Gouvernance de l'IA générative : vers un usage sûr et sécurisé en région EMEA

Par Chris Novak, Directeur senior, Cybersecurity Consulting, Verizon

Introduction

La maîtrise de l'intelligence artificielle (IA) est devenue un vecteur de compétitivité essentiel, comme en témoigne le fort retour sur investissement dans ce domaine. On estime ainsi que chaque dollar investi se traduit par un rendement moyen frôlant les 4 dollars sur un peu plus d'an[1].

Cet élan doit toutefois être encadré par une gouvernance solide, garante d'une « IA responsable » répondant à un code éthique rigoureux. Cette gouvernance doit aussi prendre en compte les menaces et vulnérabilités propres à l'IA générative (GenAI), qu'il s'agisse de répondre à des contraintes techniques, d'anticiper les vecteurs d'attaque ou d'implémenter des mesures de sécurité efficaces.

Certes, les attaques liées à l'IA ne représentent actuellement qu'un faible pourcentage de l'ensemble des cyberattaques, mais leur croissance annoncée est un sujet à prendre très au sérieux.

Santé, finance, réchauffement climatique, énergie, prévention des incendies, Industrie 4.0, productivité, retail… les champs d'application de l'IA semblent infinis. Chez Verizon, nous nous sommes fixé pour mission d'aider les entreprises à exploiter tout son potentiel.

Grâce à l'IA, au cloud et à l'edge computing d'un côté, et aux atouts de la 5G (haut débit, faible latence et forte capacité) de l'autre, les données pourront bientôt circuler librement et facilement au sein de votre réseau d'entreprise[2]. Mais pour les RSSI et les Comex, la sécurité d'une telle infrastructure représente un défi de taille.

C'est la raison pour laquelle nous avons décidé de faire le point sur les promesses et les menaces liées à ces technologies disruptives dans la région EMEA (Europe, Moyen-Orient, Afrique), qui abrite 32,5 % de la population mondiale[3] et génère 38 % du PIB de la planète[4] . Devant de tels enjeux, il devient en effet urgent d'implémenter des mesures de gouvernance et de sécurité à même d'encadrer l'innovation par une sécurité et des règles éthiques adaptées.

1. D. Schubmehl, R. Jyoti et IDC, How leading organizations are using AI to drive impact across every industry and addressing barriers such as AI governance, upskilling, and cost, 2023, ICD. https://news.microsoft.com/source/wp-content/uploads/2023/11/US51315823-IG-ADA.pdf
2. 5G and AI: creating a connected global business, 18 septembre 2020, Verizon Enterprise. https://www.verizon.com/business/resources/articles/s/5g-and-ai-creating-connected-global-business/
3. World Population Clock : la population mondiale atteint 8,2 milliards d'habitants (LIVE, 2024), Worldometer (non daté). https://www.worldometers.info/world-population/
4. J. Boshers Liste des pays de la région EMEA, 5 mars 2024, IstiZada. https://istizada.com/list-of-emea-countries/

GenAI : la terre promise ?

Contrairement à l'IA prédictive, la GenAI est capable de créer ou de générer de nouveaux contenus, idées ou modèles de données sans avoir été explicitement programmée pour le faire.

1. Amélioration de l'infrastructure : la GenAI permet de traiter et d'acheminer les masses de données nécessaires à l'entraînement de modèles d'IA plus complexes, améliorant ainsi les performances et la fiabilité du réseau.

2. Transformation opérationnelle : la GenAI a un fort impact sur les opérations internes, notamment dans les domaines de la vente et de l'ingénierie. En interrogeant des déploiements, des solutions clients et des choix conceptuels antérieurs, les outils conversationnels permettent d'accéder à des informations auparavant cloisonnées.

3. Développement produit et service client : la GenAI analyse les données et les interactions en quasi-temps réel. Elle permet ainsi de développer des fonctionnalités telles que la transcription de flux vidéo ou de proposer un service d'assistance instantané, gage d'une expérience client plus dynamique et plus réactive.

