LG CNS

AI를 활용한 내부 정보유출 탐지 사례

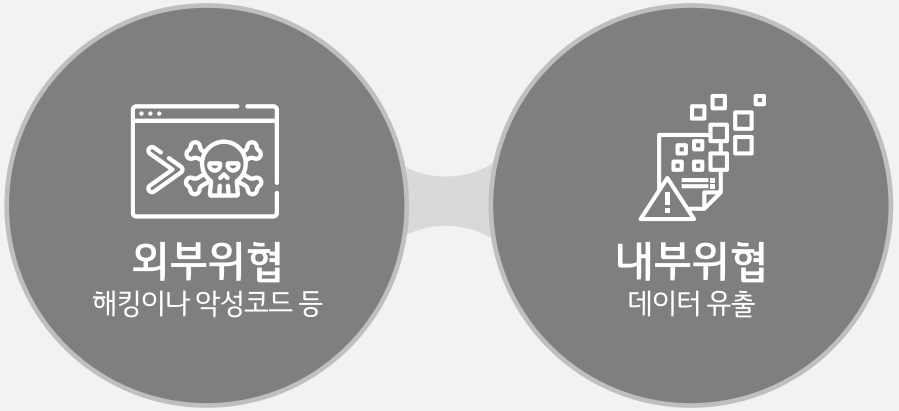
2021. 5.
LG CNS 보안기술전략팀 정좌연 책임

Contents

AI를 활용한 내부 정보유출 탐지 사례

내부위협, 데이터유출 현황

