

# 기업의 S·AIP 활용 방안

서현민 이사



 **S·AIP**

# There is No Free AI Lunch



Forbes

FORBES > INNOVATION > AI

## What Large Models Cost You – There Is No Free AI Lunch

Craig S. Smith Contributor

Craig S. Smith is a former correspondent and executive at The New York Times. He is host of the...

Follow



Sep 8, 2023, 10:43am EDT



Burning US five and one dollar bills. (Photo by Tom Stoddart/Getty Images) GETTY IMAGES

GPT-4, PaLM, Claude, Bard, LaMDA, LLaMA, Chinchilla, Sparrow – the list of large-language models on the market continues to grow. But behind their remarkable capabilities, users are discovering substantial costs.



내가 승진할 상인가?

직장에서 승진하는 방법은 다음과 같습니다.



내부 데이터를 조회할 수 있어야 하고

데이터의 외부 유출 걱정이 없으며

출처를 표기해줄 수 있는 기술



## 목차

### 1. 산업별 S·AIP 활용 시나리오

# 보안

# 금융

# 제조

### 2. 기업용 생성형 AI 플랫폼 구축 시 고려 사항

### 3. S·AIP 진행 과정

### 4. Why S2W ?

### 5. 기대효과



# 보안 분야 활용 예시

# Jenkins 취약점에 대해서 알려줘



**Exploits released for critical Jenkins RCE flaw, patch now**

By Bill Toulas January 28, 2024 10:17 AM



Multiple proof-of-concept (PoC) exploits for a critical Jenkins vulnerability allowing unauthenticated attackers to read arbitrary files have been made publicly available, with some researchers reporting attackers actively exploiting the flaws in attacks.

Jenkins is an open-source automation server widely used in software development, particularly for Continuous Integration (CI) and Continuous Deployment (CD).

🕒 히스토리    👤 내 업무

📄 새로운 질문

오늘

Jenkins 취약점

지난달 공격그룹 활동 동향

어제

2023 연평균 대출현량

## Jenkins 취약점이 우리 회사에 꼭 필요한 패치일까?

귀사에서 Jenkins 취약점으로 인해 영향을 받을 수 있는 것은 아래와 같습니다.

- Jenkins 2.319.2 이전 버전
- Jenkins 2.319.2 이전 버전의 각종 플러그인

최근 6개월 동안 위 소프트웨어와 관련해 발표된 취약점 중 귀사에 관련된 내용은 아래 링크에서 상세하게 확인하실 수 있습니다.

**asset.s2w.inc**

IP address 00.0.000.00    Port 8090 (Open)

CVE-ID	EPSS	CVSS	Software	Version
<b>CVE-2024-23897</b>	11.94%	7.5	Jenkins	not downconverted
<p>Jenkins 2.441 and earlier, LTS 2.426.2 and earlier does not disable a feature of its CLI command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read arbitrary files on the Jenkins controller file system.</p>				
<b>CVE-2024-23898</b>	0.09%	8.8	Jenkins	not downconverted
<p>Jenkins 2.217 through 2.441 (both inclusive), LTS 2.222.1 through 2.426.2 (both inclusive) does not perform origin validation of requests made through the CLI WebSocket endpoint, resulting in a cross-site WebSocket hijacking (CSWSH) vulnerability, allowing attackers to execute CLI commands on the Jenkins controller.</p>				

ASM Plus  
[asm.quaxar.io/asset](https://asm.quaxar.io/asset)

관련 부서와의 협의를 통해 즉시 조치하는 것을 권장드립니다. Jenkins의 최신수정 버전으로 업데이트하거나 CLI 접근을 비활성화하는 권장 사항을 적용해야 합니다.

외부 지식 검색 포함

🔗 S·AIP가 무엇을 도와드릴까요?

