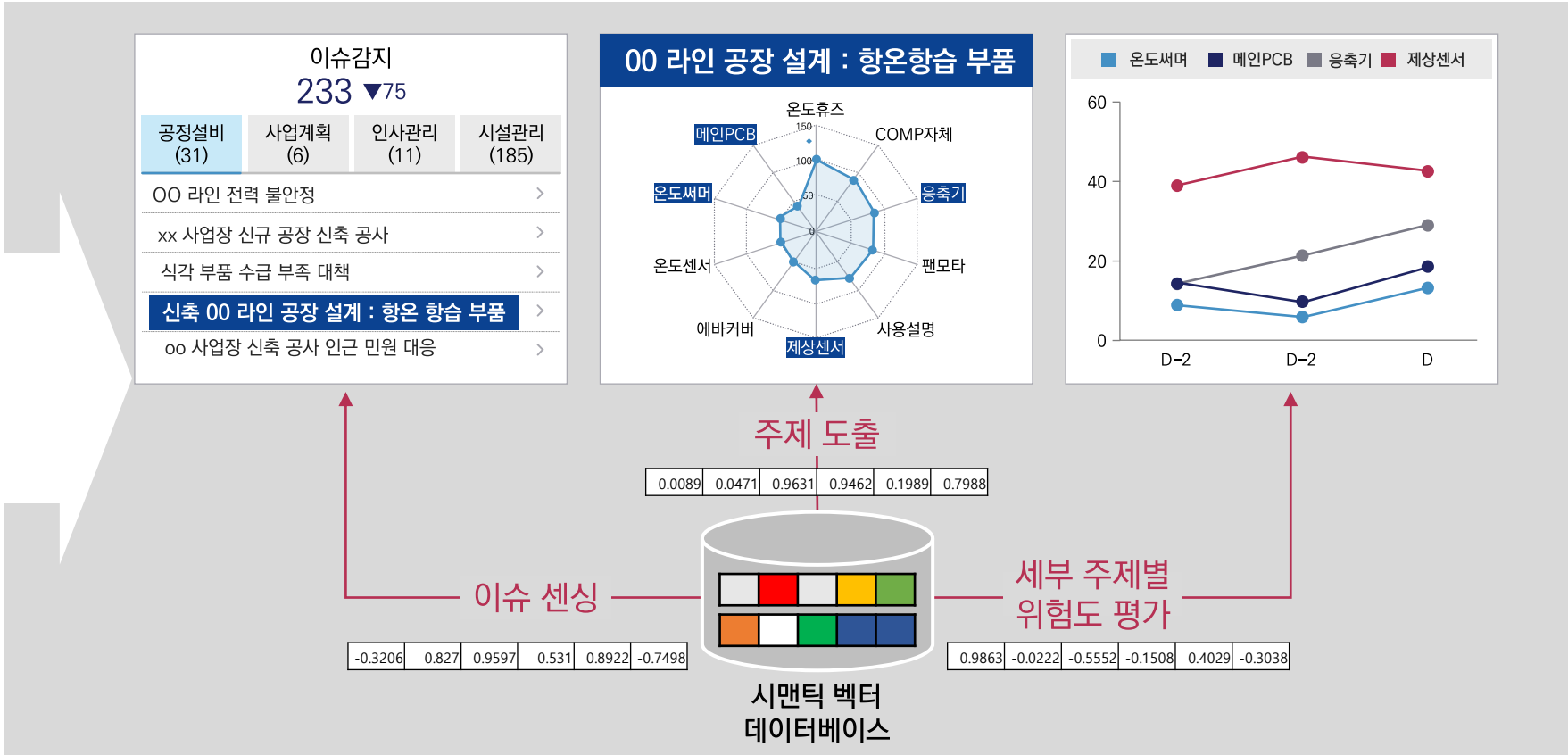
Chapter

V Feasible Cases

01 자연어 이해 기술 : 이슈감지 · 주제분류 · 위험도 평가

EMASS AI는 자연어 이해 기술을 사용하여 대규모 이메일 대상 이슈감지, 주제분류, 세부 주제별 위험도 평가 등이 가능합니다.
사용자는 보다 입체적인 콘텐츠 분석을 통해 위험평가가 가능하고, 정보유출 사고를 방지할 수 있습니다.