Verizon Connect a récemment lancé sa Dashcam intelligente sur le marché EMEA. Véritable copilote[5], cette solution avancée fournit aux chauffeurs des recommandations en temps réel. Par exemple, si vous suivez de trop près le véhicule devant vous, la Dashcam vous invitera à rétablir la distance de sécurité.

Des entreprises du monde entier s'appuient ainsi sur nos plateformes 5G pour trouver de nouveaux moyens d'exploiter les masses de données fournies par leurs réseaux distribués. C'est notamment le cas des acteurs de santé, qui s'appuient sur les informations collectées en temps réel par leurs appareils de monitoring pour améliorer la qualité des soins.

Grâce aux outils d'IA, tels que la vidéosurveillance intelligente[6] et le traçage des équipements médicaux, les établissements de santé ont dorénavant toutes les cartes en main pour améliorer leurs procédures de diagnostic, la gestion des blocs opératoires et la sécurité des patients.

Expansion de la surface d'attaque

Toutefois, en accélérant la migration vers le cloud et le développement de la 5G distribuée, l'IA expose aussi les entreprises à de nouvelles menaces[7].

Et cette expansion de la surface d'attaque, associée aux capacités puissantes de la GenAI, constitue une source de risque importante pour les organisations qui adoptent l'IA à marche forcée, sans tenir compte de tous les dangers qui l'accompagnent.

Mais si les menaces sont de plus en plus sophistiquées, les attaques reposent encore souvent sur une technique rudimentaire bien connue : l'exploitation des vulnérabilités. Cette méthode figure en effet parmi les trois principaux vecteurs d'accès malveillant à une infrastructure. De même, le Data Breach Investigation Report (DBIR) 2024 de Verizon souligne l'augmentation rapide des vulnérabilités zero-day, insistant au passage sur la nécessité d'améliorer la gestion des correctifs et d'accélérer les temps de réponse[8].

5. New Verizon Connect AI Dashcam delivers enhanced fleet safety and management capability, 18 janvier 2023. Communiqué de presse | Verizon. https://www.verizon.com/about/news/new-verizon-connect-ai-dashcam-deliver
6. How 5G can Improve Patient Data Analytics in Healthcare | Verizon Business. (non daté). Verizon Business. https://www.verizon.com/business/resources/5g/5g-business-use-cases/workforce-productivity/patient-data-analytics/#solution
7. R. Lowman, How AI in edge computing drives 5G and the IoT, 21 février 2020, Semiconductor Engineering. https://semiengineering.com/how-ai-in-edge-computing-drives-5g-and-the-iot/
8. Verizon Business, DBIR 2024. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

En soumettant vos systèmes d'IA naissants à un examen minutieux, vous pourriez par ailleurs découvrir de nouvelles pistes d'optimisation de votre stratégie dans ce domaine, avec à la clé un renforcement de votre posture de sécurité à long terme. Et quand on sait que les vulnérabilités et expositions communes (CVE) devraient augmenter de 25 % d'ici mi-2025[9], il n'est pas étonnant que ces questions soient au cœur des préoccupations des responsables IT.

Le côté obscur de la GenAI

Malgré tout l'engouement que suscite l'IA générative, son usage n'en soulève pas moins des questions de confidentialité. En effet, les technologies GenAI traitent et analysent de grandes quantités d'informations potentiellement sensibles. Il est donc primordial de veiller à l'exactitude des réponses ainsi qu'à l'utilisation éthique des données.

Il n'est pas rare, par exemple, que les grands modèles de langage (LLM) fournissent des informations fausses et erronées. D'apparence souvent véridique, ces « hallucinations » sont parfois le simple fait d'une source erronée[10]. Ce phénomène suscite de sérieuses inquiétudes quant à la fiabilité de ces modèles et au risque de diffusion d'informations trompeuses qui les accompagne, notamment dans le domaine de la santé.