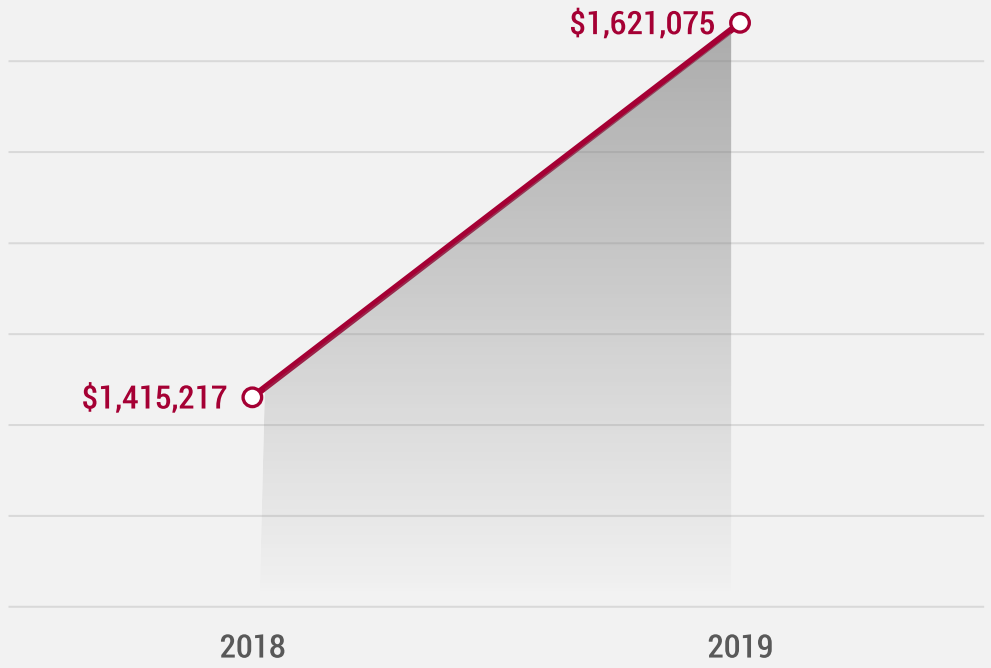
보안의 위협 대응영역



주요 보안 위협 사례

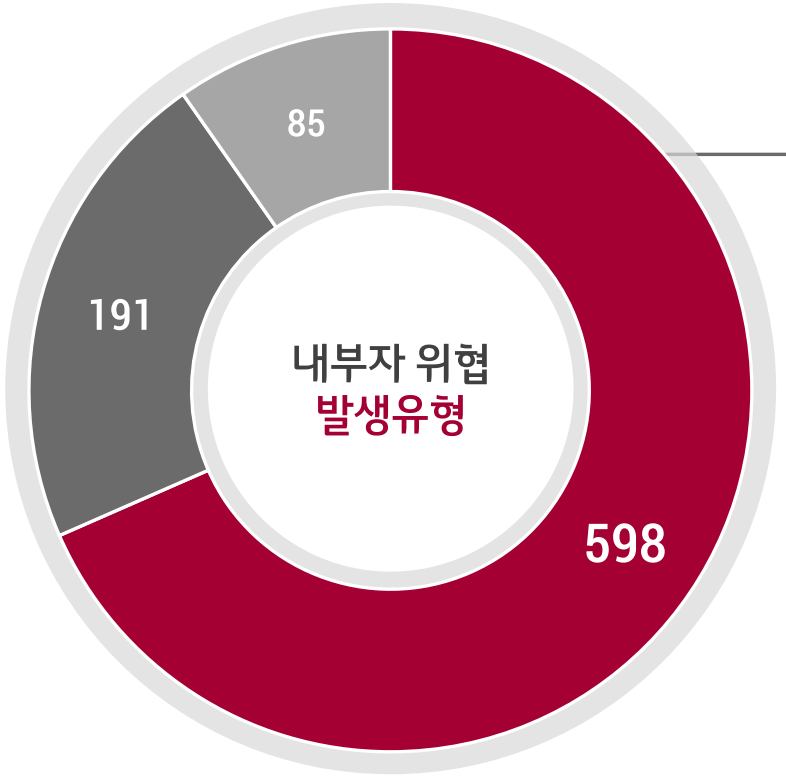
- '14년 | 1억 4천만 건의 개인정보 유출
- '20년 | N번방 피의자 주민 정보 불법 조회