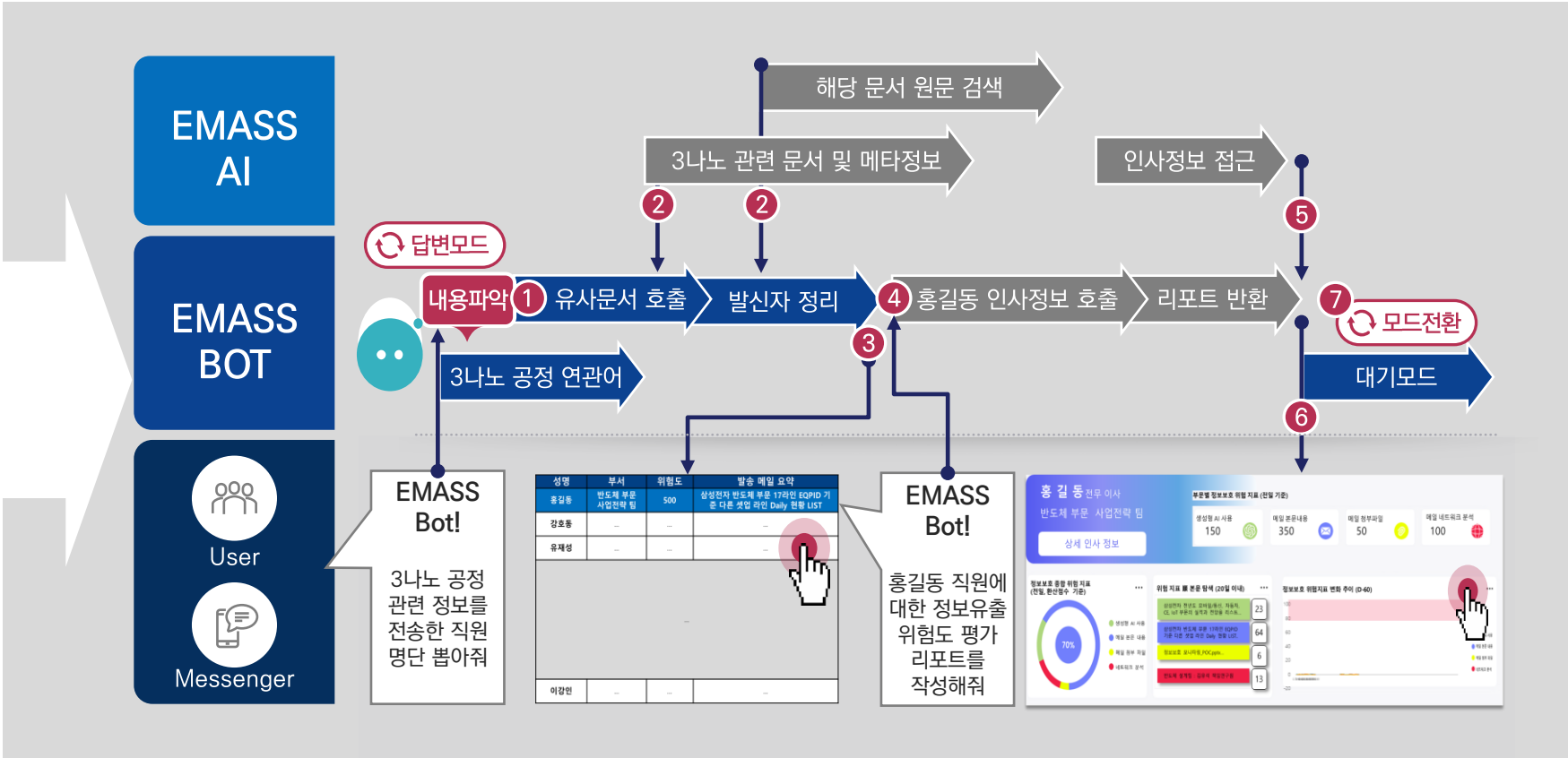
텍스트 요약 (text summarization)	메일 문서 단위 내용 요약 이슈 및 주제 단위 내용 요약
자연어 이해 (Natural-language understanding)	텍스트 자동 분류 · 주제 도출 문서 단위 위험도 수준 반영자동 경보
자연어 생성 (Natural-language generation)	정보 유출 보고서 자동생성 사용자 평가 보고서 자동생성
대화관리 · 질문답변 (Dialogue system)	메일 문서 단위 내용 요약 이슈 및 주제 단위 내용 요약



02 대화관리 · 질문답변 기술 기반 EMASS BOT 서비스

EMASS AI는 대화관리 · 질문답변 기술을 사용하여 분석 결과 데이터를 대화방식으로 제공하는 EMASS BOT 서비스를 제공합니다.
사용자는 대화 기반의 질문 답변을 통해 보다 신속하고 효과적으로 정보유출 관련 데이터를 얻을 수 있습니다.