Des chercheurs ont également découvert qu'ils pouvaient récupérer les données d'entraînement de ChatGPT[11] en lui demandant de répéter un mot à l'infini. Cette étrange expérience, qui a permis aux chercheurs d'accéder à des informations personnelles, montre à quel point il est difficile d'empêcher les modèles d'IA de partager involontairement les données sensibles qu'ils ont mémorisées.

Les collaborateurs qui soumettent des informations confidentielles aux assistants conversationnels exposent donc leur entreprise à des compromissions et à des divulgations de données accidentelles. Utilisation de ces informations privées pour entraîner l'IA, exposition de contenus confidentiels à des utilisateurs non autorisés ou à des serveurs tiers, violation des lois sur la protection des données… les conséquences sont multiples.

Il est donc essentiel que les entreprises abordent l'IA de manière responsable et réfléchie, pour qu'innovation rime avec protection des données personnelles et respect de la vie privée.

L'IA et ses vulnérabilités émergentes

L'analyse des cyberattaques réelles et les exercices de sécurité permettent de dresser un constat des vulnérabilités propres aux systèmes d'IA[12].

Même si ces menaces évoluent continuellement, on voit néanmoins émerger un certain nombre de schémas récurrents.

- Empoisonnement des données : des attaquants manipulent les données d'entraînement des modèles d'IA en introduisant des erreurs ou des éléments permettant de déclencher des comportements malveillants. Cet « empoisonnement » reprogramme discrètement l'IA en y intégrant des vulnérabilités ou des backdoors qui s'actionnent sous des conditions spécifiques, compromettant ainsi l'intégrité et la fiabilité du système.

9. S. Staff, CVEs expected to increase 25% in 2024, 21 février 2024, Security Magazine. https://www.securitymagazine.com/articles/100426-cves-expected-to-increase-25-in-2024
10. Large Language Models pose risk to science with false answers, says Oxford study, 20 novembre 2023. https://www.ox.ac.uk/news/2023-11-20-large-language-models-pose-risk-science-false-answers-says-oxford-study
11. M. Nasr, N. Carlini, J. Hayase, M. Jagielski, A.F. Cooper, D. Ippolito, C.A. Choquette-Choo, E. Wallace, F. Tramèr et K. Lee, « Scalable Extraction of Training Data from (Production) Language Models », prépublication arXiv : 2311.17035, Cornell University, 2023. https://arxiv.org/abs/2311.17035
12. MITRE ATLAS™. (non daté). https://atlas.mitre.org/

- Tromper pour contourner : les attaquants créent des entrées capables de tromper les modèles d'IA et de générer des résultats erronés. Grâce à cette technique connue sous le nom de Prompt Injection[13], les attaquants peuvent contourner les systèmes de défense IA en exploitant ses vulnérabilités, dans le but de lui faire exécuter des actions involontaires. Un peu comme si l'on se faufilait derrière des agents de sécurité !

- Repérages de l'architecture : des attaquants explorent les architectures d'IA à l'aide d'une technique connue sous le nom de Discover Machine Learning (ML) Model Ontology[14], et ce afin d'en identifier les faiblesses. Ils peuvent ainsi détecter les vulnérabilités exploitables et concevoir des attaques ciblées qui sapent les défenses du système avec une précision chirurgicale.

Focus sur les menaces réelles

Selon le Data Breach Investigations Report 2024 de Verizon, la majorité (68 %) des compromissions peuvent encore être imputées au facteur humain[15]. Ce chiffre inclut notamment les attaques d'ingénierie sociale et les erreurs commises par les utilisateurs, tout en excluant les abus de privilèges.

En comparaison, les attaques basées sur l'IA font figure d'exception. Malgré cela, les conférences sur la cybersécurité ont tendance à leur accorder une importance démesurée, ce qui peut parfois susciter des inquiétudes injustifiées.