내부 위협에 의한 피해 비용



Data provided by Accenture & Ponemon's 2019 Cost of Cybercrime Study

내부자 위협의 발생유형



3가지 데이터 유출 유형에 대한 발생 비율

1st
부주의한 내부자 | 64.9%

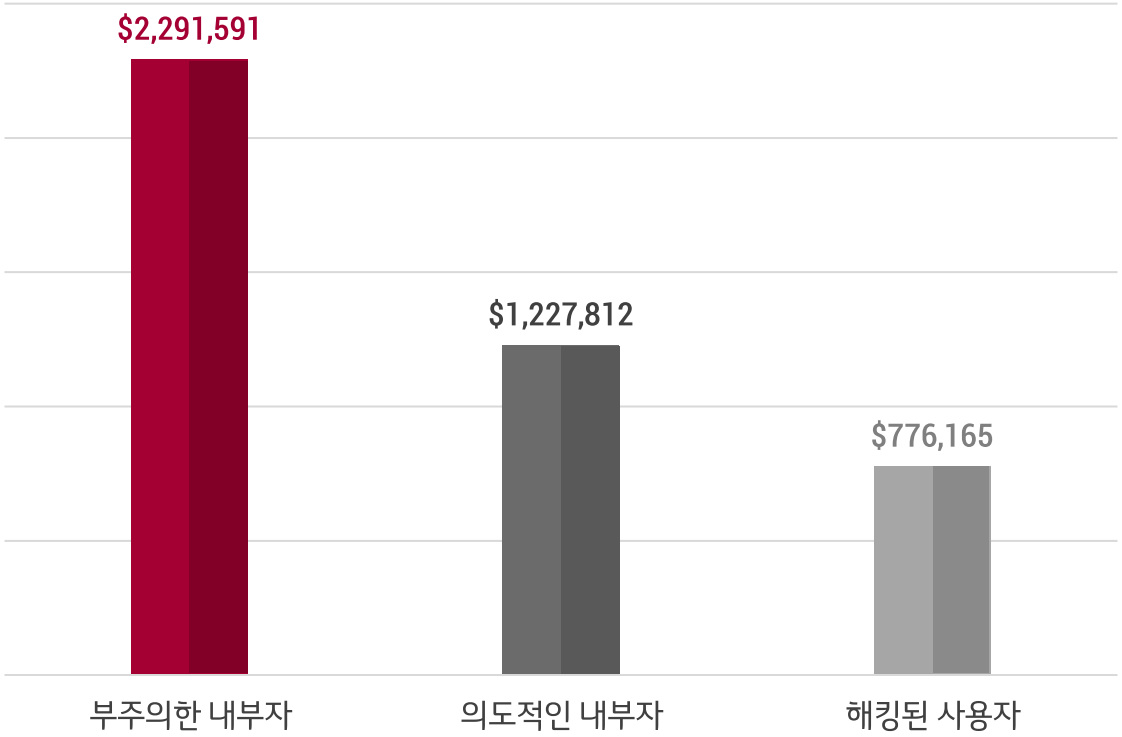
2nd
의도적인 내부자 | 21.8%

3rd
해킹된 사용자 | 9.7%

출처: Ponemon Institute

내부자 위협의 유형별 피해 규모

3가지 데이터 유출 유형에 대한 연간 평균 피해 금액



출처: Ponemon Institute

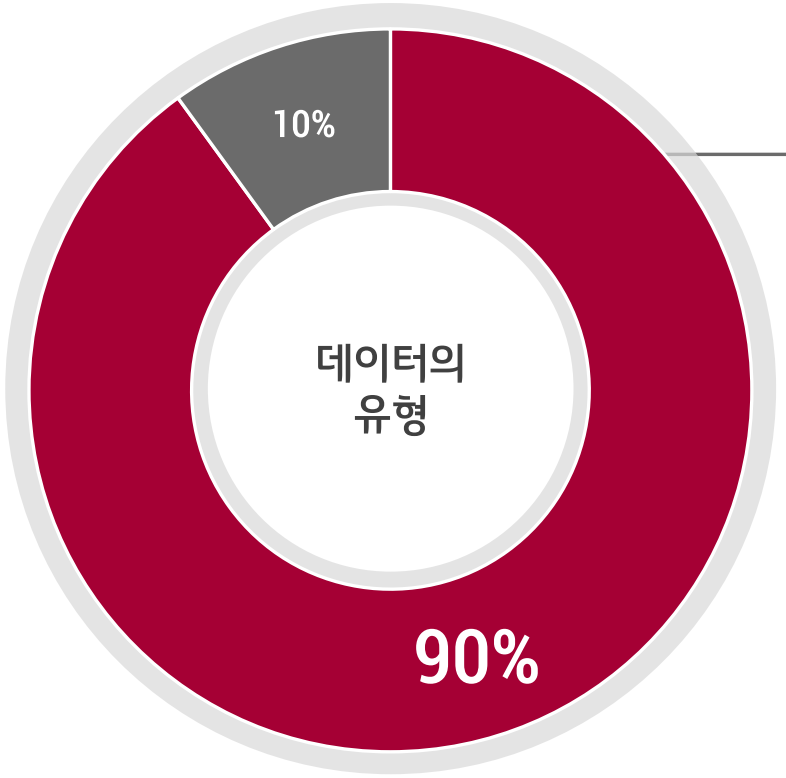
내부자 유출에 따른 대응방법

내부자 유출 유형	대응 방법
부주의한 내부자	직원 보안 교육
해킹된 사용자	탐지 기능 개선
의도적인 내부자	사용자 행위 분석(UBA or UEBA)

- STEP 01 사용자의 모든 행위 모니터링
- STEP 02 분석 엔진을 통한 의심 사용자 식별
- STEP 03 정황정보(Context)와 증거확보

