Guide de cybersécurité

Les Défis D'UN Nouveau MONDE

L'IA générative et la cybersécurité : comment en tirer parti sans compromettre la vie privée et la conformité ?

Un guide cocréé avec un panel de CISO

Alliancy

elastic

Sommaire

Avant-propos

Vers une adoption maîtrisée de l'IAG

2024 sera une nouvelle fois l'année de l'intelligence artificielle. En particulier, après avoir été abondamment commentés ces derniers mois, les impacts de l'intelligence artificielle générative (IAG) sur les organisations vont pouvoir être véritablement constatés, et de nombreuses entreprises passeront leurs épreuves du feu de l'adoption et de la mise en œuvre de projets à l'échelle. En matière de cybersécurité, la démocratisation de l'accès aux *large language models* (LLM) ne manquera pas non plus de changer la donne.

Dans la course entre attaquants et défenseurs, les cybercriminels ne manquent jamais d'avoir un coup d'avance, profitant de toute innovation technologique pour prendre l'avantage. Cependant, ces outils peuvent également contribuer à autonomiser les équipes chargées de contrer les menaces. C'est l'un des points sur lesquels insistent les *chief information security officers* qu'Alliancy a rencontrés, dans le cadre d'un atelier organisé sur le thème de l'IAG, en partenariat avec Elastic.

L'occasion d'une discussion exploratoire sur la façon dont CISO et RSSI voient le sujet de l'IAG à leur porte. Mais sous quelles conditions une adoption réussie de ces pratiques et outils est-elle possible ? Cette question devient plus que jamais cruciale dans un contexte bien connu de tension, caractérisé par la pénurie de compétences et l'accroissement de la complexité des systèmes d'information, souvent associés à une vulnérabilité accrue. Qu'il s'agisse d'organisations d'importance vitale (OIV), d'acteurs publics ou de grandes entreprises opérant dans des environnements réglementés, ces organisations ne peuvent pas se permettre d'introduire l'IAG de manière improvisée.

Nos témoins ont d'ailleurs conscience des points faibles potentiels autour du sujet, notamment en ce qui concerne la protection des données et la gestion des « hallucinations » de la part de l'outil, pouvant entraîner des approximations préjudiciables, voire des erreurs directes. Les directeurs de la cybersécurité ont ainsi conscience que, pour être en mesure de profiter des avantages amenés par l'intelligence artificielle directement au niveau de leur métier, ils devront répondre à une gamme étendue de questions.

Nous avons synthétisé ici leurs convictions, interrogations et leurs axes de réponses.

Nous vous en souhaitons une agréable lecture.

Dorian Marcellin, rédacteur en chef

En pratique

L'intelligence artificielle générative transforme en profondeur le monde de la cybersécurité

Fin 2023, une dizaine de *chief information security officers* (CISO) d'organisations publiques et privées françaises se réunissaient au sein de la rédaction d'Alliancy, à l'invitation du média et de son partenaire, Elastic. L'occasion d'un atelier pour tracer les grands axes de préoccupation autour d'un sujet émergeant : l'impact de l'intelligence artificielle générative sur les métiers de la cybersécurité et leur environnement. Comme souvent dans l'univers de l'innovation *tech*, une réalité prévaut : la forte médiatisation du sujet IAG en 2023 a contribué à rendre difficile la distinction du « bruit » et du « signal ». Toutes les entreprises doivent communiquer d'une façon ou d'une autre sur le sujet, faire miroiter des engagements et des projets… tout en subissant bien souvent en réalité le caractère très soudain de ces thématiques pour celles et ceux qui n'ont pas d'équipes entières consacrées à la recherche en IA. Malgré tout, le marché lui, se positionne tous azimuts ; les offres commerciales de suites logicielles, intégrant d'une manière ou d'une autre l'IAG, se multipliant à l'envi, menées par les tenants Microsoft, Google et consorts. Dans ce contexte, sur quoi s'accordent *a minima* tous les CISO ? Qu'est-ce qui existe d'ores et déjà dans leur organisation et comment anticipent-ils les prochains mois ?

