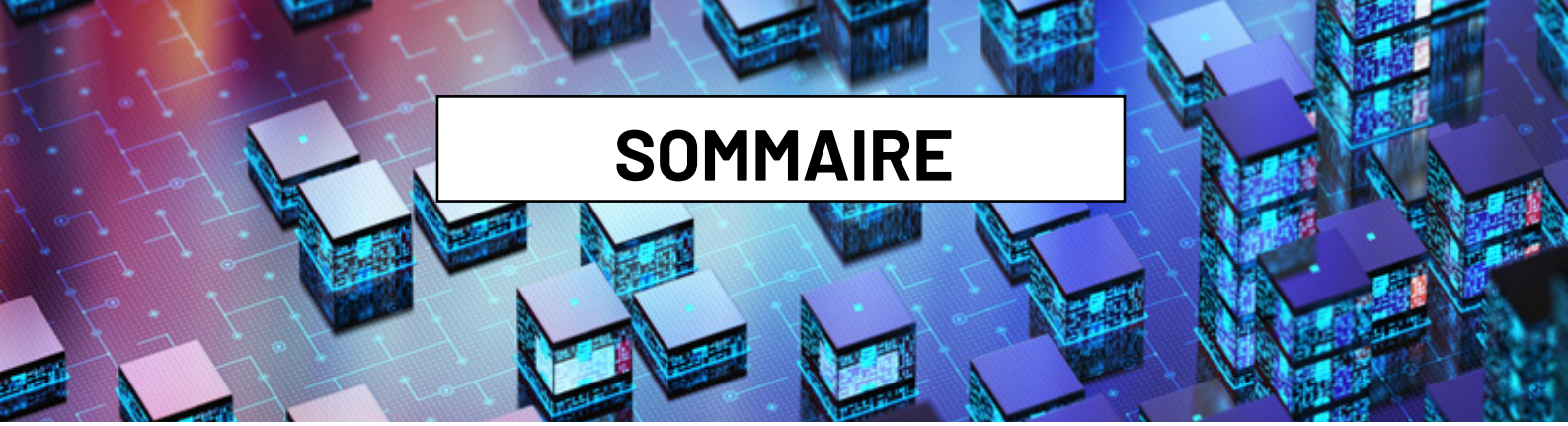
Synthèse

L'intelligence artificielle, potion et poison du management des risques cyber



SOMMAIRE

A propos de Numeum

Numeum est l'organisation professionnelle de l'écosystème numérique en France. Elle représente les entreprises de services du numérique (ESN), les éditeurs de logiciels, les plateformes et les sociétés d'Ingénierie et de Conseil en Technologies (ICT). Numeum rassemble plus de 2 500 entreprises adhérentes qui réalisent 85% du chiffre d'affaires total du secteur. Présidée par Véronique Torner, Numeum se fixe trois priorités : les territoires, pour accompagner les adhérents en région, les compétences, pour répondre aux défis de la mixité et de l'attractivité et le numérique responsable, pour accompagner et soutenir le développement d'un écosystème numérique dans une trajectoire d'impact positif sur le plan économique, social, sociétal et environnemental à l'échelle européenne, nationale et locale.

Numeum est membre de la fédération Syntec. Le secteur du numérique représente 65 milliards d'euros de chiffre d'affaires et 661 000 employés en France.

A propos d'Eurocloud

EuroCloud France est la branche française de l'organisation européenne EuroCloud, premier réseau d'acteurs du Cloud en Europe avec 1500 entreprises membres réparties dans 31 pays.

Objectif : favoriser le développement du cloud computing en France par les acteurs et les usages

· Des commissions qui expliquent, proposent, explorent.
· Les Etats Généraux du Cloud, chaque année depuis 2006 intégrés depuis 2015 au sein de la Cloud Week Paris.
· Un lieu de rencontre et de partenariats
· Les trophées du Cloud depuis 2007
· Des actions d'informations sur le terrain

Qui sont les membres d'Eurocloud France ?