데이터의 90%가 비정형 데이터이다

* IDC, Oracle Corporation



데이터의 90%가 비정형 데이터

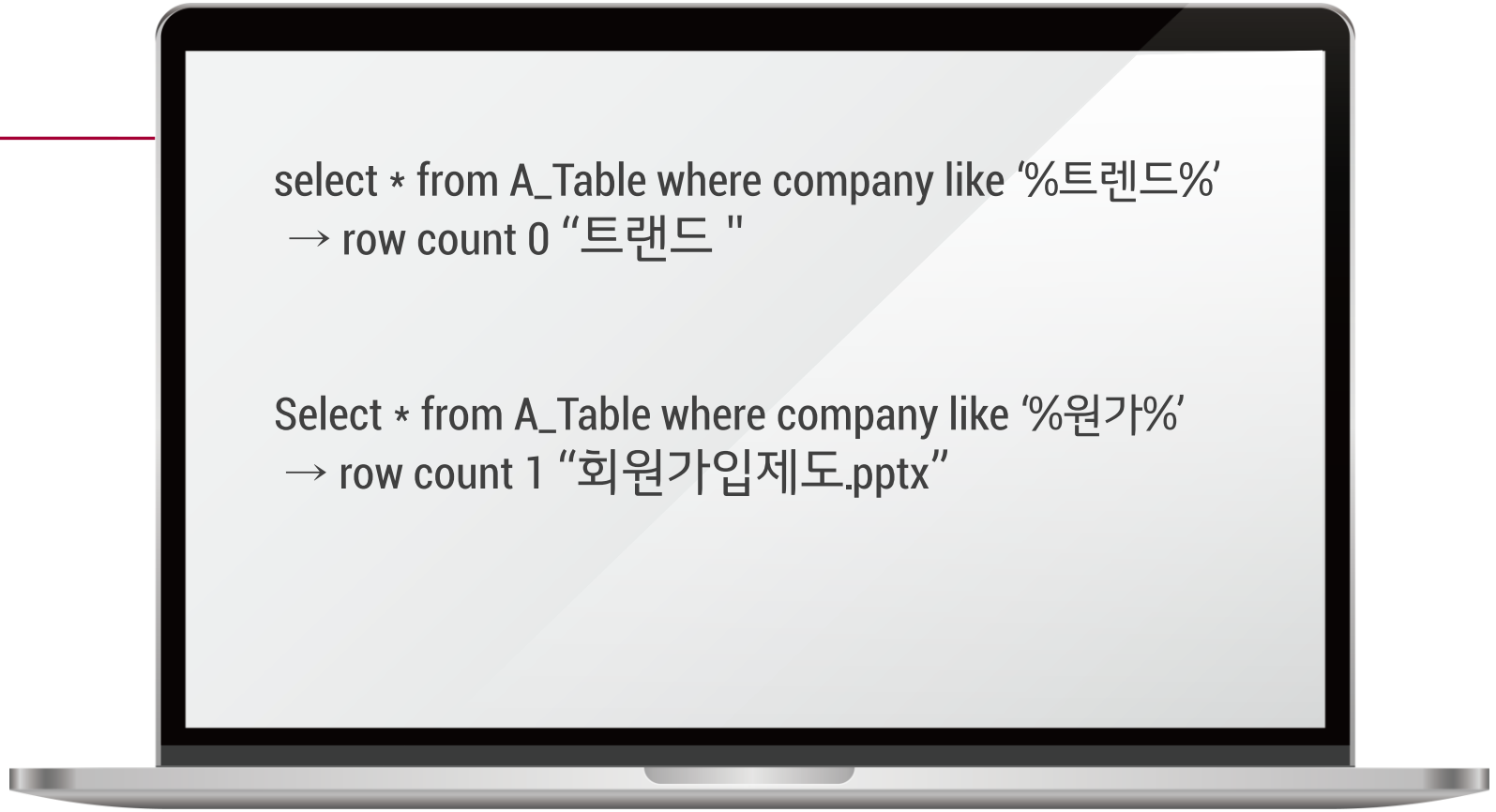
Unstructured or semi-structured data

Examples

- 시스템 로그
- 개인정보 및 접속로그
- 이메일
- 출력물
- 패킷 및 기타 보안 솔루션 로그

패턴 탐지에서 사용되는 SQL의 어려움

SQL Query의 한계



자연어처리를 활용한 문자열 비교 – 유사도 식별(python)

유사수준
약 90%로 식별 가능

```
import jellyfish
import json

column_text1 =  ' 트렌드 '
column_text2 =  ' 트랜드 '

class table_object(object):
  def __init__(self, table, column_text):
     self.table = table
     self.column_text = column_text

table_objects = []
table_objects.append(table_object('table1', column_text1))
table_objects.append(table_object('table2', column_text2))
jellyfish.jaro_distance(table_objects[0].column_text, table_objects[1].column_text)
```