Un premier élément ressort clairement des échanges menés par la rédaction avec les CISO mobilisés : ils préfèrent voir l'arrivée de l'intelligence artificielle comme une opportunité pour améliorer leurs capacités, plutôt qu'une menace. Si les expressions liées aux risques cybers et à la protection des données, ainsi qu'à l'augmentation de la surface d'attaque sont bien citées, tous ont préféré, dès le départ, évoquer d'autres termes : accélération, gain de temps, assistant performant, facilitation des tâches, gains dus à l'automatisation… En l'occurrence, les professionnels de la sécurité ont bien conscience que l'intelligence artificielle est un facteur d'accélération majeur pour les cybercriminels en premier lieu et qu'ils doivent jouer avec les mêmes armes.

« Clairement ce que l'on voit, c'est que l'IA permet d'adapter ou de générer des codes pour faire évoluer la menace. […] Une population plus large d'attaquants va pouvoir profiter de ce levier, même sans connaissance préalable. L'intelligence artificielle générative abaisse la barrière d'entrée sur le marché des cyberattaques », témoigne ainsi Jean-Baptiste Fouad, *chief information security officer* de SFR Business & Wholesale (voir notre interview).

Accompagner le business dans l'aventure

Mais plus encore, les CISO veulent accompagner les business dans leurs usages croissants, en jouant au maximum leur rôle d'anges gardiens. « Tous les CISO vont devoir s'emparer des solutions d'IAG, bien sûr dans une logique de *attacker view* car les attaquants les utilisent déjà, mais également dans une logique d'accompagnement business parce que nos métiers vont les utiliser, pour faire en sorte que ces nouveaux usages soient sûrs. Il faut d'ores et déjà travailler à l'acculturation à ces nouvelles technologies au sein des entreprises avec le support des RH, pour préparer nos collaborateurs à l'évolution de leurs métiers avec l'IAG », souligne Richard Guidoux, VP, *cybersecurity director for B2B products & services* du spécialiste de la biométrie, de l'analyse de données et de la vidéo, Idemia. Lors de l'atelier, les CISO ne manquent d'ailleurs pas de souligner les enjeux en matière de formation et de formation continue, mais aussi les craintes de ne pas parvenir à embarquer efficacement les départements des ressources humaines dans ces transformations, notamment du fait des implications sur les modifications des tâches selon les postes, l'apparition de nouveaux métiers, ou plus globalement le changement de travail qu'implique une infusion ambitieuse de l'IAG à tous les niveaux.

Les changements s'annoncent nombreux également pour les CISO eux-mêmes, qui voient des opportunités variées pour leur travail quotidien. Générer des scénarios d'attaques potentiels ; améliorer les analyses comportementales ; générer des modèles pour la détection, la prévention, la réponse aux menaces ; traiter plus facilement de grandes quantités de données… sont autant de points mis en avant par les directeurs cybersécurité pour tracer leur avenir. Les outils intégrant l'IAG commencent déjà à être utilisés par les équipes sécurité. Plusieurs témoignages font état d'expérimentations et d'adaptations des usages quotidiens autour, par exemple, de l'offre Copilot de Microsoft, qui a l'avantage de venir se greffer à des outils bureautiques déjà utilisés par de nombreuses organisations.

« L'usage de Copilot de Microsoft pour les équipes de sécurité concerne déjà certains usages basiques, mais qui ont une valeur ajoutée évidente. Il faut le voir comme une sorte d'assistant, qui va aider à des tâches de création de contenus ou d'explications. Une équipe peut avoir de très bons analystes, mais qui gagneront beaucoup de temps grâce à l'IAG sur de tels usages pour transmettre plus facilement et rapidement des informations utiles », explique ainsi Benoît Herment, *group CISO* de Vinci.

Un assistant motorisé par l'IA au sein des SIEM *(security information management system)* et SOC *(security operation center)*

L'intérêt de l'outil est également mesuré à l'aune de sa capacité à générer plus facilement du code. « Cela fait près de 25 ans que je n'ai pas eu à développer moi-même, et pourtant j'arrive à faire des petits prototypes rapides très facilement avec un tel outil. On imagine bien le temps que peuvent gagner nos équipes en s'appuyant sur un tel assistant », lance un autre participant. Sophie Troistorff, directrice générale d'Elastic en France pousse l'analyse plus loin (voir notre interview) : « L'IAG peut permettre "d'augmenter" les personnes au sein des départements de la sécurité des systèmes d'information, par exemple en aidant de nouvelles recrues à devenir beaucoup plus rapidement opérationnelles. […] Par ailleurs, avoir un assistant motorisé par l'IA, au sein d'un SIEM ou d'un SOC, est également un moyen de faire la différence. En détection d'intrusion, l'IA peut aider en allant chercher les informations utiles dans une base de connaissance comme MITRE ATT&CK, afin de présenter les protocoles à appliquer et les réponses à déployer plus rapidement. »

