Deloitte
Insights

July 2025

생성형 AI 시대, 사이버보안 리더의 리스크 분석 및 대응 방안

Deloitte Insights

Deloitte.

백철호 파트너

One Cyber & Resilience 리더

생성형 AI는 조직의 혁신을 가속화할 수 있는
강력한 도구인 동시에, 새로운 리스크를 수반합니다.
특히 데이터 출처 불확실성, 보안, 규제 준수와 같은
복합적인 해결 과제가 조직 전반에 영향을 미치고 있습니다.
이에 따라 많은 기업들이 사이버 보안에 대한 투자를
확대하며 대응에 나서고 있습니다.
하지만 지속적으로 진화하는 리스크에 효과적으로 대응하려면
전략적이고 체계적인 보안 접근이 필수적입니다.
신뢰 기반의 생성형 AI 도입을 위한 프레임워크를 구축하고
미래를 준비해야 합니다.

Deloitte.

생성형 AI의 4가지 리스크 분류

사이버 의사결정권자 약 1,200명 대상 조사 결과 분석

01 기업 리스크

조직 운영과 데이터에 대한 위협

02 생성형 AI 역량 리스크

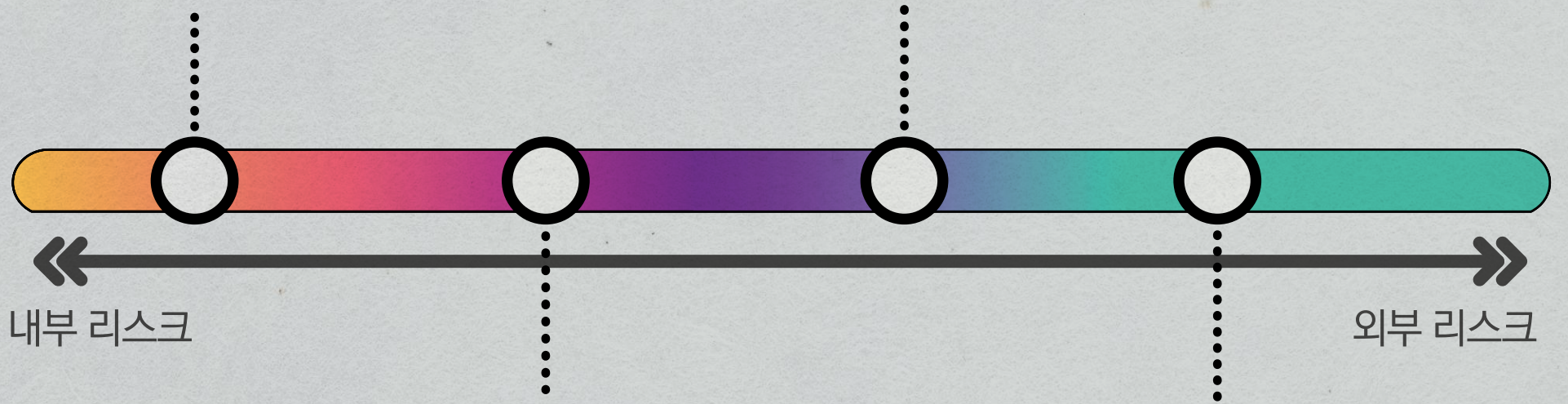
AI 시스템 오작동이나
악용 가능성과 같은
기술적 취약성

03 적대적 AI 리스크

악의적 행위자가 생성형 AI를
활용해 가하는 위협

04 시장 리스크

AI 도입과 보안에
영향을 미치는 경제적,
법적, 경쟁적 압력



출처: 딜로이트 분석

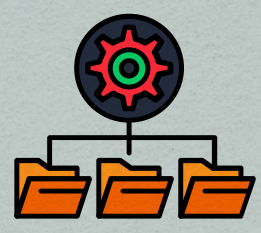
상세한 내용은 리포트 전문에서 확인하세요!

Deloitte.

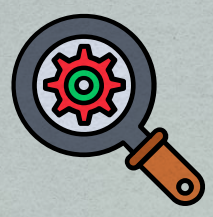
01 기업 리스크

리스크 종류

데이터 출처
추적의 어려움



창작물 주체의
모호성



민감하고 다양한
개인정보 유출

생성형 AI를 소프트웨어
개발 프로세스에 도입

대응 방안

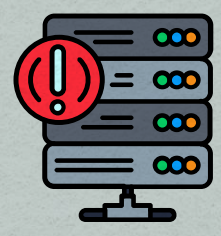
- 디지털 자산 관리 및 데이터 프라이버시 통제
- 지식재산권(IP) 관리 전략 고도화
- 프롬프트 엔지니어링 시대에 맞는
  DevSecOps (개발·보안·운영 통합) 재구성

Deloitte.