De nombreuses préoccupations se font également entendre concernant les appels téléphoniques frauduleux (deepfakes) et les risques d'attaques d'ingénierie sociale avancées, notamment à l'occasion des élections.

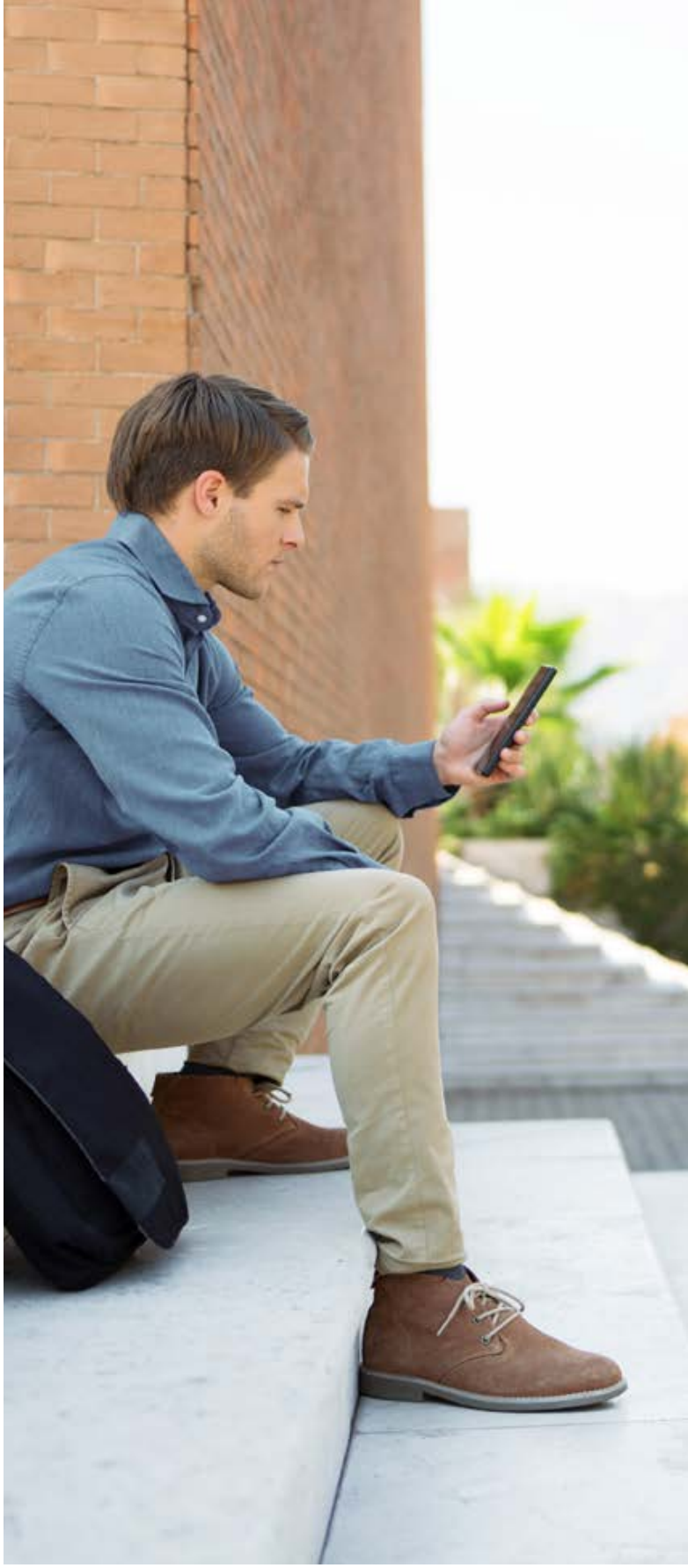
Il convient donc de rétablir certaines vérités à propos de ces attaques :

- La probabilité de subir une attaque de grande ampleur reposant sur des techniques d'IA avancées est actuellement très faible.