### 참고 자료

- [The Hacker News](#)  
[thehackernews.com/2024/01/critical-jenkins-vul...](https://thehackernews.com/2024/01/critical-jenkins-vul...)  
Critical Jenkins **Jenkins** Vulnerability Exposes Servers to RCE Attacks - Patch ASAP! The maintainers of the open-source continuous integration/continuous delivery and d...
- [SecurityWeek](#)  
[www.securityweek.com/critical-jenkins-vulnerabi...](https://www.securityweek.com/critical-jenkins-vulnerabi...)  
**Jenkins** 2.441 and earlier, LTS 2.426.2 and earlier does not disable a feature of its CLI command parser that replaces an '@' character followed by a file path in an arg...
- [Black Hat](#)  
[www.blackhatethicalhacking.com/news/several-...](https://www.blackhatethicalhacking.com/news/several-...)  
Researchers caution that multiple proof-of-concept (PoC) exploits, aimed at the recently revealed critical **Jenkins** vulnerability CVE-2024-23897, have been disclosed to t...




1. 잘 모르는 것에 대한 **컨텍스트 파악**이 쉬움
2. 제품 **Integration**으로 내 **업무 관련성**에 대한 질문과 답변

최근 한달 간 발생한  
다크웹 랜섬웨어 그룹의 동향을 추적하고,  
각 그룹별로 공격에 사용한 공격 전술에 대해 알려줘.



 히스토리

 내 업무

 새로운 질문

오늘

다크웹 랜섬웨어 그룹 동향

Jenkins 취약점

지난달 공격그룹 활동 동향

어제

2023 연평균 대출현향



최근 한달 간 발생한 다크웹 랜섬웨어 그룹의 동향을 추적하고 각 그룹별 공격 대상 사용된 공격 전술에 대해 알려줘.



1월 한 달 동안 랜섬웨어 활동은 상당한 활동을 목격했으며, 277개의 회사가 공격을 받아 랜섬웨어 그룹이 운영하는 Leak 사이트에 해당 사실이 게시되었습니다. 이 달에는 4개의 Leak 사이트가 새롭게 발견되거나 업데이트 되었습니다. 총35개의 랜섬웨어 공격 그룹이 활동 중으로 확인되었으며, 가장 활발하게 활동한 그룹은 [LockBit](#)(59건), [8Base](#)(28건), [AKIRA](#)(26건), [BlackCat](#)(20건), [BlackBasta](#)(16건)입니다.

이러한 공격의 주요 피해자는 다양한 국가와 산업군에 걸쳐 있으며, 미국이 144개의 피해 회사로 가장 많았습니다. 캐나다, 프랑스, 영국, 이탈리아가 그 뒤를 이었습니다. 제조업 부문이 55건으로 가장 큰 타격을 입었으며, 소매업, 건설업, 의료업, 교육 부문이 그 뒤를 이었습니다.

지난달과 비교했을 때, 피해를 입은 회사의 총 수는 63개가 감소했습니다. AKIRA와 Hunters International이 피해 회사 수에서 가장 큰 증가를 보였으며, 반면 PLAY와 LockBit는 가장 큰 감소를 관찰했습니다.

1월의 주요 랜섬웨어 관련 발전은 세 가지 주요 영역으로 분류되었습니다:


1. 멀웨어 진화: 새로운 랜섬웨어 복호화 도구가 출시되었고, Werewolves와 BianLian과 같은 랜섬웨어 그룹 간의 연관성이 공개되었습니다.
2. 취약점 악용: [AKIRA](#)와 [Mimus 랜섬웨어 그룹](#)이 취약점을 악용하여 랜섬웨어를 유포한 사실이 공개되었습니다.
3. 협박전략: LockBit은 피해 회사의 홈페이지에 랜섬노트를 노출하는 새로운 협박 전략을 사용하기 시작했습니다.

다크웹 영역에서는 두 개의 새로운 Ransomware-as-a-Service(RaaS) 제안이 다크웹 포럼에 게시되었습니다. 또한 BlackCat 랜섬웨어의 소스 코드를 \$30,000에 판매한다는 게시글이 올라왔으며, Affiliate에 의한 유출 가능성이 제기되었습니다. 게다가 8개의 회사가 반복적인 공격을 받은 사실이 공개되어, 사이버 범죄의 지속적이고 진화하는 위협 환경을 강조했습니다. **1**

참고 자료:

- 1 [portal.quaxar.io/knowled...](#)


참고 자료

 QUAXAR

[portal.quaxar.io/knowledgebase/document/repor...](#)

1월 한 달간 277개의 기업이 랜섬웨어 공격에 피해를 당하여 랜섬웨어 그룹이 운영하는 Leak 사이트에 감염 사실이 게시됨. 1월 한 달간 새롭게 발견되거나 주소가 변경된 Leak 사이트는 4건으로 확인됨...

