AYI NEDJIMI Consultants

CyberSec-Assistant-3B : LLM spécialisé cybe français

10 mai 2026 • Mis à jour le 17 mai 2026 • 13 min de lecture • 1969 mots

CyberSec-Assistant-3B est un modèle 3B fine-tuné sur CVE, MITRE ATT&C déployable localement pour SOC francophones.

CyberSec-Assistant-3B est un modèle de langage compact mis à disposition sur l de Ayi Nedjimi et entraîné spécifiquement pour assister les analystes cybersécurit Construit sur une base 3 milliards de paramètres, il a été fine-tuné via SFT et DPO 000 instructions techniques extraites de CVE annotées, de la matrice MITRE ATT& des bulletins du CERT-FR et des guides ANSSI publiquement diffusés. Le modèle tenir dans 8 Go de VRAM sur une carte grand public ou tourner sur CPU en quanti répondant pertinemment aux questions techniques d'un opérateur SOC qui veut c rédiger une recommandation de remédiation, traduire une procédure offensive en expliquer une norme à un comité de direction. Cet article décrit le périmètre du mo d'entraînement, ses cas d'usage opérationnels et se .

À RETENIR

Points clés

CyberSec-Assistant-3B est un LLM francophone spécialisé cybersécurité, en local CPU ou GPU.

Fine-tuning SFT et DPO sur 350 000 instructions issues de CVE, ATT&CK, CERT-FR.

Format GGUF Q4 disponible pour Ollama, llama.cpp, LM Studio et vLLM.

Aucun appel cloud requis : confidentialité native pour SOC souverain et inv sensibles.

Pourquoi un LLM spécialisé cybersécurité francophone

Les grands modèles généralistes savent répondre en français à des questions de peinent sur trois axes. Premièrement, la terminologie franco-française précise : AI SecNumCloud, OIV, OSE n'apparaissent que faiblement dans leurs corpus d'entraî anglophones. Deuxièmement, la précision factuelle sur les techniques MITRE ATT souvent confondu avec un T1078.001 dans une réponse improvisée. Troisièmemen analystes SOC ne peuvent pas envoyer des artefacts d'incident à un service cloud une fuite de propriété intellectuelle ou de données client.

CyberSec-Assistant-3B répond à ces trois exigences. Son corpus de fine-tuning e une dominante française. Les exemples factuels ont été ancrés sur la base CVE-M ANSSI publics afin de réduire les hallucinations. Surt ste permet cent locale, sans aucune dépendance externe.

Réponse sous 24h

Devis gratuit →