- L'IA peut parfois être utilisée pour lancer des attaques plus sophistiquées, mais celles-ci restent rares et ciblent généralement des personnalités publiques de premier plan.

- La plupart des gens sont en réalité plus susceptibles d'être victimes d'attaques de phishing traditionnelles (e-mails et messages frauduleux) que d'attaques basées sur l'IA.

Cette mise en perspective permet de mieux comprendre le champ actuel des menaces et d'orienter les dispositifs de défense dans la bonne direction.



Le rôle de la gouvernance de l'IA

Les entreprises jouent actuellement au chat et à la souris avec les attaquants, qui ne cesseront de perfectionner leurs techniques s'ils y sont contraints.

13. MITRE ATLAS™. (non daté). https://atlas.mitre.org/techniques/AML.T0051
14. MITRE ATLAS™. (non daté). https://atlas.mitre.org/techniques/AML.T0013
15. Verizon Business, Data Breach Investigations Report 2024. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

Les risques semblent par ailleurs de plus en plus sérieux, notamment lorsque les dispositifs d'encadrement de nouveaux modèles d'IA montrent des signes de faiblesses, alors qu'ils sont pourtant censés encourager l'innovation et protéger les entreprises et les acteurs publics. Combattre l'IA par l'IA n'est donc pas qu'une formule clinquante, mais un impératif absolu.

C'est dans cet esprit que l'ANSSI a récemment publié des « Recommandations de sécurité pour un système d'IA générative »[16]. Dans son introduction, ce document met notamment l'accent sur l'importance des questions de sécurité de l'IA, insistant sur les risques pour la confidentialité des données et l'intégrité des systèmes d'information. Le guide propose ainsi des conseils de protection pour les différentes phases du cycle de vie d'un système d'IA.

Dans la même veine, le gouvernement britannique s'efforce d'évaluer et de traiter les menaces et les risques associés à l'IA. Dans cette optique, le National Cyber Security Centre a récemment publié une évaluation intitulée « The near-term impact of AI on the cyber threat », un document analysant l'impact de l'IA sur l'efficacité des cyberopérations, ainsi que les répercussions des cybermenaces au cours des deux années à venir. Il souligne notamment que « s'il est essentiel de se pencher sur les risques posés par l'IA, les professionnels de la cybersécurité doivent également se saisir des opportunités considérables qu'elle leur offre. »[17].

De fait, la ferveur qui entoure le développement d'une première solution GenAI en interne ne doit pas masquer une question fondamentale : comment va-t-on la tester ? Car des tests aléatoires effectués par des personnes qui maîtrisent mal l'IA ont peu de chance de vous apporter des garanties de sécurité suffisantes. C'est un peu comme si vous faisiez appel à un spécialiste de la sécurité résidentielle pour protéger le Pentagone ; l'échelle n'est pas tout à fait la même.

Effectuer un simple test d'intrusion dans un environnement d'IA complexe revient à laisser une porte grande ouverte sur vos systèmes, à l'heure même où la surface d'attaque s'étend aux environnements IoT et où l'Industrie 4.0 a donné naissance aux usines intelligentes. Car les attaquants ne respectent aucune règle d'engagement. Pour eux, tout est permis et tout est bon pour semer le chaos. Les testeurs doivent donc rester vigilants et toujours penser avec un temps d'avance.

Vulnérabilité des supply chains

Les opérateurs d'importance vitale (OIV) travaillant sur des projets IA pilotes peuvent par ailleurs être la cible d'États disposant d'un arsenal cyber plus sophistiqué. C'est la raison pour laquelle il est essentiel de protéger l'ensemble des chaînes d'approvisionnement. Par exemple, en 2022, une cyberattaque contre trois sociétés européennes de transport et de stockage de pétrole (SEA-Invest en Belgique, Oiltanking en Allemagne et Evos aux Pays-Bas) a eu un effet domino sur des dizaines de terminaux dans le monde entier et perturbé l'approvisionnement dans plusieurs ports. Cet événement a ainsi clairement démontré que tous les maillons de la chaîne d'approvisionnement sont concernés, pas seulement les fournisseurs et sous-traitants directs de la cible finale.