 외부 지식 검색 포함

 S·AIP가 무엇을 도와드릴까요?


🕒 히스토리    🏠 내 업무

📄 새로운 질문

오늘

다크웹 랜섬웨어 그룹 동향

Jenkins 취약점

지난달 공격그룹 활동 동향

어제

2023 연평균 대출현량



보고서 형태로 바꿔줘.



## 다크웹 랜섬웨어 그룹 동향 보고서 2024년 1월

Date | 2024.02.23

### 배경

2024년 1월 한 달 동안의 랜섬웨어 활동은 주목할 만한 변화와 중요한 사건들로 특징지어졌습니다. 총 277개의기업이 랜섬웨어 공격을 받았으며, 이들의 감염 사실이 랜섬웨어 그룹의 Leak 사이트에 공개되었습니다. 또한, 4개의 새로운 또는 주소가 변경된 Leak 사이트가 확인되었고, 35개의 랜섬웨어 공격 그룹이 활동한 것으로 기록되었습니다.

### 활동적인 랜섬웨어그룹

- LockBit: 59건의 공격으로 가장 활발한 활동을 보임
- 8Base: 28건
- AKIRA: 26건
- BlackCat: 20건
- BlackBasta: 16건

### 피해 상황

- TOP 5 국가: 미국(144), 캐나다(17), 프랑스(15), 영국(14), 이탈리아(8)
- TOP 5 산업군: 제조업(55), 소매업(23), 건설업(22), 의료업(21), 교육(18)

### 주요 변화

- 전월 대비 총 피해 기업 수에서 63개 감소를 기록
- 피해 기업 수 증가 TOP5: AKIRA(+10), Hunters International(+10), Trigona(+8), Mydata(+7), 8Base(+6)
- 피해 기업 수 감소 TOP5: PLAY(-23), LockBit(-22), DragonForce(-20), Werewolves(-17), Cactus(-10)

### 주요 사건

- Malware: Werewolves와 BianLian간의 연관성이 밝혀지고, 1개의 랜섬웨어 복호화 도구가 공개됨
- Vulnerability: AKIRA와 Mimus가 취약점을 악용하여 랜섬웨어를 유포한 사실이 공개됨

### 참고 자료

📄 QUAXAR

<portal.quaxar.io/knowledgebase/document/repor...>

1월 한 달간 277개의 기업이 랜섬웨어 공격에 피해를 당하여 랜섬웨어 그룹이 운영하는 Leak 사이트에 감염 사실이 게시됨. 1월 한 달간 새롭게 발견되거나 주소가 변경된 Leak 사이트는 4건으로 확인됨...

외부 지식 검색 포함

🔗 S·AIP가 무엇을 도와드릴까요?