Les participants à l'atelier reconnaissent cependant que ces gains n'iront pas sans une adaptation conséquente. Invité à témoigner sur le sujet de la sécurisation de l'IAG, le ministère des Armées en fait un thème central d'une approche pérenne, appelant à la mise en place, dans les organisations, de cadres stricts et d'une maîtrise des sujets émergents sur des domaines de développement précis, à l'image de ce que les armées elles-mêmes ont mis en place ces dernières années. Cloisonnement ; contrôle de l'accès à la donnée ; transparence et maîtrise des données qui alimentent les outils… font partie des fondamentaux à ne pas sous-estimer dans l'expérience de l'institution.

Un impératif dont les CISO ont bien conscience. « Il y a un parallèle très fort à faire avec les enjeux de la data, et la *data governance* que les organisations ont dû mettre en place pour cadrer cet usage. C'est une *"IA Governance"* qui doit maintenant s'installer au plus vite dans les entreprises, dont l'encadrement sera à la fois juridique et opérationnel », analyse Richard Guidoux.

Un argument partagé au sein de Vinci : « Une entreprise n'a certainement pas intérêt à attendre la fin de ses grands chantiers engagés sur la data pour déterminer une doctrine en matière d'IAG. Car la question clé derrière les usages qui émergent est : quel type de données pour quel type d'IA ? Cela implique une approche collective, réunissant les directions juridiques, data, RH, éthique, IT… », met en avant Benoît Herment. L'apparition de *task forces* mixtes dédiées au sujet depuis 2023 dans les grandes entreprises vise à déterminer ces directives IA. Mais les CISO le savent bien : celles-ci seront amenées à évoluer rapidement, car les outils eux-mêmes et leur capacité évoluent à très grande vitesse.

Trouver l'équilibre entre les positions extrêmes

Présent lors des échanges, Michel Juvin, expert cybersécurité et chroniqueur Alliancy, suit de près ces transformations. « Si l'on résume la situation, on peut dire qu'il est clair qu'utiliser l'intelligence artificielle va avoir de nombreux impacts positifs, mais que seul un contrôle strict permettra aux équipes sécurité de ne pas être dépassées. Entre les deux extrêmes qui consistent à vouloir bloquer complètement ces nouveaux usages, au risque de créer des contournements, ou au contraire de s'y ouvrir totalement à des fins d'innovation, mais en s'ouvrant ainsi à de nombreuses attaques potentielles – en particulier par *flooding* ou *data poisoning* – les organisations doivent trouver le juste milieu. »

Pour l'expert, il ne faut pas non plus sous-estimer les risques de dépendance qui vont se renforcer autour des principaux fournisseurs de capacités d'IAG, dans un contexte géopolitique et réglementaire particulièrement tendu. Enfin, il encourage à anticiper au maximum l'impact RH : « L'IAG connaîtra une deuxième phase d'accélération quand elle se diffusera plus largement dans les systèmes et plus encore quand elle atteindra les robots eux-mêmes. Il est donc nécessaire de développer une vision cohérente sur les compétences, les carrières, le travail des équipes pour l'ère de l'IA à venir. »

Entretien

Ce que doit savoir un CISO avant d'utiliser l'IAG

Après avoir participé à notre *workshop* sur les enjeux cybers de l'intelligence artificielle générative, Jean-Baptiste Fouad, *chief information security officer* SFR Business & Wholesale, différencie les problématiques auxquelles doivent faire face les directeurs cybersécurité français.

Quel regard portez-vous sur la maturité de la communauté cyber concernant l'intelligence artificielle générative en France ?