Risques et inquiétudes à l'échelle mondiale

La cybercriminalité constitue donc une menace réelle pour les entreprises de la région EMEA (Europe, Moyen-Orient et Afrique). Une étude récente a ainsi révélé que plus d'un tiers des sociétés allemandes avaient été victimes d'une cyberattaque au cours des deux dernières années[18]. Pour plus de la moitié d'entre elles, les pertes ont même augmenté, avec comme principaux coupables le phishing, les fuites de données et les attaques sur les services cloud. Dans ce contexte, on comprend pourquoi la majorité des entreprises estiment que les risques sont élevés voire très élevés.

On peut aussi penser aux répercussions sur les événements sportifs mondiaux, tels que les Jeux olympiques d'hiver de Milan Cortina 2026. L'IA est en effet appelée à devenir le principal vecteur d'attaque lors de ces grands rassemblements planétaires, engendrant des dommages potentiellement considérables sur les plans infrastructurel et financier.

C'est la raison pour laquelle, lors du Super Bowl 2024, les experts de Verizon Frontline ont collaboré avec des dizaines d'agences fédérales pour s'assurer que les équipes de sécurité étaient prêtes à faire face à tout type de menaces : chimiques, biologiques, radiologiques, nucléaires ou cyber. Ils ont notamment procédé à des évaluations continues de la sécurité de l'infrastructure et des sites afin de pouvoir anticiper les potentielles attaques.

Sécurité de la GenAI

D'après l'article « 4 Types of Gen AI Risk and How to Mitigate Them » publié en mai 2024 dans la Harvard Business Review, « les risques liés à l'utilisation de la GenAI peuvent être classés selon deux facteurs : l'intention et l'usage »[19]. L'article revient également sur les raisons pour lesquelles « de nombreuses entreprises hésitent, à juste titre, à adopter des solutions de GenAI. Elles évoquent entre autres des préoccupations concernant la sécurité, le respect des données personnelles et des droits d'auteur ainsi que les risques de biais et de discrimination ».

En région EMEA, les acteurs publics et privés doivent faire abstraction de ces craintes pour se concentrer sur l'échéance de 2030, autour d'une « IA responsable » et garante d'une cybersécurité renforcée. Car sans une

16. ANSSI, Recommandations de sécurité pour un système d'IA générative, 29 avril 2024, https://cyber.gouv.fr/publications/recommandations-de-securite-pour-un-systeme-dia-generative
17. The near-term impact of AI on the cyber threat. (non daté). https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat#:~:text=Artificial%20intelligence%20(AI)%20will%20almost,techniques%20and%20procedures%20(TTPs).
18. C. Reisbeck, Damage to German companies due to cyber attacks is increasing, 27 mai 2024, KPMG. https://kpmg.com/de/en/home/media/press-releases/2024/05/cyber-attacks-damage-for-german-companies-increasing.html#:~:text=Cybercrime%20remains%20a%20real%20threat,in%20the%20past%20two%20years.
19. Ö Isik, 4 Types of gen AI risk and how to mitigate them, 31 mai 2024, Harvard Business Review. https://hbr.org/2024/05/4-types-of-gen-ai-risk-and-how-to-mitigate-them
20. DBIR Report 2024: Public Administration data breaches | Verizon. (non daté). Verizon Business. https://www.verizon.com/business/resources/reports/dbir/2024/industries-intro/public-administration-data-breaches/

gouvernance solide, l'IA pourrait faire plus de mal que de bien en tombant dans de nombreux travers : atteintes à l'éthique, modèles biaisés ou désinformations. D'après le Data Breach Investigations Report 2024 de Verizon, les acteurs des pouvoirs publics détiennent le triste record du nombre d'incidents (12 217), avec plus de 1 085 divulgations de données confirmées[20].