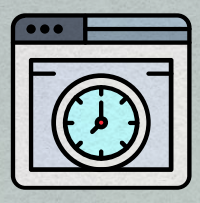
02 생성형 AI 역량 리스크

리스크 종류

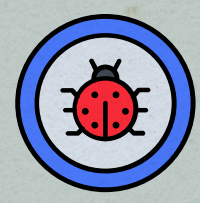
프롬프트 인젝션



회피 공격



데이터 중독



생성형 AI 모델의 환각

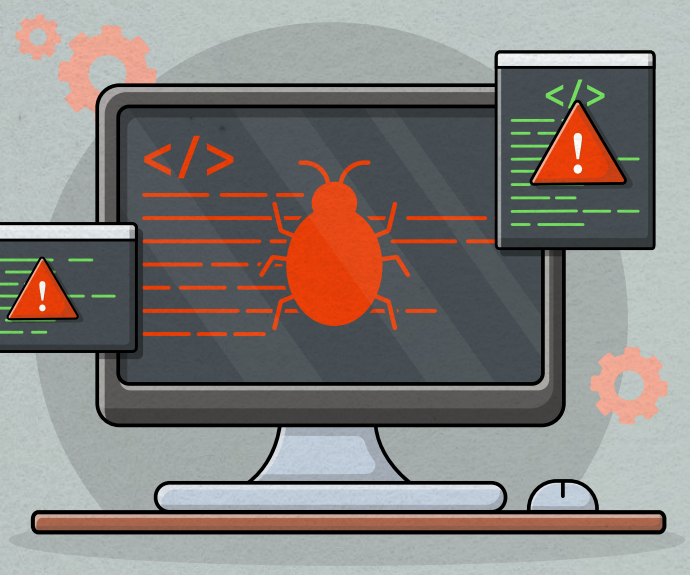
대응 방안

- 입력 가드레일과 모델 방화벽을 통한 프롬프트 인젝션 대응
- 정확도 향상을 위한 파인튜닝
- 생성형 AI를 사이버 역량에 통합

Deloitte.

03 적대적 AI 리스크

리스크 종류



AI 생성 악성코드

사람처럼 보이는 피싱 공격

사칭공격

대응 방안

- 기존 위협 탐지 및 대응 역량 확장
- 적대적 훈련 프로그램 업데이트

Deloitte.

04 시장 리스크

리스크 종류

- 규제의 불확실성
- 생성형 AI 확산에 따른 컴퓨팅 인프라 리스크
- 새로운 가치 사슬의 등장
- 벤더 종속으로 인한 애플리케이션 유연성 부족
- 가치 실현에 대한 우려

대응 방안

- 소형 언어 모델(SLM)과 워크로드 축소로 컴퓨팅 수요 절감
- 전략적이고 효율적인 인프라 투자 의사결정
- 에너지 효율적인 하드웨어 및 워크로드 균형
- 전력 소비 및 전력망 부담 관리

Deloitte.

한국 딜로이트 그룹 전문가

사이버 보안 및 리스크

한국 딜로이트 그룹은 사이버 리스크 대응을 위한 정보보호 및 개인정보보호 자문, 정보보안 인증, 기술적 취약점 진단 및 대책 수립, 정보보호 전략 수립, Cyber Incident 대응 등의 서비스를 제공하고 있습니다. 또한, 수많은 유형의 사이버 리스크를 사전에 방지해 기업 운영의 든든한 조력자 역할을 수행합니다. 리스크 최소화를 통한 안정적인 기업 경영, 딜로이트가 함께 합니다.

백철호 파트너
One Cyber & Resilience 리더

02-6676-2250
cbaek@deloitte.com

서영수 파트너
One Cyber & Resilience

02-6676-1929
youngseo@deloitte.com

유선희 파트너
One Cyber & Resilience

02-6676-2956
sunhyou@deloitte.com

이상훈 수석위원
One Cyber & Resilience

02-6676-2937
sanghunlee@deloitte.com

문범석 파트너
One Cyber & Resilience

02-6676-2949
bsmoon@deloitte.com

이창성 파트너
One Cyber & Resilience

02-6099-4888
changsulee@deloitte.com

Deloitte.

앱스토어, 구글플레이/카카오톡에서 '딜로이트 인사이트'를 검색해보세요.
더욱 다양한 소식을 만나보실 수 있습니다.

Deloitte. Insights

성장전략부문 대표
손재호 Partner
jaehoson@deloitte.com

딜로이트 인사이트 편집장
박경은 Director
kyungepark@deloitte.com

Contact us
krinsightsend@deloitte.com

연구원
양원석 Senior Consultant
wonsukyang@deloitte.com

디자이너
박근령 Senior Consultant
keunrpark@deloitte.com