Le sujet est en ébullition depuis plus d'un an. Aucun responsable ne peut l'ignorer, ne serait-ce que parce que nous constatons de nombreuses personnes utiliser dorénavant des outils comme ChatGPT, y compris à des fins professionnelles et de manière assez chaotique… En matière de maturité, il manque clairement un cadre formalisé : on ne voit pas encore assez de directions des systèmes d'information qui mettent en œuvre une approche globale cohérente. Pour le moment, cela conduit à la multiplication d'usages de produits gratuits ou payants : chacun y va de son initiative. Certaines sociétés ont décidé tout simplement de bloquer les URL vers ChatGPT ou autre. Pourtant, sur le sujet, la sensibilisation vaut souvent mieux que le blocage, qui provoque des contournements. Certaines approches sont toutefois un peu mieux cadrées. Pour prendre un exemple, l'usage de Copilot, intégré à l'offre Microsoft quand on dispose des bonnes licences, est devenu assez prononcé dans le milieu cyber. Nous vérifions aujourd'hui si cela mérite une généralisation par rapport à nos besoins.

Voyez-vous l'adoption de l'IAG comme un facteur de menace ?

Si l'on prend le prisme du risque plutôt que celui de la productivité, clairement ce que l'on voit, c'est que l'IA permet d'adapter ou générer des codes pour faire évoluer la menace. Les *malwares* et le *phishing* en profitent déjà. En fait, c'est

Jean-Baptiste Fouad, responsable sécurité des systèmes d'information (RSSI) de SFR Business

là aussi un effet de démocratisation : une population plus large d'attaquants va pouvoir profiter de ce levier, même sans connaissance préalable. L'IAG abaisse la barrière d'entrée sur le marché des cyberattaques, un peu dans le même esprit que les script *kiddies* à l'époque. L'IAG dépasse cependant largement les scripts très limités qui sortaient de cette première forme d'automatisation. N'importe qui va pouvoir demander à l'IA : « Je veux un programme dans tel langage qui va… » et donc concevoir un code malveillant. On sort du prêt-à-porter pour aller vers du sur-mesure dans la création des menaces, et c'est beaucoup plus dangereux. Bien entendu, les principales IAG du marché sont protégées pour éviter ces abus en matière d'usages. Elles ne sont pas censées répondre à quelqu'un qui demanderait un code pour faire un *malware*. Toutefois, on dispose déjà de nombreux exemples pour contourner ces limites et obtenir des recettes et contenus nuisibles ou illégaux. Et par ailleurs, les IAG vont dorénavant fleurir comme des pâquerettes. Assez vite, un bon nombre d'entre elles ne seront plus bridées de la sorte.

Est-ce que vous croyez en un RSSI augmenté par l'IAG ? Quelles en seraient les caractéristiques ?

C'est un sujet à double tranchant, comme tous les usages IA. Si vous comptez uniquement sur l'IAG pour vous aider à prendre vos décisions, vous allez à la catastrophe. Les risques d'erreur, les approximations, sont réels.

Les phénomènes d'hallucination sont bien documentés. Un RSSI doit donc avoir de très bonnes bases et des convictions pour pouvoir utiliser ces outils à bon escient. Pour le RSSI, l'IAG a vocation à être un conseiller et un *sparring partner*. Elle peut challenger, conforter, forcer à se poser des questions.

Mais à l'inverse, si vous l'utilisez pour découvrir un sujet que vous connaissez mal, vous allez droit dans le mur. Quand vous connaissez le résultat attendu, qu'il est objectivement vérifiable, l'IAG est très utile. Quand il y a une dimension moins contrôlable, plus subjective, biaisée… soudainement, la valeur à en tirer est moins évidente et l'usage devient plus complexe. Demander à une IAG quel est le meilleur outil à utiliser, c'est ainsi très différent que de lui demander de pointer les différences entre plusieurs d'entre eux. Enfin, dernier point important : plus les IAG sont généralistes, comme celles actuellement sur le marché, plus il est difficile d'avoir un usage satisfaisant. Il faut donc une forte spécialisation verticale des outils et un peu de recul. Une IA spécialisée sur la *cyber threat intelligence* par exemple, de façon à éviter les hallucinations, est le genre d'outil qui nous rapprochera du RSSI augmenté. En attendant, l'IAG peut nous aider à créer des contenus plus facilement, pour simuler des scénarios par exemple. Mais il faudra rapidement aller plus loin, pour automatiser les déroulements en la couplant à d'autres systèmes. Ces interactions seront la clé de la valeur apportée, pour sortir des visions statiques, un peu artificielles, et provoquer des situations dynamiques. Imaginez une IA spécialisée sur la simulation de cybermenaces qui interagira avec une autre spécialisée sur le fonctionnement des systèmes industriels : c'est à partir de là que de grands progrès pourront être faits.