Mobilisation générale autour de la GenAI

Bien que les lignes directrices de l'IA ne soient pas toujours évidentes à mettre en œuvre dans une région EMEA particulièrement hétérogène, on distingue une réelle volonté de placer cette technologie au service de l'intérêt général.

Malgré un certain retard dans le développement de l'IA face aux États-Unis et à la Chine, l'Union européenne (UE) fait figure de référence mondiale sur le plan juridique, à l'image de son Artificial Intelligence Act, première loi du genre à encadrer l'intelligence artificielle. Ce texte vise avant tout à s'assurer que les technologies développées sont sûres, transparentes et qu'elles respectent les droits humains fondamentaux. Il classe également les systèmes d'IA en fonction de leur niveau de risque, imposant des exigences plus strictes aux applications les plus sensibles, comme celles destinées aux enfants ou utilisées dans le cadre des processus de recrutement[21].

Et pour exploiter pleinement le potentiel et les promesses de l'IA, les entreprises de la région EMEA doivent se montrer tout aussi avant-gardistes. C'est cet esprit visionnaire qui leur permettra de transformer leurs business models dans de nombreux domaines : marketing, gestion des connaissances, ingénierie logicielle, etc.

En ce sens, la gestion du risque doit être intégrée en amont de toute initiative IA, et non après-coup. De même, le recours à un service de quantification du risque peut également aider à identifier les faiblesses et les écarts de conformité potentiels.

C'est la raison pour laquelle le Cybersecurity Assessment de Verizon comprend des tests d'intrusion Red Team s'appuyant sur des simulations d'attaque réelles, y compris autour de l'IA. Ces tests peuvent par ailleurs exécuter des programmes automatiques pour sonder les systèmes à la recherche de vecteurs d'attaque et de vulnérabilités, ou encore aider à la sélection de cibles.

En interne, Verizon a également mis en œuvre des mesures de gouvernance de l'IA. Les data scientists doivent ainsi faire contrôler leurs modèles d'IA, tandis que les grands modèles de langage (LLM) sont passés au crible pour éviter les éventuels biais et contenus abusifs.

Ces efforts s'inscrivent dans le cadre d'une action plus large pour une IA responsable. Ils font par ailleurs partie intégrante de nos services de gouvernance, risque et conformité (GRC), qui constituent l'un des piliers essentiels d'une approche de sécurité Zero Trust.

Face à l'ampleur de la tâche, les organisations devront coopérer si elles veulent combler les lacunes de la GenAI avant 2030. Des règles d'éthique aux cadres législatifs, les disparités des systèmes de gouvernance pourraient en effet creuser la fracture technologique et générer des vulnérabilités, avec de sévères répercussions dans des domaines allant de la cybersécurité à la croissance économique.

Cependant, grâce au framework « Secure-by-Design »[22], même les petites structures peuvent se lancer dans l'IA et l'innovation technologique avec des équipes IT compactes.

À travers le monde, 21 agences travaillent ainsi sous l'égide de ce framework pour aider les professionnels de l'IA à prendre des décisions conformes aux bonnes pratiques de cybersécurité tout au long du cycle de développement.

21. AI Act,. Shaping Europe's Digital Future, 30 juillet 2024. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
22. Secure by design | CISA. (non daté). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/securebydesign

L'avenir de la GenAI, entre innovation et sécurité

Si beaucoup voient dans l'IA le « grand égalisateur »[23] de demain, la réalité se révèle pour le moins plus nuancée. Dans la région EMEA, la plupart des acteurs publics sont en effet confrontés à une pénurie de talents et de compétences qui menace la sécurité de leurs citoyens.