비정형데이터 포함한 통합분석

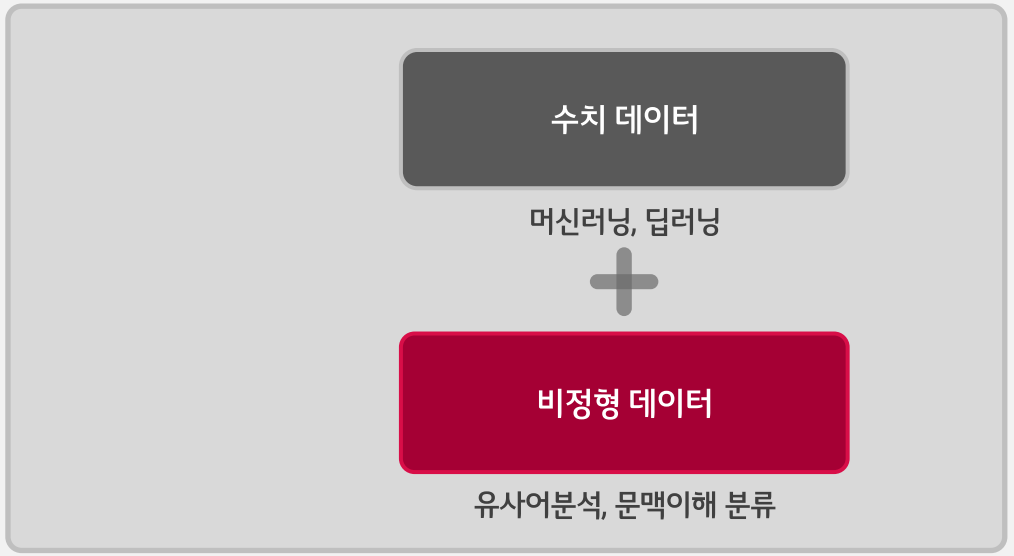
새로운 Insight 추출 가능

[AS-IS] 규칙기반 or 머신러닝

- 낮은 정확도, 높은 오탐율

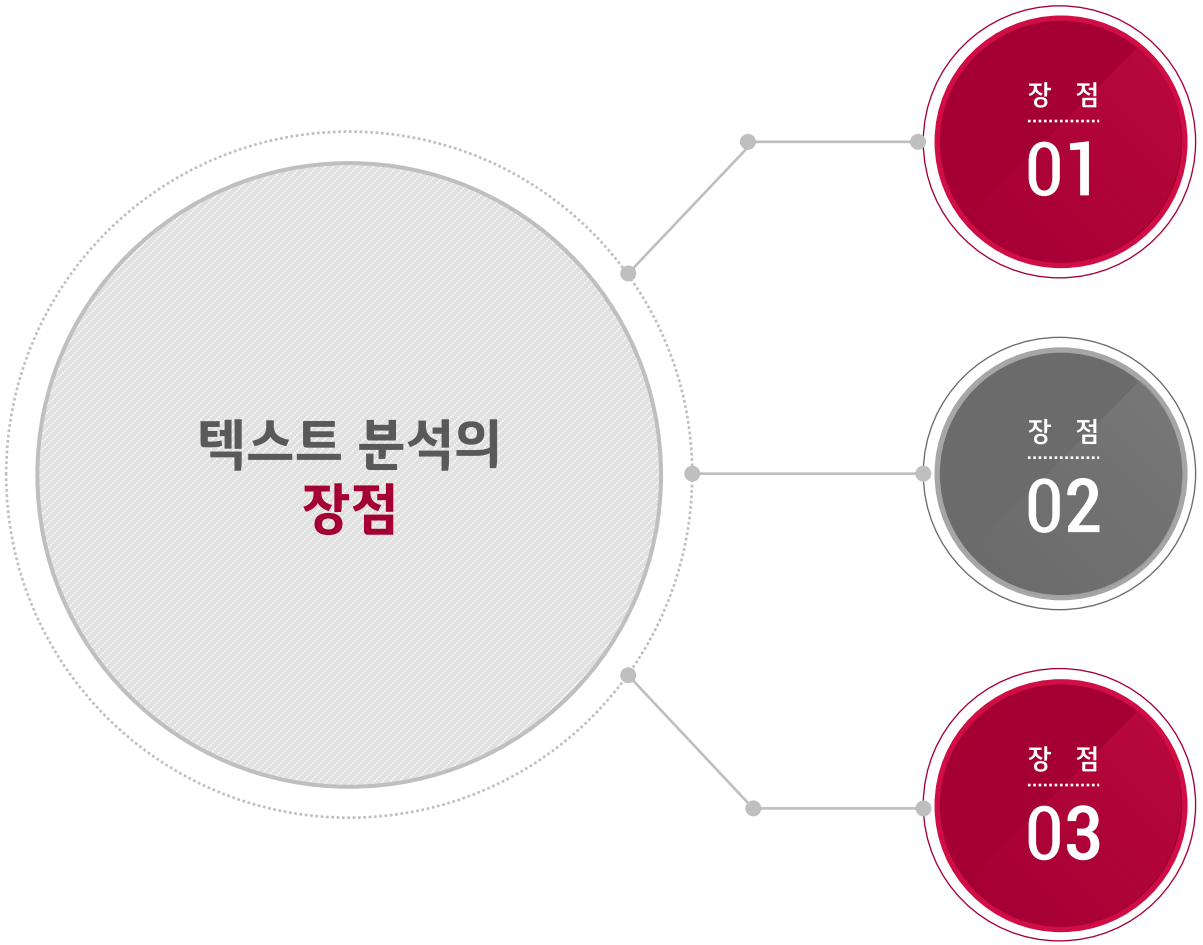
[ABBA] 딥러닝 + 텍스트분석

(한글자연어 처리 포함)