RECAP

1. 정보의 정확성을 위해 **지식그래프를 활용한** 데이터 추출
2. 내가 받은 답변을 **보고서 형태로** 작성

# 금융 분야 활용 예시





금융 분야 활용 예시

이 자료에서 중고 자동차 할부 금융 관련 부분을  
블렛 포인트로 요약해줘



🕒 히스토리

👤 내 업무

📄 새로운 질문

오늘

중고 자동차 할부 금융

산업별 연평균 대출 현황

다크웹 랜섬웨어 그룹 동향

Jenkins 취약점

지난달 공격그룹 활동 동향

어제

2023 연평균 대출현황



이 자료에서 중고 자동차 할부 금융 관련 부분을 볼렛 포인트로 요약해줘

📄 할부 금융 보고서(최종본).pdf ×



보고서에 따르면 중고차 할부 금융과 관련된 주요 내용은 다음과 같습니다

- 중고차 할부 금융 상품의 이자율은 신차 할부 금융 상품에 비해 2~3배 높음.
- 주로 신용등급 5등급 이하의 서민계층이 중고차 할부 금융 상품을 이용하며, 이들은 25% 내외의 고금리로 인해 경제적 부담을 겪고 있음.
- 중고차 할부 금융 상품의 이자율에는 할부 금융사들이 제휴점에 지급하는 중개수수료가 포함되어 있어 소비자가 이를 전액 부담함.
- 최근 6년 동안 중고차 할부 중개 수수료는 지속적으로 상승해, 2006년 4~5%에서 2011년 상반기에는 최고 9.9%까지 올라 중고차 할부 금융 금리 형성에 큰 영향을 미치고 있음.



외부 지식 검색 포함

📄 그렇다면 중고 자동차 할부 금융을 가장 많이 이용하는 신용등급을 알려주고 해당 신용등급에 대한 회사별 대출 금리와 평균 금리, 현재 우리 회사의 평균 금리를 비교하는 그래프를 그려줘. ▶

🛡️ 채팅 내에 사용되는 데이터는 안전하게 보호됩니다.

외부 지식 검색 포함

📄 그렇다면 중고 자동차 할부 금융을 가장 많이 이용하는 신용등급을 알려주고 해당 신용등급에 대한 회사별 대출 금리와 평균 금리, 현재 우리 회사의 평균 금리를 비교하는 그래프를 그려줘. ▶

참고 자료

입력창에 질문을 하시면, 참고 자료를 여기서 확인하실 수 있습니다.





RECAP

1. 내 업무 PC에 있는 PDF파일을 첨부하여 빠르게 요약
2. 첨부한 PDF와 내부 시스템 정보를 결합하여 분석 가능

내가 첨부한 테이블에서 산업별 연평균 대출현황 성장률을 계산해주고,  
2023년 연평균을 기준으로 각 산업별 대출현황 대비  
자사의 산업별 대출현황의 비중을 분석해줘.



