CAMPUS CYBER

ENSEMBLE, AU SERVICE
D'UNE GRANDE NATION CYBER.

Mise en place de la sécurité de l'IA dans un groupe du CAC40

PROGRAMME DE TRANSFERT AUX CAMPUS CYBER

PERSONAL FINANCE & MOBILITY

Mise en place de la sécurité de l'IA dans un groupe du CAC40

De l'expérimentation à l'industrialisation d'une IA de confiance

Avec l'IA générative et les agents autonomes :

- le modèle devient un **actif critique** ;
- il influence des **décisions** ;
- il manipule des **données parfois sensibles** ;
- il devient une **cible d'attaque**.

👉 Peut-on **faire confiance à une IA** ?

👉 Comment mesurer **un risque qui évolue en permanence** ?

👉 Qui est **responsable lorsqu'une IA se trompe** ?

Mise en place de la sécurité de l'IA dans un groupe du CAC40

Créer un cadre de manière proactive avec une dynamique de veille et d'innovation

PERSONAL FINANCE & MOBILITY

ITD TECHNOLOGIES, DIGITAL & PAIEMENTS

Mise en place d'un Framework Sécurité IA

Mise en place d'un Comité IA

Processus de validation de modèle LLM

Création de la Design Authority IA CA

Mise en place d'un Cadre Normatif IA CA

Partage au Cercle des CISO Monde CA

Participation active à divers GT IA (CA , Campus Cyber)

Prospectives sur les LLM Frontières

Création d'un Standard PSSI IA

Lancement d'un RFI pour la sécurité IA

Bug Bounty IA

Mise en place de la sécurité de l'IA dans un groupe du CAC40

Face aux risques : Mobiliser un continuum de sécurité et de conformité est impératif

La théorie de la Reine Rouge :
Evoluer face aux menaces

Défense : L'IA est déjà utilisée comme outil supplémentaire (non autonome) pour détecter les attaques sur les réseaux et automatiser les réponses.

Attaque (IA adverse) : des acteurs malveillants utilisent l'IA pour améliorer leurs méthodes, notamment en créant des campagnes d'hameçonnage plus sophistiquées et en automatisant les tentatives de piratage.

Réévaluation : Ces menaces amplifiées par l'IA obligent les organisations à réévaluer leurs stratégies de cybersécurité pour garder une longueur d'avance.

LAKERA Giskard AI Red Team CALYPSOAI Deepkeep NeuralTrust

YesWeHack BUG BOUNTY PROGRAMME

Mise en place de la sécurité de l'IA dans un groupe du CAC40

Les essentiels à retenir pour garder le cap

« **La véritable question n'est pas comment déployer l'IA plus vite.** La véritable question est comment déployer une IA suffisamment sûre pour mériter la confiance de nos clients, de nos collaborateurs et de nos régulateurs. »

Les 5 convictions à retenir

1. **L'IA est un sujet de gouvernance** avant d'être un sujet technologique.
2. La cybersécurité seule ne suffit plus : **il faut une sécurité spécifique IA.**
3. **La confiance se construit** grâce à la traçabilité et à l'observabilité.
4. Le **Red Teaming IA et le SOC IA** deviendront des standards.
5. Les entreprises qui réussiront seront celles qui associeront innovation, sécurité et conformité dès la conception **tout en restant Business Partner**.

Image générée par l'IA Gemini

Ready for the Future?

L'IA ne nous remplacera pas. En revanche, une personne sachant utiliser l'IA aura un avantage certain.

Il nous appartient de la guider pour qu'elle devienne un outil de progrès pour tous.

Make Cyber Security Great Again !