- 높은 정확도, 종합적인 분석 접근
- 다양한 사용자의 행위 분석 가능

보안에서의 Text Analytics의 활용



보안전문가의 판단 지식 내재화

- 학습데이터 생성을 통해 보안전문가의 판단이 반영된 학습데이터 생성 필요
- 해당 모델이 반영된 머신러닝/딥러닝 모델 구성

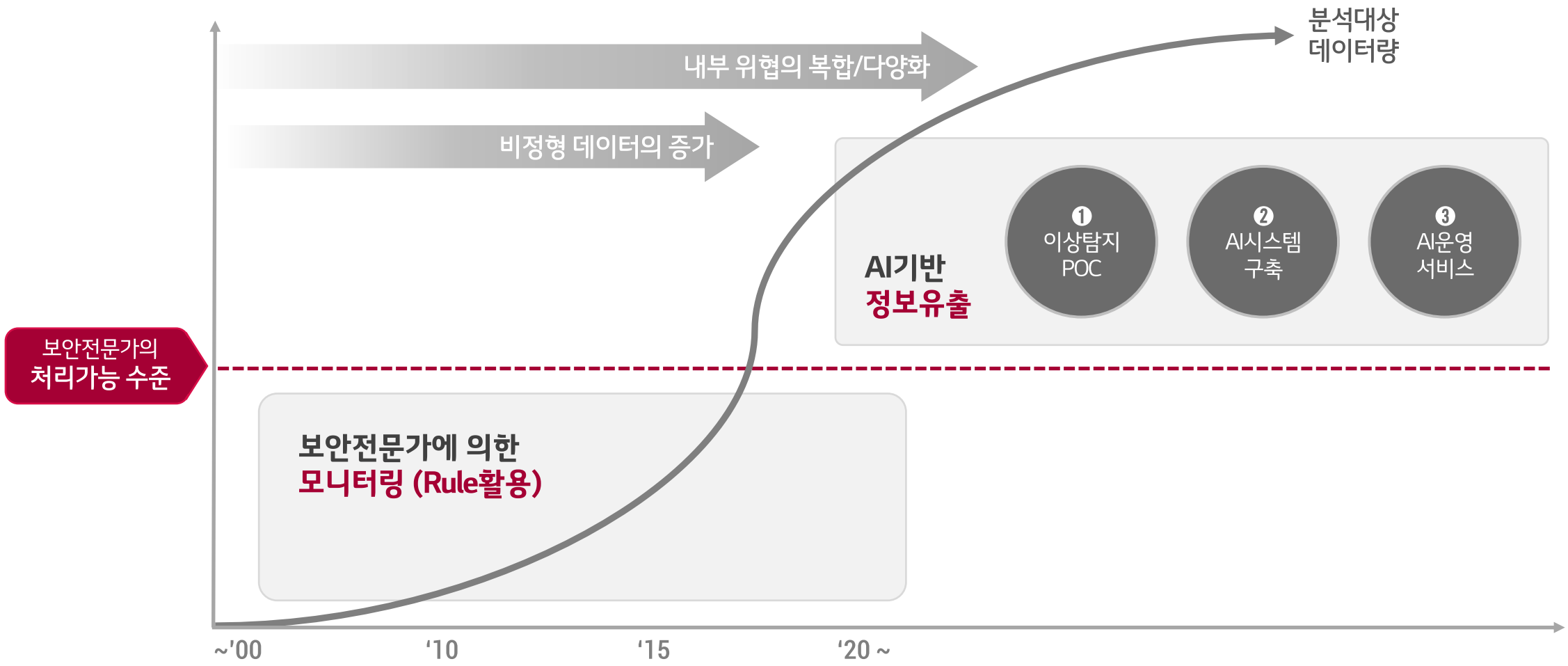
개인성향에 의존한 판단결과가 아닌 조직의 기준을 수립

- 동일한 정황에 대한 판단 기준이 상이
- 조직 차원의 기준 및 표준을 재정립

데이터기반의 유출패턴 탐지와 자동화

- 정확도 개선(오탐/미탐 최소화)에 따른 수동 판정 최소화
- 실시간 분석 및 자동화가 가능

적용 방향성


분석대상
데이터량
내부 위협의 복합/다양화
비정형 데이터의 증가
AI기반
정보유출
❶ 이상탐지 POC
❷ AI시스템 구축
❸ AI운영 서비스
보안전문가의
처리가능 수준
보안전문가에 의한
모니터링 (Rule활용)
~'00
'10
'15
'20 ~

Rule 기반의 한계 개선

AI 도입 전 정보유출 담당자의 고충

❶ 보안 키워드 문자 검색의 한계
- SQL Query의 방식에는 정확한 검색 어려움 (ex. "C.E.O")

❷ 비정상업무/정상업무 판정업무 증가
- 오탐이 포함된 대량의 탐지 결과 증가 (ex. "입사지원서")
- 반복적인 오탐 분류로 업무 부하 증가