Quel est votre avis sur la façon dont les éditeurs de cybersécurité s'emparent de la question aujourd'hui ?

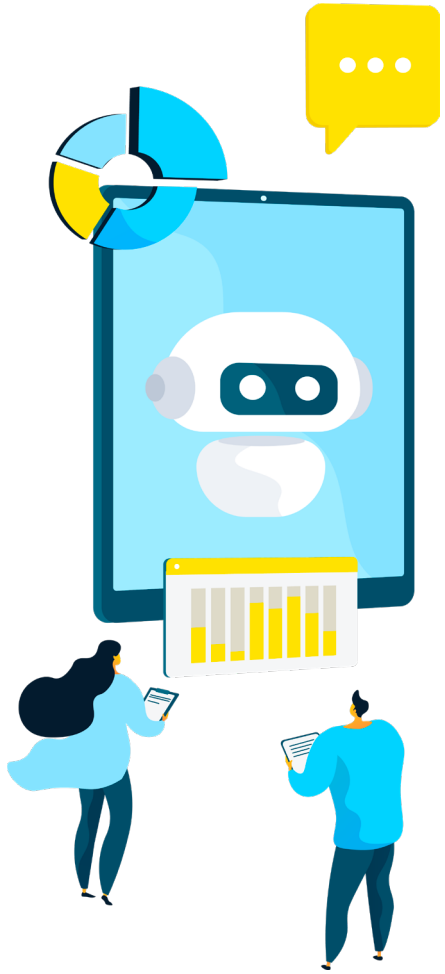
Le sujet est encore trop neuf. Je ne vois pas d'IAG vraiment dédiée au monde du multimédia et de l'internet, et entraînée sur des données spécifiques en ce sens en ce début 2024. Toutefois, cela va arriver vite. Nous allons sans doute avoir un copilote cyber. Toute la question est de savoir s'il va être nécessaire d'attendre quelques mois seulement ou plutôt quelques années pour que la promesse soit au rendez-vous. D'autres secteurs comme la pharmacie avancent vite, mais on constate que cela leur demande un travail énorme sur la data, la puissance de calcul et les algorithmes, pour en arriver là. La puissance de calcul et les algorithmes progressent en permanence, mais pour le moment, la principale difficulté pour les entreprises utilisatrices comme pour les éditeurs, reste le sujet des données. Il en faut beaucoup et surtout, il faut que la qualité soit là.

Comment garder la maîtrise des outils IAG ?

La vraie question est celle de l'IAG de confiance. On se souvient tous des IA apprenant sur Twitter en *open bar* et devenues complètement racistes et sexistes en quelques jours. Le risque de transformation et de biais au sein d'une IAG apprenante est clair. C'est pour cela que la tentation était grande chez les spécialistes de l'IA pendant longtemps d'agir uniquement sur des données complètement maîtrisées. Le travail de contrôle va donc devoir se concentrer sur la façon dont ces IA s'alimentent. Si l'IA s'ouvre, il faut que le contrôle soit à l'avenant. Le risque de *data poisoning* est réel. Pour l'éviter, on sera aussi bien sur un travail humain que sur une évolution des algorithmes eux-mêmes.

Dans ce contexte, l'autre point à prendre en considération est que ces IAG fonctionneront *a priori* dans le cloud. Mais à ce titre, les risques d'un point de vue cyber restent assez classiques. La préoccupation sera moins la disponibilité que l'intégrité. Que va-t-il se passer si certaines données sont modifiées, supprimées, sans la connaissance du client ? Plus encore, la préoccupation peut être sur la confidentialité. Les jeux de données qui devront être dans le cloud pour nourrir l'IA pourraient être en risque dans le cadre du *cloud act* ou de FISA (la loi *foreign intelligence surveillance act* des États-Unis, renouvelée il y a quelques mois, N.D.L.R.). Mais ce n'est pas si différent de ce à quoi nous sommes déjà confrontés pour de nombreux autres outils cloud.