· Acteurs ou futurs acteurs du Cloud Computing
· Editeurs, hébergeurs, Constructeurs, Telecom, Intégrateurs, VARs, SSII, Consultants, Grossistes
· De toute la France

EDITO

Nolwenn Le Ster, CEO de Capgemini Cybersécurité, Présidente de la Commission Cybersécurité de Numeum

Les récentes avancées de l'intelligence artificielle notamment génératives conduisent à réinventer notre manière d'appréhender le risque cyber. La réinventer afin de parer la massification et la complexification des attaques qu'elle permet, mais également afin de découvrir et développer de nouvelles méthodes d'analyse et de défense, et renforcer notre résilience collective notamment grâce à la sensibilisation qu'elle facilite.

La confiance dans le numérique, dont la cybersécurité constitue un pilier fondamental, est une des priorités de Numeum, dont j'ai l'honneur de présider la Commission Cybersécurité. En réunissant 40 des meilleurs experts en cybersécurité et en IA de nos entreprises adhérentes, et en publiant la présente synthèse, Numeum a souhaité contribuer à faire avancer l'intelligence collective et à augmenter le niveau global de maturité cyber de nos entreprises dans un contexte d'accroissement des cyberattaques. Cette synthèse ouvre de nombreuses questions, et nul doute que Numeum animera ou contribuera à d'autres travaux dans le domaine dans les prochaines semaines.

EDITO

Eric Melki, Président de la Commission Cybersécurité EuroCloud et Vice-Président EuroCloud

Nous le savons bien, toutes les grandes découvertes et innovations sont à la fois porteuses de promesses et d'espoir mais également de doutes et de peurs pouvant faire craindre à des dérives comme l'avènement de modification de l'ordre mondial voire de grandes catastrophes.

L'IA comme la Cyber figurent parmi les enjeux les plus importants auxquels les entreprises doivent faire face à court terme. Les perspectives et les promesses de l'IA sont immenses et nécessitent une réaction très rapide et concertée face à l'extrême violence liée à son introduction au sein de nos sociétés.

L'IA permettra au pirate informatique d'être plus précis et plus ciblé. Il pourra industrialiser ses stratégies et procéder à des attaques en masse.

De même et grâce à l'IA, les équipes de Cybersécurité seront plus réactives et pourront anticiper des attaques sans démultiplier les moyens techniques et humains.

L'Intelligence Artificielle, la Cybersécurité et le Cloud Computing sont trois notions intimement liées. EuroCloud se positionne avec l'ensemble de ses adhérents en tant qu'acteur majeur sur l'ensemble de ses questions.

NUMEUM CAMP CYBER
IA : potion et poison du management des risques cyber

L'explosion des usages de l'intelligence artificielle, qu'elle soit générative ou non, soulève des questions légitimes quant à aux conséquences sur la cybersécurité des entreprises. Cette technologie constitue tout aussi bien une menace en termes stratégiques, défensifs et de gestion des données qu'une opportunité sous la forme de leviers de croissance ou d'opportunités de sensibiliser et d'accompagner le public.

Le Numeum Camp Cyber du 5 décembre 2023, organisé avec EuroCloud France, a rassemblé professionnels et experts de la cybersécurité et de l'IA afin de conduire une réflexion commune à propos de l'utilisation de l'intelligence artificielle au sein des entreprises. Selon les termes introductifs de Nolwenn Le Ster, présidente de la Commission Cybersécurité de Numeum et Directrice des activités cybersécurité de Capgemini, l'objectif est de livrer une contribution positive à l'ensemble de l'écosystème.

De cette réflexion naît naturellement un double constat légitimant l'existence de cette réflexion. L'intelligence artificielle et son utilisation désormais répandue comporte, de fait, non seulement des opportunités mais également des menaces pour le management des risques cyber des entreprises.