텍스트 요약 (text summarization)	메일 문서 단위 내용 요약 이슈 및 주제 단위 내용 요약
자연어 이해 (Natural-language understanding)	텍스트 자동 분류 · 주제 도출 문서 단위 위험도 수준 반영자동 경보
자연어 생성 (Natural-language generation)	정보 유출 보고서 자동생성 사용자 평가 보고서 자동생성
대화관리 · 질문답변 (Dialogue system)	메일 문서 단위 내용 요약 이슈 및 주제 단위 내용 요약



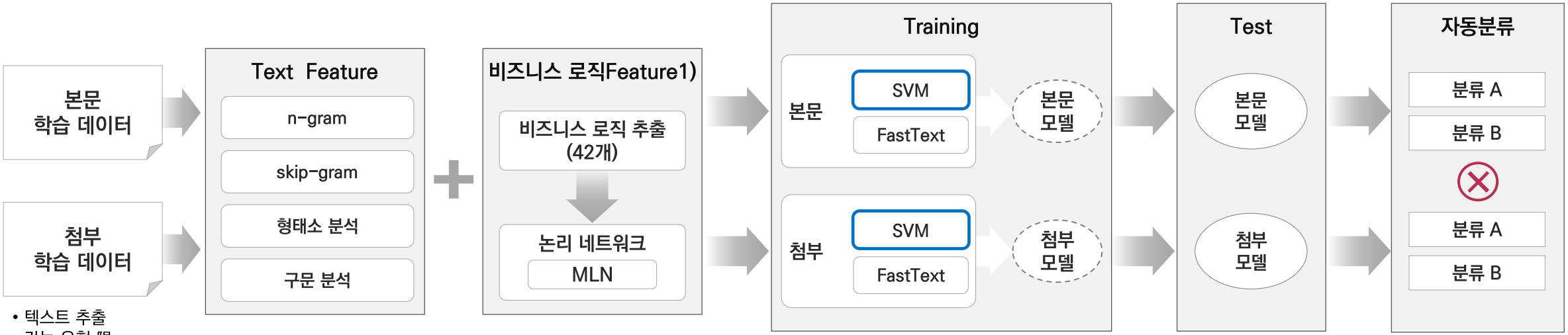
XCURENET

Chapter

VI Use Cases

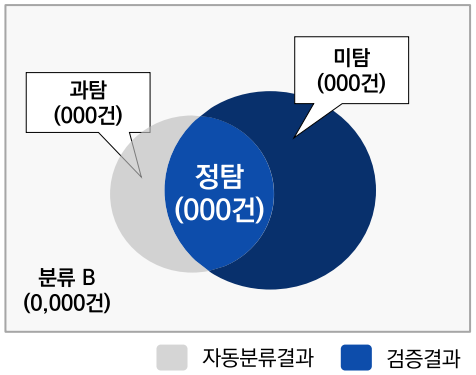
삼성전자/삼성전기 적용 사례

SVM 및 FastText 알고리즘 기반의 정보보호 이슈 문서 자동 분류 모델 개발 후 성능 비교 검증



1) 비즈니스 로직 Feature : 비즈니스 로직을 통계치로 변환하여 Feature로 사용 (특정 Rule에 대한 가중치 부여)

1차 검증 결과

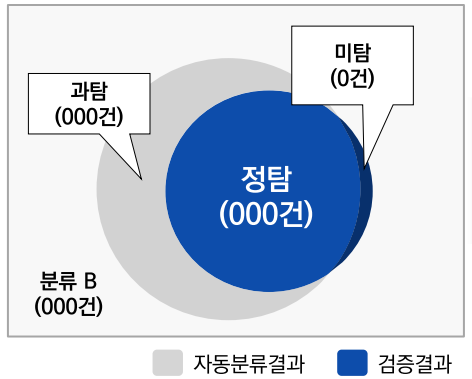


구분		자동분류		합계
		분류 A	분류 B	
검증결과	분류 A	000	000	000
	분류 B	000	0,000	0,000
합계		000	0,000	0,000

- 재현율 = 00% (000건/ 000건)
- 정밀도 = 00% (000건/ 000건)
- F1 Score = 00%

※ 검증결과상 1순위,2순위 분류를 분류 A로 구분

2차 검증 결과



구분		자동분류		합계
		분류 A	분류 B	
검증결과	분류 A	000	0	000
	분류 B	000	000	0,000
합계		0,000	000	0,000