Selon moi, le problème majeur est plutôt celui de l'effet boîte noire et du manque global de transparence autour de ces outils. Les éditeurs d'IAG spécialisée vont développer en PaaS, donc sur le cloud, mais ce sont eux qui auront la maîtrise des sujets, depuis le code jusqu'à la donnée. En ce sens, ce sont bien aux éditeurs d'apporter des gages de confiance, plus qu'aux *cloud providers* eux-mêmes.



Entretien

Face aux cyberattaques, des opérateurs cyber-augmentés par l'IAG

Elastic, la société leader en *search analytics*, a été saluée en 2023 comme l'un des fournisseurs de technologies clés dans la ruée vers l'or mondiale des entreprises de l'intelligence artificielle générative (IAG). Sophie Troistorff, directrice générale d'Elastic France, a coanimé avec Alliancy notre atelier sur l'IAG et la cybersécurité. Elle fait le point sur les questions que les entreprises doivent urgemment se poser sur le sujet.

Pourquoi vous paraît-il important aujourd'hui de faire un focus sur la rencontre entre les usages issus de l'IAG et le monde de la cybersécurité ?

Depuis dix-huit mois, l'intelligence artificielle générative est dans l'esprit de tous les dirigeants. Mais au-delà des enjeux business, tous ne mesurent pas à quel point l'IAG peut être à la fois un risque et une opportunité pour la cybersécurité de leur organisation. Selon leurs choix, la balance penchera d'un côté ou de l'autre. Il est important de comprendre que cette question de fond présente deux aspects bien différents. D'abord, il est certain que l'intelligence artificielle générative peut apporter beaucoup aux usages cybers. Cependant, il faut aussi prendre en compte le fait que des outils et pratiques de cybersécurité sont également nécessaires pour permettre une bonne adoption de l'IAG de manière à être conforme aux réglementations et respectueux de la sensibilité des données. On ne peut pas ignorer l'un ou l'autre.

Dans les discussions menées avec les directeurs cybersécurité que nous avons réunis, qu'est-ce qui vous a le plus marqué ?

Les approches sont encore assez exploratoires. Nous avons noté que les entreprises allaient assez naturellement vers un cas d'usage central pour leurs spécialistes du numérique : la génération de code grâce à l'intelligence artificielle, pour la rendre beaucoup plus rapide. C'est un usage générique, mais qui peut bien s'appliquer au monde de la cybersécurité. Les *chief information security officers* (CISO) en ont conscience et veulent s'organiser pour accompagner le mouvement au sein des DSI, mais aussi pour leur propre équipe le cas échéant.

Ils ont en tête qu'il existe une gradation de cas d'usage, qui n'ont pas tous les mêmes implications en matière de gains de productivité, mais aussi de sécurité. Les plus basiques consistent à utiliser l'IAG comme une sorte de super moteur de recherche, pour fournir des synthèses ou des explications rapides, souvent sur des sujets généralistes. Cela devient plus sophistiqué quand l'expertise métier entre en jeu, avec des processus complexes à prendre en compte. Enfin, et c'est le cas de la génération de code, tout un pan des nouveaux usages consiste à créer un nouvel item, par exemple un morceau de code, qui, à son tour, produira un service. En la matière, les questionnements sur la protection de l'information et la propriété intellectuelle deviennent beaucoup plus aigus.

Chaque entreprise aura des approches différentes, mais la réalité pour les CISO, c'est que ces différents cas d'usage vont entraîner des conséquences sur les données qui seront exposées dans les systèmes, la façon dont elles le seront et la manière dont les utilisateurs accéderont aux systèmes en question. Cela pose fondamentalement une question de cybersécurité. Or, quelles sont les entreprises qui peuvent dire qu'elles sont prêtes à mettre en place une sorte de « jumeau cyber » calqué sur le parcours utilisateur et le parcours de la donnée liés à ces cas d'usage naissants ? Très peu à ce jour, car leur priorité est déjà de définir la valeur qu'elles peuvent tirer de ces nouveaux parcours.

En quoi voyez-vous le plus l'IAG changer le quotidien des CISO à court terme ?

