Veille Technologique : IA générative, Cloud & Cybersécurité – AWS / Amazon

Sécurisation de l’IA générative et montée en puissance du cloud

La sécurité de l’IA générative devient un enjeu majeur. Les fuites de données et l’usage non autorisé d’outils d’IA représentent des risques importants pour les entreprises et les organisations gouvernementales. AWS recommande une approche *security-by-design*, avec des contrôles adaptés dès la conception des projets IA, des rôles IAM granulaires, et la surveillance des workloads via GuardDuty et Amazon Inspector.

Parallèlement, Amazon EKS franchit une échelle inédite, jusqu’à 100 000 nœuds, pour supporter des architectures microservices et des workloads IA massifs. Cette montée en puissance facilite l’entraînement et l’inférence de modèles très volumineux mais augmente aussi la complexité et les besoins en sécurité des systèmes.

Enfin, Amazon investit 50 milliards de dollars dans des infrastructures IA pour des missions critiques (cybersécurité, recherche médicale) auprès du gouvernement américain, incluant des environnements classifiés Top Secret / GovCloud. Cette double problématique montre l’importance de sécuriser les workloads IA tout en garantissant performance et fiabilité, en particulier dans les secteurs sensibles.

Sources :

AWS – Re:Inforce 2025 : sécuriser l’IA générative dès la conception

ITsocial – Amazon EKS franchit l’ultra-échelle pour absorber la complexité des microservices et de l’IA

BFMTV – Amazon investit 50 milliards de dollars dans des infrastructures IA pour des missions critiques