히스토리

내 업무



산업별 대출 현황 성장률과 2023년 기준 자사의 대출현황 비중을 기준으로 분산형 그래프를 그려줘

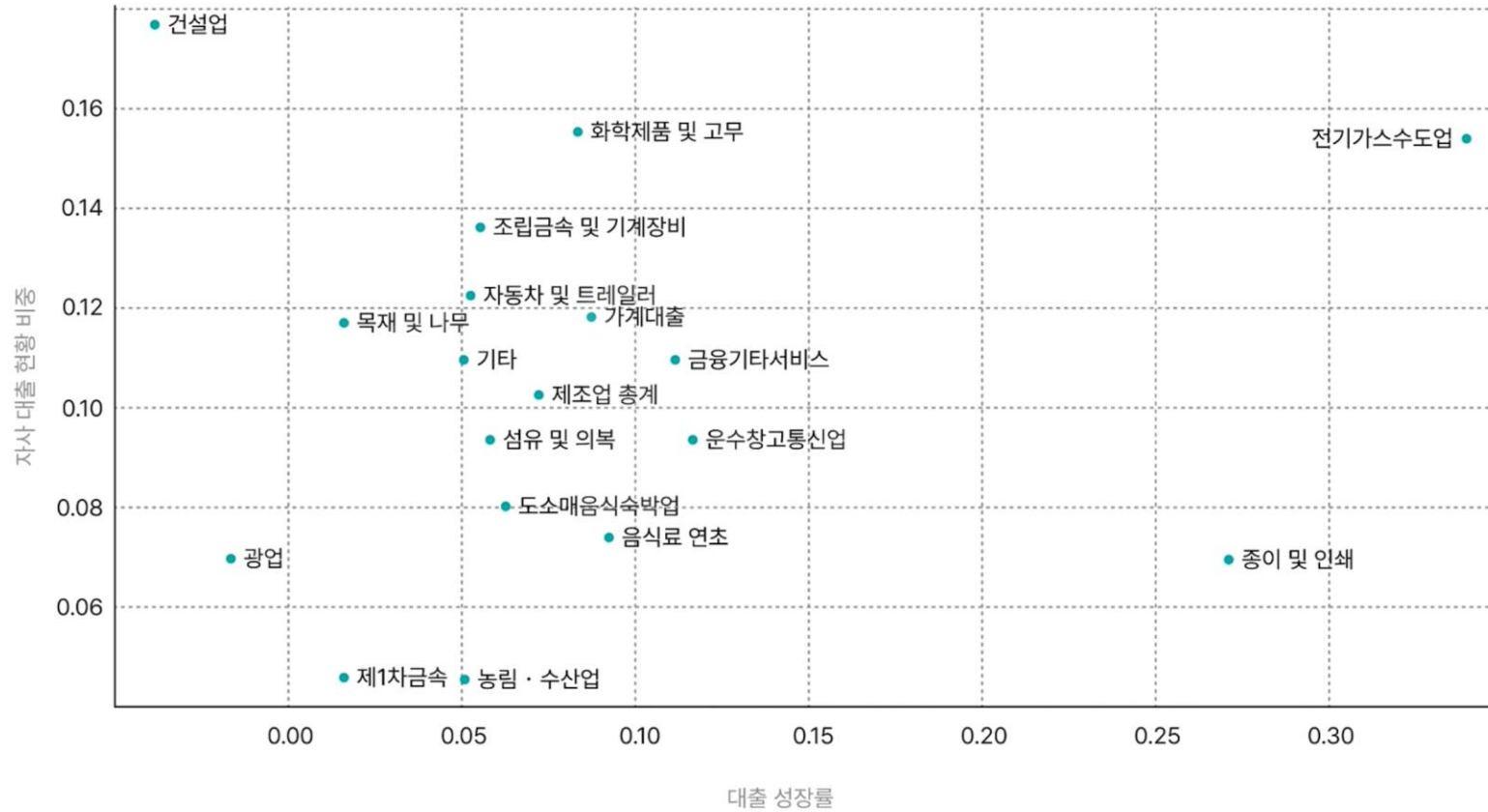
참고 자료

산업별 대출 현황

산업별 대출 현황\_202...xlsx

출, 일시 : '20. 12. 02 (수), 안전조치 : 11/15 06:33  
3 (0.2h), 11/15 06:43 ~ 11/15 07:02 (0.3h), 조업  
6:33 ~ 11/15 07:02 (0.5h), 고장개요 : 2CB Car...

산업별 대출 성장률 vs 자사 대출 현황 비중



Copy image

최근 질문 목록

S·AIP가 무엇을 도와드릴까요?





RECAP

1. 첨부 파일에 대한 **데이터 분석**이 가능
2. 데이터 시각화를 위한 **그래프 형태 분석** 가능



# 제조 분야 활용 예시

최근 6개월 간 일어났던  
안전사고 내역과 사고 유형이  
재작년에 비해 어느정도 변했는지 알려줘



🕒 히스토리 📁 내 업무

📄 새로운 질문

오늘

최근 6개월 안전사고 내역

중고 자동차 할부 금융

산업별 연평균 대출 현황

다크웹 랜섬웨어 그룹 동향

Jenkins 취약점

지난달 공격그룹 활동 동향

어제

2023 연평균 대출현황



### 최근 6개월 간 일어났던 안전사고 내역과 사고 유형이 재작년에 비해 어느 정도 변했는지 알려줘



최근 6개월 간 일어난 안전사고 내역과 그 유형이 재작년 대비 어떻게 변했는지 분석합니다.

- 사고 일자
- 사고 유형 (예: 기계 고장, 화학 물질 누출, 작업자 부주의, 전기적 문제 등)
- 부상자 수
- 사망자 수

재작년(2022년)과 올해(2024년 상반기)의 데이터를 기반으로 제조업에서 발생한 안전사고의 유형 변화를 분석한 결과는 다음과 같습니다.

2022년 사고 유형별 발생 빈도 1 2 3

사고 유형	2022년 1월-6월 사건 수	2022년 1월-6월 사건 비중	최근 6개월 사건 수	최근 6개월 비중
전기적 문제	34	33.66%	27	36.00%
기계 고장	27	26.73%	21	28.00%
화학 물질 누출	21	20.79%	20	26.67%
작업자 부주의	19	18.81%	7	9.33%
총계	101	100%	75	100.00%

Python code

Download sheet

이 데이터를 통해 다음과 같은 관찰을 할 수 있습니다.