L'utilisation de l'intelligence artificielle s'inscrit dans la dynamique généralisée de professionnalisation des attaquants et de croissance des risques cybers. En face, du côté des entreprises, nous assistons à une complexification des systèmes et à une pénurie de compétences disponibles : l'asymétrie se creuse. Mais l'intelligence artificielle peut aider à rétablir un certain équilibre. Elle peut permettre « d'augmenter » les

Sophie Troistorff, *country manager* de Elastic

personnes au sein des départements de la sécurité des systèmes d'information, par exemple en aidant de nouvelles recrues à devenir beaucoup plus rapidement opérationnelles. Il faut ainsi revoir l'*onboarding* et la formation en ce sens. Par ailleurs, avoir un assistant motorisé par l'IA, au sein d'un SIEM ou d'un SOC, est également un moyen de faire la différence. En détection d'intrusion, l'IA peut aider en allant chercher les informations utiles dans une base de connaissance comme MITRE ATT&CK par exemple, afin de présenter les protocoles à appliquer et les réponses à déployer plus rapidement. Aller plus vite dans la réponse des entreprises aux menaces, cela doit devenir le B.A.-BA de la cyber avec l'IA, car on a surtout besoin de stopper les attaques et limiter leurs conséquences (fuites de données, indisponibilité des SI…).

Imaginez-vous d'autres cas d'usage accessibles ?

Dans le cadre de l'entraînement et des tests de cybersécurité, les usages génératifs permettent aussi de changer la donne en matière de simulations d'attaque et de simulations de réponse à ces attaques. C'est plus sophistiqué, mais cela va devenir rapidement une réalité répandue pour les *red/blue teams*.

À quoi va-t-il falloir faire attention pour que ces nouveaux usages d'IAG en cybersécurité changent vraiment la donne ?

Quand on parle de définir un « opérateur cyberaugmenté », une des notions centrales va être l'accès de celui-ci à la connaissance et, derrière cela, la nature de la base de connaissance. Il faut donc s'interroger sur la capacité d'une organisation à collecter et stocker les données pertinentes pour nourrir l'IAG, mais aussi sur la nature des connexions nécessaires entre celle-ci et des systèmes externes. À quel point le système de sécurité est-il donc ouvert, scalable, réactif… pour avoir un niveau de réponse pertinent ?

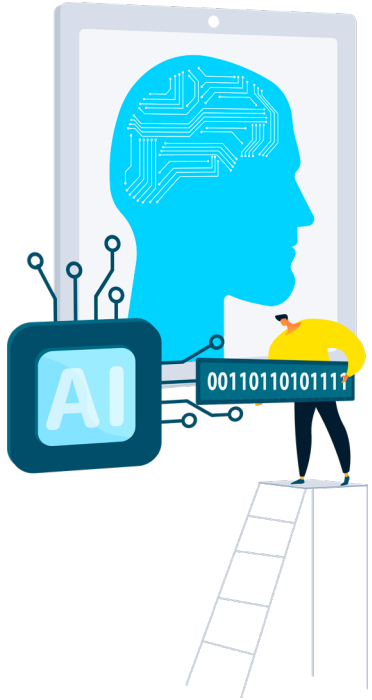
Ces critères sont au cœur de ce qui va faire la réussite ou l'échec d'un outil technologique appliquant l'IAG à la cybersécurité. Notre contexte cyber est qu'il existe de plus en plus de signaux faibles, dans une vaste mer d'informations hétéroclites et distribuées, parfois difficiles à ingérer. Des routines IA peuvent déjà en sortir des alertes, mais il faut pouvoir faire le tri dans ces alertes ; et savoir bâtir un cycle qui nourrit également l'IAG, avec un moteur performant. Ces dernières années, la sophistication de la recherche vectorielle (*vector search*) a permis de faire beaucoup de progrès en ce sens, mais l'alimentation de la base de connaissance doit rester un point d'attention majeur.

Quelles mesures de contrôle mettre en place pour éviter d'éventuels problèmes générés par l'usage de l'IAG au sein d'une entreprise ?

En gagnant en maturité, les entreprises vont sortir du simple usage d'un LLM sur un corpus de données public, et aller explorer des corpus verticaux formés par leurs propres données et savoir-faire, qui ne sont pas exposés au public sur internet : leurs données propriétaire. L'exploitation de ces corpus de données avec l'IA fait rentrer dans le monde de la protection de la donnée et de la propriété intellectuelle, même quand les données ne sont pas forcément sensibles… En effet, les entreprises ne vont pas créer chacune leur propre *large language model* (LLM). Elles vont être amenées à utiliser des outils, et bien souvent dans le cloud car leurs besoins de puissance de calcul vont devenir exponentiels. Le besoin de maîtrise reste donc évident. Nous ne sommes pas loin des questions que les entreprises se posent déjà sur d'autres usages cloud. Qui accède à quoi ? Qui chiffre et déchiffre ? Où ? Le questionnement important est de comprendre comment sont exposées les données et comment fonctionnent les LLM non éduqués sur internet. Est-ce qu'on sait être rapide, pertinent, scalable, malgré le fait qu'on ne soit pas sur cette alimentation internet, type ChatGPT ? C'est pour répondre à ces questions qu'Elastic travaille sur ces sujets depuis plusieurs années, avec ces technologies.