- 재현율 = 00% (000건/ 000건)
- 정밀도 = 00% (000건/ 0,000건)
- F1 Score = 00%

한국인터넷진흥원 스팸데이터 분류 적용 사례

딥러닝 기반의 자동 스팸 여부 판별 시스템을 구현해 한국인터넷진흥원이 접수·수집한 스팸 데이터를 자동으로 스팸과 非스팸으로 분류

Data Source

Source Data

Source System

Training Data (Training Set)

- 머신러닝을 위해 가공된 약 980만여건의 학습 데이터 (spamkind 부착)

Test Data (Validation Set)

- KISA에서 선별한 검증용 데이터 집합

Classification System

전처리 영역

OCR 추출 | 오류건 제어 | EML 추출 | 토큰 분석

- 전처리 지원 엔진 활용
- 실제 시스템 구현에서 활용 가능한 pre built-in 분석 엔진 제공 등 프로젝트 수행을 지원하는 기능 제공

분류 학습 영역 (ML)

Supervised Learning Model | Feature/ Kernel Engineering | Deep Learning

- 실험 환경 구성
  GPU : Quadro RTX A6000 (48GB, '21.12)
  Module : Transformers 4.9.2, Pytorch 1.9.0+cu102, Python 3.7.12
  Parameters : MAX_LEN = 210, BATCH_SIZE= 210, epochs = 4/8/16

	학습 건수	전체 건수	실험1	실험2	실험3
			정확도(%)	정확도(%)	정확도(%)
총계	**6,214	**2,460	97.71	97.51	98.13