Management des risques de cybersécurité : les risques et menaces liés au déploiement de l'IA

Principal enjeu lié au déploiement et à l'utilisation démocratisée de l'intelligence artificielle, en particulier générative, la généralisation des attaques et l'augmentation de la volumétrie de ces dernières sont des préoccupations majeures.

L'apport de la technologie dans la production de code informatique va rendre ces attaques plus simples et plus rapides (et potentiellement accroître l'appétit de "script kiddies", ces néophytes qui, avec peu de connaissances en cybersécurité, tentent d'infiltrer des systèmes en se servant de programmes efficaces et simples d'utilisation). On risque donc d'assister à une croissance exponentielle des attaques face à des défenseurs parfois insuffisamment préparés. Cette agilité rendue possible par l'IA permettant de démultiplier l'impact d'attaques pourtant techniquement simples.

En corollaire, concernant les LLM non censurés ou détournés, des scénarios d'attaque particulièrement malins pourraient être mis sur pied moyennant l'utilisation de ressources informatiques importantes procurant notamment une vitesse de calcul conséquente. L'IA générative peut donc servir pour attaquer, mais également pour identifier de nouvelles vulnérabilités. A terme, il n'est pas exclu d'imaginer par exemple l'émergence

d'un botnet capable d'alimenter ce type de LLM. Des services similaires à un "DarkGPT" pourraient alors prendre de l'ampleur et mettre en risque bon nombre d'institutions, de citoyens et d'entreprises. La vulgarisation de cette technologie entraîne indubitablement une massification des attaques.

Ce constat est également applicable s'agissant des attaques ciblant les utilisateurs eux-mêmes. On pense naturellement à l'arrivée de phishing de meilleure qualité (avec de nouveaux scénarios encore plus efficaces et peu voire pas de faute d'orthographe) ou au spearphishing augmenté (une variante d'hameçonnage permise par des techniques d'ingénierie sociale qui se concentre sur un nombre limité d'utilisateurs dont le message serait fortement personnalisé grâce à l'IAG).

L'augmentation des attaques, couplée à leur automatisation et à leur complexification sont donc des aspects qu'il convient d'appréhender dans le cadre de son management des risques cyber. L'utilisation de l'IA par les cyberattaquants est ainsi malheureusement susceptible de renforcer la maxime voulant que « les criminels sont meilleurs en attaque que les entreprises en défense ».

L'utilisation des données d'entrainement, une menace à ne pas négliger

L'une des menaces majeures de l'utilisation de l'IA pour le management des risques cyber concerne le fait que les données d'entraînement, c'est-à-dire les données utilisées pour alimenter et faire fonctionner les services d'IA générative, sont susceptibles d'être à leur tour exploitées par des attaquants. En ce sens, les données des entreprises se trouvent davantage exposées, et les données dérobées risquent d'être exploitées à dessein, soit en ciblant directement l'entreprise, soit en établissant des scénarios d'attaque génériques à partir des données subtilisées.

Par effet domino, si le coût de la donnée est plus faible, de nombreux attaquants potentiels seront à même d'y accéder, et les experts de Numeum et EuroCloud y voient la possibilité de voir les services liés au dark web se développer. Aussi, tout comme la génération de code malveillant est plus simple et plus rapide, l'IA est entrainée sur davantage de données et renforce sa capacité à générer des lignes de code puissantes. En somme, les modèles s'entraînent et se renforcent à force d'être utilisés, également du côté des attaquants.

Il est donc primordial que chaque éditeur de LLM sécurise au mieux ses algorithmes et les jeux de données issues de l'utilisation des LLM.

Enfin, parmi les risques liés aux données, il est évident que le sujet de la souveraineté risque de s'inviter aux débats des régulateurs spécialisés dans les sujets numériques. A court terme, si les utilisateurs d'IA génératives n'ont pas conscience de la potentielle fuite de données qu'ils engendrent, certaines informations passeront inévitablement dans d'autres mains.

