목차

2025 Top 10의 새로운 소식	프로젝트 리더 서문	1
한국어 번역팀 2 번역 정보 2 LLM01: 2025 프롬프트 인잭션 3 설명 3 일반적 취약점 예시 3 예방 및 완화 전략 4 공격 시나리오 예시 5 참조 링크 6 관련 프레임워크 및 분류 6 LLM02: 2025 민감 정보 유출 7 설명 7 일반적 취약점 예시 7 예방 및 완화 전략 8 공격 시나리오 예시 9 참조 링크 9 관련 프레임워크 및 분류 9 LLM03: 2025 공급망 10 설명 10 일반적 취약점 예시 10 예방 및 완화 전략 11 공격 시나리오 예시 10 예방 및 완화 전략 11 공격 시나리오 예시 12 참조 링크 11 관련 프레임워크 및 분류 11 관련 프레임워크 및 분류 11 관련 프레임워크 및 분류 11 관련 프레임워크 및 분류 15 LLM04: 2025 데이터 및 모델 오염 15	2025 Top 10의 새로운 소식	1
번역 정보 2 LLM01: 2025 프롬프트 인잭션 3 설명 3 일반적 취약점 예시 3 사라 로 경크 6 관련 프레임워크 및 분류 6 LLM02: 2025 민감 정보 유출 7 설명 7 일반적 취약점 예시 7 예방 및 완화 전략 8 공격 시나리오 예시 9 참조 링크 9 관련 프레임워크 및 분류 9 LLM03: 2025 공급망 10 실명 10 일반적 취약점 예시 10 예방 및 완화 전략 11 공격 시나리오 예시 12 참조 링크 14 관련 프레임워크 및 분류 14 LLM04: 2025 데이터 및 모델 오염 15	앞으로의 전망	2
LLM01: 2025 프롬프트 인젝션3설명3일반적 취약점 예시3예방 및 완화 전략4공격 시나리오 예시5참조 링크6관련 프레임워크 및 분류6LLM02: 2025 민감 정보 유출7설명7일반적 취약점 예시7예방 및 완화 전략8공격 시나리오 예시9관련 프레임워크 및 분류9LLM03: 2025 공급망10설명10일반적 취약점 예시10예방 및 완화 전략11공격 시나리오 예시12참조 링크14관련 프레임워크 및 분류14관련 프레임워크 및 분류14관련 프레임워크 및 분류14관련 프레임워크 및 분류14LLM04: 2025 데이터 및 모델 오염15	한국어 번역팀	2
설명 33 일반적 취약점 예시 33 예방 및 안화 전략 44 공격 시나리오 예시 55 참조 링크 66 관련 프레임워크 및 분류 66 LLLM02: 2025 민감 정보 유출 7 설명 7 일반적 취약점 예시 7 예방 및 안화 전략 8 공격 시나리오 예시 9 참조 링크 9 관련 프레임워크 및 분류 9 LLLM03: 2025 공급망 10 일반적 취약점 예시 9 참조 링크 9 관련 프레임워크 및 분류 9 LLLM03: 2025 공급망 10 일반적 취약점 예시 10 예방 및 안화 전략 10 일반적 취약점 예시 10 예방 및 안화 전략 11 공격 시나리오 예시 12 참조 링크 14 관련 프레임워크 및 분류 15	번역 정보	2
일반적 취약점 예시 4 경격 시나리오 예시 5 참조 링크 6 관련 프레임워크 및 분류 6 LLMO2: 2025 민감 정보 유출 7 설명 7 일반적 취약점 예시 7 예방 및 완화 전략 8 공격 시나리오 예시 9 참조 링크 9 관련 프레임워크 및 분류 9 LLMO3: 2025 공급망 10 일반적 취약점 예시 10 예방 및 완화 전략 10 일반적 취약점 예시 10 예방 및 완화 전략 10 일반적 취약점 예시 10 예방 및 완화 전략 11 공격 시나리오 예시 12 참조 링크 14 관련 프레임워크 및 분류 14 관련 프레임워크 및 분류 15 LLMO4: 2025 데이터 및 모델 오염 15	LLM01: 2025 프롬프트 인젝션	3
예방 및 완화 전략 4 공격 시나리오 예시 5 참조 링크 6 관련 프레임워크 및 분류 6 LLM02: 2025 민감 정보 유출 7 설명 7 일반적 취약점 예시 7 예방 및 완화 전략 8 공격 시나리오 예시 9 참조 링크 9 관련 프레임워크 및 분류 9 LLM03: 2025 공급망 10 일반적 취약점 예시 10 예방 및 완화 전략 10 일반적 취약점 예시 10 예방 및 완화 전략 11 공격 시나리오 예시 10 예방 및 완화 전략 11 공격 시나리오 예시 10 예방 및 완화 전략 11 공격 시나리오 예시 12 참조 링크 14 관련 프레임워크 및 분류 14 LLM04: 2025 데이터 및 모델 오염 15	설명	3
공격 시나리오 예시5참조 링크6관련 프레임워크 및 분류6LLM02: 2025 민감 정보 유출7설명7일반적 취약점 예시7예방 및 완화 전략8공격 시나리오 예시9관련 프레임워크 및 분류9LLM03: 2025 공급망10설명10일반적 취약점 예시10예방 및 완화 전략11공격 시나리오 예시12참조 링크14관련 프레임워크 및 분류14관련 프레임워크 및 분류14LLM04: 2025 데이터 및 모델 오염15	일반적 취약점 예시	3
