

# 목차

<b>프로젝트 리더 서문</b>	<b>1</b>
2025 Top 10의 새로운 소식	1
앞으로의 전망	2
한국어 번역팀	2
번역 정보	2
<b>LLM01: 2025 프롬프트 인젝션</b>	<b>3</b>
설명	3
일반적 취약점 예시	3
예방 및 완화 전략	4
공격 시나리오 예시	5
참조 링크	6
관련 프레임워크 및 분류	6
<b>LLM02: 2025 민감 정보 유출</b>	<b>7</b>
설명	7
일반적 취약점 예시	7
예방 및 완화 전략	8
공격 시나리오 예시	9
참조 링크	9
관련 프레임워크 및 분류	9
<b>LLM03: 2025 공급망</b>	<b>10</b>
설명	10
일반적 취약점 예시	10
예방 및 완화 전략	11
공격 시나리오 예시	12
참조 링크	14
관련 프레임워크 및 분류	14
<b>LLM04: 2025 데이터 및 모델 오염</b>	<b>15</b>
설명	15