Quelles transformations avez-vous connues chez Elastic du fait de la démocratisation de l'IAG dans le monde ?

Mener une adaptation ambitieuse à l'IAG a été très tôt un moteur pour notre stratégie. Nous avons intégré le meilleur de la recherche avec le meilleur de l'IA pour créer des solutions d'analyse plus performantes, en temps réel, sécurisées et qui tirent parti de l'ensemble de vos données. Nous ne sommes pas un éditeur qui génère des LLM : nous proposons des outils de recherche qui permettent aux LLM d'accéder aux données de façon rapide, pertinente et à l'échelle. La combinaison est donc intéressante : nos outils sont éprouvés et nous avons maintenant des cas d'usage IAG qui tournent avec nos solutions. Il y a quelques mois, nous avons par exemple annoncé la sortie d'Elastic Relevance Engine, qui fait la connexion entre le réceptacle Elastic pour que les utilisateurs d'Elastic puissent exposer leurs données propriétaire aux LLM, en toute sécurité. C'est un axe fort de génération de valeur pour les mois à venir, par rapport à la situation que je décrivais plus en amont.



À propos

elastic

Elastic permet à quiconque de trouver les réponses dont il a besoin en temps réel, en utilisant toutes les données client, à grande échelle. Elastic propose des solutions complètes basées sur le cloud pour la sécurité, l'observabilité et la recherche, construites sur Elasticsearch, la plateforme de développement alimentée par l'IA, utilisée par des milliers d'entreprises, dont plus de 50 % des entreprises du Fortune 500.

Pour plus d'informations, rendez-vous sur : https://www.elastic.co/fr/

Alliancy
LE MAG NUMÉRIQUE ET BUSINESS

Média sur la transformation numérique des entreprises, engagé en faveur du « plus forts ensemble », Alliancy sélectionne pour vous les témoignages et les retours d'expériences de femmes et d'hommes actifs dans une dynamique d'innovation. Vision stratégique, gouvernance et modes d'organisation, utilisation de la donnée, enrichissement et animation d'écosystèmes (innovation, ressources humaines, systèmes d'information, finances et achats…), cloud, sécurité et pilotage du système d'information… Nous nous intéressons à ces différents leviers de la transformation pour qu'ils s'invitent peu à peu dans votre quotidien. Stimulez votre curiosité, gagnez du temps et identifiez les clés de la réussite de votre entreprise.

alliancy.fr

La collection des guides : *Les défis d'un nouveau monde*

Dans un monde plus incertain, un nouveau chapitre de transformation s'est ouvert pour les entreprises. De nouvelles questions se posent et pour être efficaces, nous devons y répondre ensemble.

C'est entre pairs et *faiseurs* que l'on apprend beaucoup, dans la confrontation de nos idées que l'on avance, pour répondre aux défis d'un monde que le numérique doit aider à rendre plus éthique et inclusif.

Ces guides sont réalisés autour d'une question d'actualité, suite à un échange entre pairs, où nous avons pu confronter les pratiques et enrichir ensemble des scénarios d'action.

Alliancy

Alliancy - 32, rue des Jeûneurs - 75002 Paris
SARL au capital de 167 500 €
792 635 138 R.C.S. Paris
alliancy.fr
Directeur de publication : Sylvain Fievet
Coordination rédactionnelle : Dorian Marcellin
Journalistes : Dorian Marcellin
Design graphique : Coralie Fau
Relecture : Emmanuel Cauchois - Le style de l'ours
Février 2024

Toute reproduction des textes publiés dans ce carnet est interdite sans autorisation explicite de la rédaction.
Pour tout renseignement, vous pouvez adresser vos questions à l'adresse suivante : redaction@alliancy.fr