- 전기적 문제는 여전히 가장 빈번한 사고 유형이지만, 발생 빈도가 감소했습니다.
- 화학 물질 누출 사고의 빈도도 감소했으나, 상대적으로 높은 비율을 유지하고 있습니다.
- 기계 고장과 작업자 부주의로 인한 사고 빈도가 상당히 감소했습니다.

참고 자료:

- 1 📄 2022 안전사고 이력관...xlsx
- 2 📄 2022 안전사고 이력관...xlsx
- 3 📄 2022 안전사고 이력관...xlsx

외부 지식 검색 포함

🔗 S-AIP가 무엇을 도와드릴까요?



1. 내부 DB 조회가 가능하며, 어떤 DB를 활용했는지 출처 명시
2. 여러 DB를 조회해서 데이터를 비교 분석





제조 분야 활용 예시

최근 3년 현장별로 **하자가 많은 사이트** 중에  
주로 어떤 민원이 발생했는지 **요약**해주고  
**소송**까지 넘어간 **케이스**도 알려줘



🕒 히스토리 🏠 내 업무

📄 새로운 질문

- 오늘
- 최근 3년 주요 민원
- 최근 6개월 안전사고 내역
- 중고 자동차 할부 금융
- 산업별 연평균 대출 현황
- 다크웹 랜섬웨어 그룹 동향
- Jenkins 취약점
- 지난달 공격그룹 활동 동향
- 어제
- 2023 연평균 대출현황

👤 최근 3년 현장별 하자가 많은 사이트 중에 주로 어떤 민원이 발생했는지 요약해주고 소송까지 넘어간 케이스도 알려줘

🤖 최근 3년 간 현장별 하자가 많은 사이트에서 발생한 주요 민원과 소송까지 이어진 케이스에 대해 요약합니다.

- 사이트 이름
- 민원 유형 (예:구조적 결함, 마감재 하자, 설비 문제, 소음 및 진동, 방수 문제 등)
- 민원 발생 횟수
- 소송으로 이어진 여부

민원 유형별 발생 횟

```

SQL query
SELECT
  S.SiteName,
  S.Location,
  D.DefectType,
  COUNT(D.DefectID) AS DefectCount,
  COUNT(L.LawsuitID) AS LawsuitCount
FROM
  Sites AS S
  INNER JOIN Defects AS D ON S.SiteID= D.SiteID
  LEFT JOIN Lawsuits AS L ON D.DefectID= L.DefectID
WHERE
  D.ReportDate>= CURDATE() - INTERVAL 3 YEAR
GROUP BY
  S.SiteName,
  S.Location,
  D.DefectType
HAVING
  DefectCount> 0
ORDER BY
  
```

Copy code

Python code

- 소송으로 이어진 사
- 판교 사이트
- Californialrvine

이 데이터를 통해 다음과 같은 결과를 얻었습니다.

- 최근 3년간 민원
- 구조적 결함, 마감재 하자, 설비 문제와 관련된 민원이 발생하였습니다.
- 소송으로 이어진 사이트는 판교사이트, Californialrvine 사이트로 확인되었습니다.

참고 자료:

- 1 📄 2022 안전사고 이력관...xlsx
- 2 📄 2022 안전사고 이력관...xlsx
- 3 📄 2022 안전사고 이력관...xlsx

외부 지식 검색 포함

🔗 S-AIP가 무엇을 도와드릴까요?