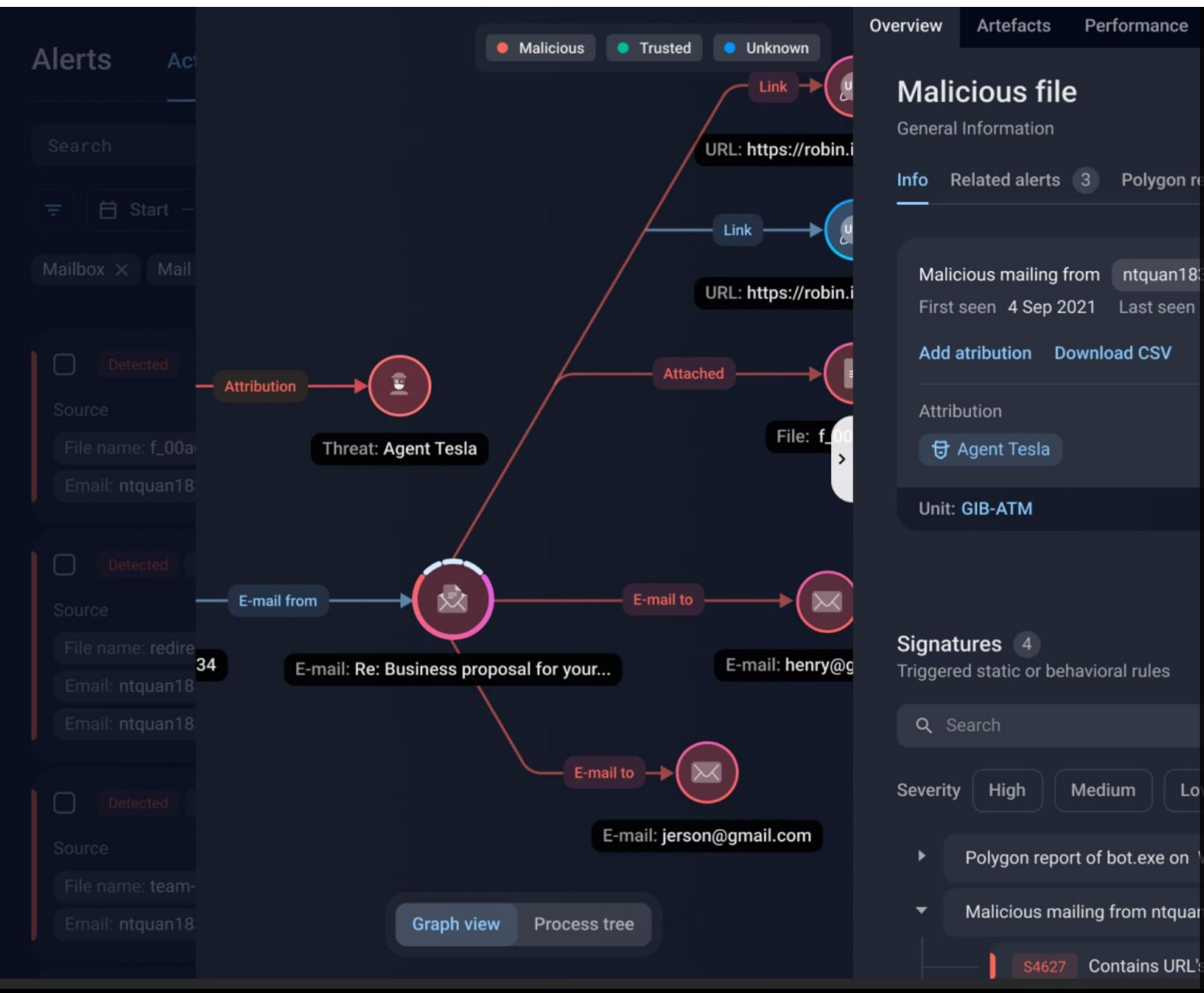
Access Layer

Deep Learning Interface

- Developer's API Built-in 으로 제공되는 DL 엔진
- 분류 모델의 시나리오에 따른 Application 레벨 커스터마이징

User Interface

- 기계학습 테스트 Tool
- 결과 탐색 수행



이메일 분석

첨부파일 및 링크분석

다양한 파일 형식을 검사하여 첨부 파일의 안전 여부를 확인합니다.
난독화되고 리디렉션된 링크를 포함한 링크를 확인할 수 있습니다.

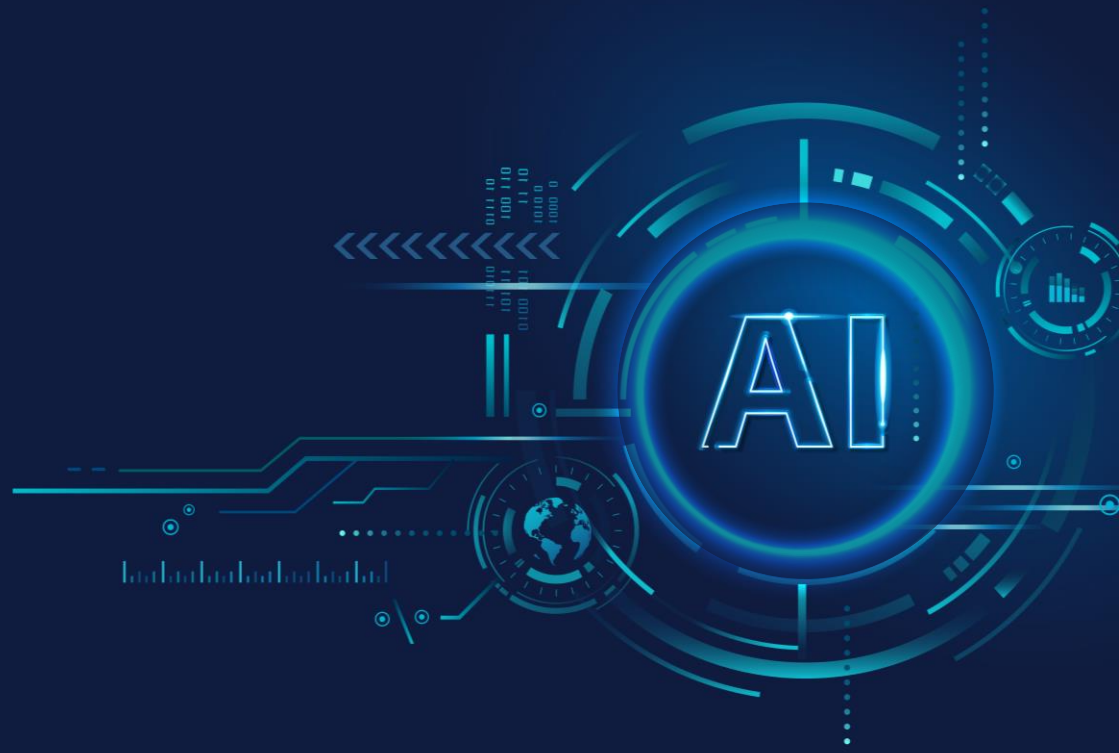
회피방지 기술

시간이 지나면서 상태 변화될 수 있는 의심스러운 URL, 첨부 파일, 개체를 반복적으로 분석하여 숨겨진 위협을 찾아냅니다.

사용자 속성 분석

EMASS AI 인텔리전스 라이브러리를 활용하여 과거 이벤트 리포트를 교차 분석하여 사용자 속성 단위의 정보유출 원인을 파악합니다.

End Of Document



XCURENET