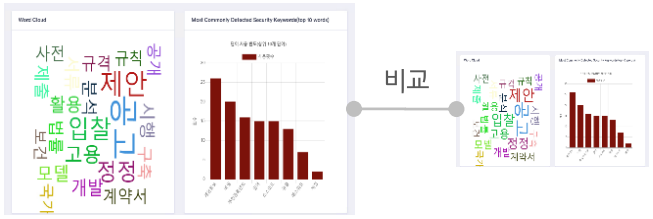
❸ 잦은 주기의 임계치 기준 설정 및 관리의 어려움
- 임계치(외부전송 파일 사이즈 등)의 지속적인 관리 필요
- 동일기준 적용시 과탐 및 미탐으로 적정 수준설정 어려움

주요 개선방안 및 적용 예시

[사례#1] 키워드 유사 단어 목록

보안키워드	유사단어	유사수준
기밀	비밀	0.799
CEO	C.E.O	0.892
.....		

[사례#2] 단어빈도 분석 보고서



[사례#3] AI 추론 후 담당자 최종 판정

No	Contents	AI 추론
1233	XX와 XX는 연관이	정상
1222	개인XX의 정보를~	비정상

AI적용 효과

모니터링 대상
1만 건

• • • 약 40건의 정보유출 행위 탐지 • • •

4. LG CNS의 AI 행위분석 솔루션

정보유출 모니터링에 특화된 AI모델 및 분석 제공을 통해 효율적인 AI모니터링 운영을 지원하는 솔루션

1) NLP 데이터 기반의 로그 자동 분류 및 2) 이상탐지에 최적화된 보안 특화 모델 제공

주요 기능 및 서비스

마치며...

현재 내부 위협 증가와 비정형 데이터가 약90%

필요 보안 전문지식과 텍스트분석 기반의 AI 역량

향후 Security Data Analyst + AI기반 보안분석솔루션

Digital Innovation Enabler

Thank You

LG CNS