참고 자료

- 📄 산업분석시스템 safety\_incident\_history\_2024
- 📄 산업분석시스템 safety\_incident\_history\_2023
- 📄 산업분석시스템 safety\_incident\_history\_2022



RECAP

1. 데이터 추출을 위한 **SQL 쿼리 생성** 가능
2. **소송**과 같은 민감 정보만 추출하여 **인사이트 도출** 가능

# KEY TAKE AWAYS

1. 잘 모르는 것에 대한 컨텍스트 파악이 쉬움
2. 제품 Integration으로 내 업무 관련성에 대한 질문과 답변
3. 정보의 정확성을 위해 지식그래프를 활용한 데이터 추출
4. 내가 받은 답변을 보고서 형태로 작성
5. 내 업무 PC에 있는 PDF파일을 첨부하여 빠르게 요약
6. 첨부한 PDF와 내부 시스템 정보를 결합하여 분석 가능
7. 첨부 파일에 대한 데이터 분석이 가능
8. 데이터 시각화를 위한 그래프 형태 분석 가능
9. 내부 DB 조회가 가능하며, 어떤 DB를 활용했는지 출처 명시
10. 여러 DB를 조회해서 데이터를 비교 분석
11. 데이터 추출을 위한 SQL 쿼리 생성 가능
12. 소송과 같은 민감 정보만 추출하여 인사이트 도출 가능

chatGPT는 못하는 것

**내부 데이터에 대한 질의** ☆

여러 번 시키면 짜증내던 것

**데이터 분석** ☆

요청하면 일주일 걸리던 것

**보고서 생성** ☆

기업용 LLM을 구축할 때 드는 걱정 🤔

# 1. Security



내부 기밀정보가 외부로 유출되는 일이 있지 않을까?



네트워크 관점에서 철저히 내부망에 구축

기업용 LLM을 구축할 때 드는 걱정 🤔

## 2. Privacy



민감정보가 학습되어 문제가 생기지는 않을까?



Machine **Unlearning**을 활용한 학습된 일부분 삭제

# 기업용 LLM을 구축할 때 드는 걱정 🤔

## 3. Access Control

임금 명세서			
성명	홍길동	사번	073542
부서	개발지원팀	직급	팀장
세부 내역			
지급		공제	
임금 항목	지급 금액(원)	공제 항목	공제 금액(원)
기본급	3,200,000	소득세	115,530
연장근로수당	379,728	국민연금	177,570
야간근로수당	15,822	고용보험	31,570
휴일근로수당	94,932	건강보험	135,350
가족수당	150,000	장기요양보험	15,590
식대	100,000	노동조합비	15,000
계열 또는 부장기 지급			
지급액 계	3940,482	공제액 계	490,610
		실 수령액 (원)	3,472,161
계산 방법			
구분	산출식 또는 산출방법	지급액 (원)	
연장근로수당	연장근로시간 수 (16시간) x 15,822원 x 1.5	379,728	
야간근로수당	야간근로시간 수 (2시간) x 15,822원 x 0.5	15,822	
휴일근로수당	휴일근로시간 수 (4시간) x 15,822원 x 1.5	94,932	
가족수당	100,000원 x 1명(배우자) + 50,000원 x 1명(자녀 1명)	150,000	

HR부서만 봐야 하는 민감정보를 타 부서에서 질문한다면?