C'est également le cas des entreprises, qui doivent pourtant agir dès maintenant pour quantifier les risques liés à l'IA[24]. Et comme souvent, l'exemple doit venir d'en haut. Le Comex doit s'emparer de cette question et impulser une véritable culture de la sécurité, plutôt que de déléguer cette responsabilité au seul RSSI.

Dans ce contexte, Verizon peut aider les entreprises à constituer une équipe pluridisciplinaire de pilotage de l'IA, chargée de poser les bases d'un développement encadré de la première application GenAI de l'entreprise. Cette transversalité se révèle en effet essentielle pour conjuguer innovation IA et cybersécurité.

Au cours des dernières années, nous avons par ailleurs mobilisé d'importantes ressources afin de mettre au point des outils d'IA répondant à des besoins quotidiens dans différents domaines : optimisation des performances réseau, identification des tendances, génération de demande et amélioration du service client.

Pour y parvenir, Verizon entraîne de vastes jeux de données à effectuer des tâches précises et clairement délimitées. En clair, l'IA est modelée pour répondre à des besoins fonctionnels et opérationnels spécifiques. De même, nous comprenons parfaitement les bénéfices et les risques en jeu.

Chaque jour, 70 milliards de points de données provenant de 29 000 sources différentes viennent enrichir nos systèmes d'IA avancés. C'est dire la complexité et l'ampleur de notre écosystème digital[25].

Enfin, nos prestations de conseil s'alignent sur les besoins propres à chaque entreprise. Nous élaborons ainsi des plans de défense solides, accompagnés de benchmarks et de rapports de sécurité détaillés, reposant sur des données fiables et des normes reconnues.

[23]E. Cosman, Cybersecurity Risk is the Great Equalizer. (non daté). https://gca.isa.org/blog/cybersecurity-risk-is-the-great-equalizer
[24]Cybersecurity Assessment (CSA). (non daté). Verizon Business. https://www.verizon.com/business/fr-fr/products/security/cyber-risk-management/governance-risk-compliance/cybersecurity-assessments/
[25]D. Meyer, Verizon's 70 billion network data points highlight genAI potential (and challenges), 8 février 2024. https://www.sdxcentral.com/articles/interview/verizons-70-billion-network-data-points-highlight-genai-potential-and-challenges/2024/02/

L'IA au service de la détection et de l'analyse des menaces

Ce dispositif nous permet d'utiliser l'IA pour mieux comprendre les méthodes des attaquants.

- Monitoring continu : les systèmes d'IA surveillent étroitement l'activité du réseau en continu, détectant des anomalies et des menaces qui pourraient facilement échapper à la vigilance humaine.
- Tests d'intrusion automatisés : ces tests simulent des attaques ciblant les systèmes informatiques, les réseaux ou les applications web afin d'identifier les vulnérabilités susceptibles d'être exploitées.
- Analyse du trafic : l'IA est capable de faire la distinction entre un trafic normal et un trafic suspect, améliorant ainsi la détection des cybermenaces les plus sophistiquées.
- Détection du phishing : en assimilant les caractéristiques des campagnes de spam et de phishing, l'IA permet de bloquer les e-mails malveillants de manière préventive.
- Identification des malwares : les outils d'IA analysent des échantillons de malware connus pour identifier de nouvelles variantes ainsi que des menaces zero-day encore inconnues.
- Sécurité des mots de passe : l'IA peut générer et recommander des mots de passe complexes difficiles à déchiffrer.
- Automatisation des tâches : l'IA permet d'automatiser les tâches répétitives. Les équipes de cybersécurité peuvent ainsi se concentrer sur des questions plus stratégiques.

Entreprises, clients et collaborateurs : tous ont à gagner de la GenAI. Dans la région EMEA, les initiatives dans ce domaine devraient non seulement rendre les entreprises plus compétitives, mais aussi offrir un cadre de vie plus sûr à tous les citoyens.

Pour en savoir plus sur nos solutions de sécurité IA, contactez votre conseiller Verizon ou appelez le +44 118 905 5000