참조 링크6관련 프레임워크 및 분류6LLM02: 2025 민감 정보 유출7설명7일반적 취약점 예시7예방 및 완화 전략8공격 시나리오 예시9참조 링크9관련 프레임워크 및 분류9LLM03: 2025 공급망10설명10일반적 취약점 예시10예방 및 완화 전략11공격 시나리오 예시12참조 링크14관련 프레임워크 및 분류14LLM04: 2025 데이터 및 모델 오염15	예방 및 완화 전략	4
관련 프레임워크 및 분류6LLM02: 2025 민감 정보 유출7설명7일반적 취약점 예시7예방 및 완화 전략8공격 시나리오 예시9참조 링크9관련 프레임워크 및 분류9LLM03: 2025 공급망10설명10일반적 취약점 예시10예방 및 완화 전략11공격 시나리오 예시12참조 링크14관련 프레임워크 및 분류14LLM04: 2025 데이터 및 모델 오염15	공격 시나리오 예시	5
LLM02: 2025 민감 정보 유출7설명7일반적 취약점 예시7예방 및 완화 전략8공격 시나리오 예시9참조 링크9관련 프레임워크 및 분류9LLM03: 2025 공급망10설명10일반적 취약점 예시10예방 및 완화 전략11공격 시나리오 예시12참조 링크14관련 프레임워크 및 분류14LLM04: 2025 데이터 및 모델 오염15	참조 링크	6
설명 7 일반적 취약점 예시 7 예방 및 완화 전략 8 공격 시나리오 예시 9 참조 링크 9 관련 프레임워크 및 분류 9 LLM03: 2025 공급망 10 설명 10 일반적 취약점 예시 10 예방 및 완화 전략 11 공격 시나리오 예시 12 참조 링크 14 관련 프레임워크 및 분류 14 LLM04: 2025 데이터 및 모델 오염 15	관련 프레임워크 및 분류	6
일반적 취약점 예시 7 예방 및 완화 전략 8 공격 시나리오 예시 9 참조 링크 9 관련 프레임워크 및 분류 9 보LLM03: 2025 공급망 10 설명 10 일반적 취약점 예시 10 예방 및 완화 전략 11 공격 시나리오 예시 12 참조 링크 14 관련 프레임워크 및 분류 14 LLM04: 2025 데이터 및 모델 오염 15	LLM02: 2025 민감 정보 유출	7
예방 및 완화 전략8공격 시나리오 예시9참조 링크9관련 프레임워크 및 분류9LLM03: 2025 공급망10설명10일반적 취약점 예시10예방 및 완화 전략11공격 시나리오 예시12참조 링크14관련 프레임워크 및 분류14LLM04: 2025 데이터 및 모델 오염15	설명	7
공격 시나리오 예시9참조 링크9관련 프레임워크 및 분류9LLM03: 2025 공급망10설명10일반적 취약점 예시10예방 및 완화 전략11공격 시나리오 예시12참조 링크14관련 프레임워크 및 분류14LLM04: 2025 데이터 및 모델 오염15	일반적 취약점 예시	7
참조 링크9관련 프레임워크 및 분류9LLM03: 2025 공급망10설명10일반적 취약점 예시10예방 및 완화 전략11공격 시나리오 예시12참조 링크14관련 프레임워크 및 분류14LLM04: 2025 데이터 및 모델 오염15	예방 및 완화 전략	8
관련 프레임워크 및 분류9LLM03: 2025 공급망10설명10일반적 취약점 예시10예방 및 완화 전략11공격 시나리오 예시12참조 링크14관련 프레임워크 및 분류14LLM04: 2025 데이터 및 모델 오염15	공격 시나리오 예시	9
LLM03: 2025 공급망10설명10일반적 취약점 예시10예방 및 완화 전략11공격 시나리오 예시12참조 링크14관련 프레임워크 및 분류14LLM04: 2025 데이터 및 모델 오염15	참조 링크	9
설명 10 일반적 취약점 예시 10 예방 및 완화 전략 11 공격 시나리오 예시 12 참조 링크 14 관련 프레임워크 및 분류 14 LLM04: 2025 데이터 및 모델 오염 15	관련 프레임워크 및 분류	9
일반적 취약점 예시 10 예방 및 완화 전략 11 공격 시나리오 예시 12 참조 링크 14 관련 프레임워크 및 분류 14 LLM04: 2025 데이터 및 모델 오염 15	LLM03: 2025 공급망	10
예방 및 완화 전략11공격 시나리오 예시12참조 링크14관련 프레임워크 및 분류14LLM04: 2025 데이터 및 모델 오염15	설명	10
공격 시나리오 예시12참조 링크14관련 프레임워크 및 분류14LLM04: 2025 데이터 및 모델 오염15	일반적 취약점 예시	10
참조 링크14관련 프레임워크 및 분류14LLM04: 2025 데이터 및 모델 오염15	예방 및 완화 전략	11
관련 프레임워크 및 분류14LLM04: 2025 데이터 및 모델 오염15	공격 시나리오 예시	12
LLM04: 2025 데이터 및 모델 오염 15	참조 링크	14
	관련 프레임워크 및 분류	14
설명 15	LLM04: 2025 데이터 및 모델 오염	15
	설명	15