RBAC, 부서별 INDEX 분리를 통한 접근 통제

기업용 LLM을 구축할 때 드는 걱정 🤔

## 4. DATA



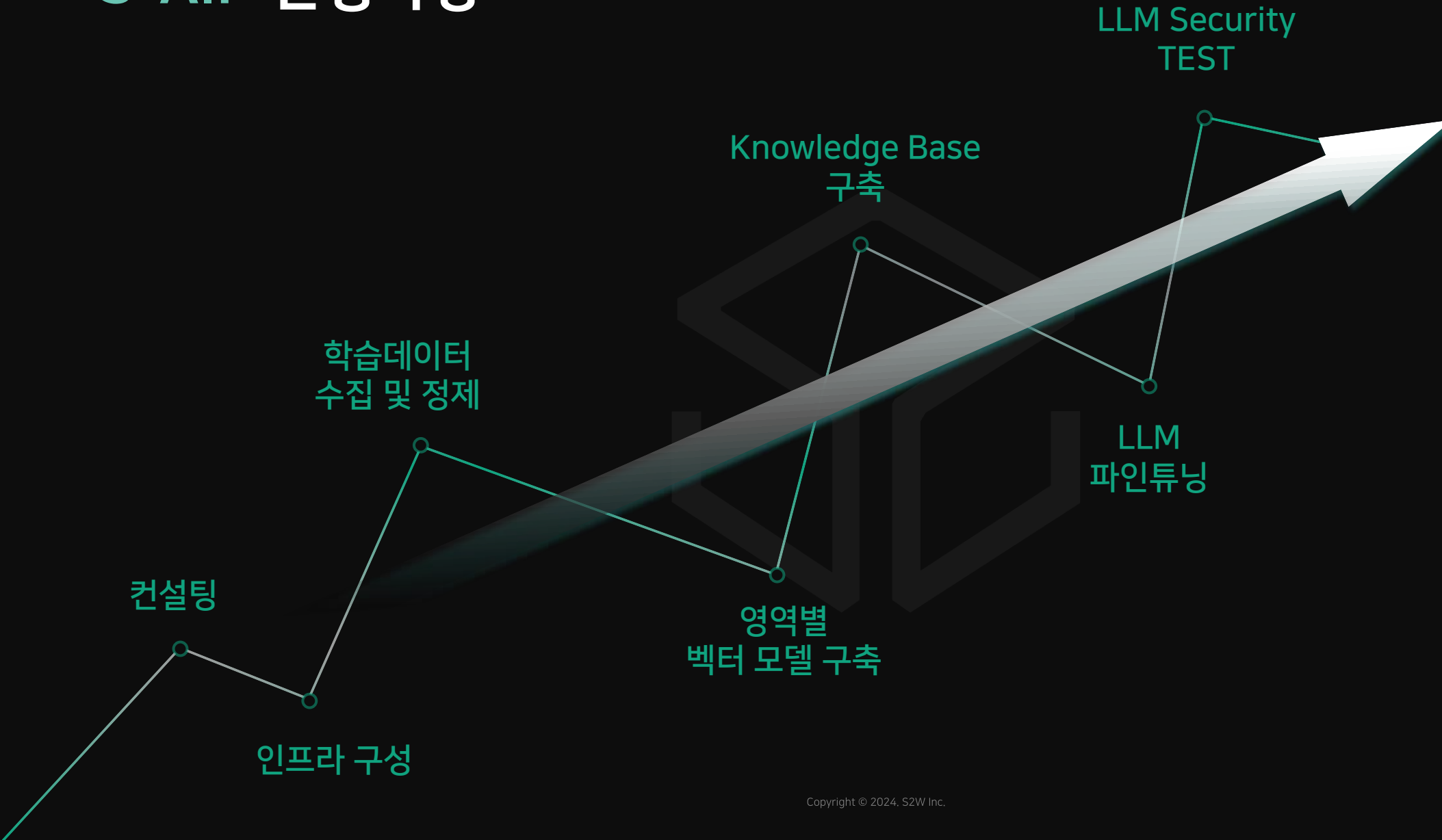
데이터가 너무 지저분하고 구조가 복잡해서 힘들지 않을까?



기업들마다 **다크한 데이터**는 존재하므로  
**비정형 데이터**를 많이 다룬 **경험**이 있는 곳 일수록 유리



# S-AIP 진행과정



# Why S2W?



# 기대효과

- 1 회사 업무를 아는 AI 만들기
- 2 감정소모 없이 AI에게 업무 지시
- 3 업무 생산성 올리기
- 4 보안걱정 없는 AI 만들기
- 5 출처 밝히는 AI 만들기



**S2W**

# 인공지능 빅데이터 인텔리전스 기업

Automated Ontology 기반의 sLLM

Knowledge Graph 기반의 빅데이터 알고리즘

검색-증강-생성-보안 (RAGS) 아키텍처



Discover more about S2W and our solutions.

Please contact us through the email below.

[info@s2w.inc](mailto:info@s2w.inc)

[www.s2w.inc](http://www.s2w.inc) | +82 07 5066 5277

12, Pangyoyeok-ro 192beon-gil #03, Bundang-gu, Seongnam-si, Gyeonggi-do, Republic of Korea

The information contained in this document is proprietary and confidential.  
If you are not the intended recipient, please note that any use or circulation of this document may be cause for legal action.

Copyright © 2024, S2W Inc.