Le numérique de confiance : éthique et explicabilité

Pour qu'elle puisse être utilisée en toute sérénité, une technologie doit pouvoir susciter la confiance auprès de ceux qui l'utilisent. Le sujet du numérique de confiance est donc clé dans la mesure où il s'avère double. Il recouvre non seulement en premier lieu la confiance que l'on accorde à l'intelligence artificielle et aux résultats qu'elle fournit mais également la manière dont cette dernière peut expliciter les fruits qu'elle produit.

Que ce soit du côté de l'attaquant ou du défenseur, cette question est centrale car la technologie ne doit pas pouvoir leur échapper. C'est pourquoi il est capital que soit instaurée une explicabilité des résultats produits par l'IA, en particulier générative, afin d'éviter la création d'un effet « boite noire ». A ce jour, certaines décisions, certes valides, ne sont pas encore explicables par une IA ou un humain.

Si ce risque n'est pas pris à sa juste mesure, des cas de corruption de l'intelligence artificielle

pourraient être à prévoir. On pense par exemple à un outil censé superviser un ensemble de capteurs industriels, qui pourrait dysfonctionner en reconnaissant certains patterns qui lui semblent familiers. Pour éviter ces effets de bords, chacun s'accorde à dire qu'à l'heure actuelle, il demeure complexe de vérifier, sinon d'attester par rétro ingénierie qu'une décision prise par l'IA n'est pas corrompue.

A ce questionnement s'ajoute naturellement le besoin d'adjoindre une éthique dans la manière dont la technologie est alimentée. Si cette éthique est nécessairement politique, elle reste nécessaire selon les experts d'EuroCloud et de Numeum.

Un manque de compétence à combler

Nombre d'experts apparentent l'émergence de l'intelligence artificielle avec l'arrivée du Web, des premiers moteurs de recherche robustes ou des smartphones. Toutefois, la rapidité avec laquelle l'IA arrive au sein des entreprises demeure inédite. Pour que chacun prenne la mesure de l'importance du mouvement à l'œuvre et soit accompagné de manière adaptée, il convient donc d'agir en termes d'explicabilité (voir supra) mais également d'agir sur l'intelligence commune et les compétences.

L'utilisation de l'IA et notamment générative sans accompagnement, sensibilisation ni acculturation constitue un terreau favorable aux risques cyber. L'Europe se doit non seulement de former ses talents à la technologie mais également les sensibiliser à l'utilisation et à l'impact que cette dernière est susceptible de provoquer.

L'explosion de l'utilisation des LLM, corrélée à leur popularité a pris de court les systèmes de formation classiques. Pourtant, le besoin demeure important pour les entreprises de recruter des personnes capables de comprendre les enjeux de sécurité conséquents à l'utilisation de l'IA générative.

A terme, de nouveaux profils métiers sont ainsi appelés à émerger, qu'ils soient séniors ou juniors. Des experts cyber, rompus à l'IA seront à même de comprendre ce que la technologie est susceptible de créer, et éventuellement d'industrialiser de nouveaux process. Aussi, des profils d'opérateurs d'IA qui ne disposent pas de compétences spécifiques en matière de script vont se faire plus nombreux dans les organisations. Pouvant être recrutés à des niveaux de formation de type Bac+2 ou +3, ces derniers pourront travailler sur des éditions de nouveaux prompts et contenus.

Le Shadow IT : la première porte d'entrée pour les vulnérabilités ?

Enfin, dernier risque, mais non des moindres, figure l'utilisation faite par les collaborateurs de la technologie. L'usage sans autorisation ou sans reporting aucun auprès des instances compétences (DSI, RSSI…) peut aboutir à la création de nouvelles vulnérabilités par exemple liées à l'injection de données sensibles au sein d'outils d'IA générative.

Management des risques de cybersécurité : les opportunités que permet l'IA

Si l'intelligence artificielle représente une menace pour les organisations, elle se présente également comme une formidable opportunité à bien des égards et notamment en cybersécurité. En ce sens, l'arrivée de la technologie emporte un volet relatif à l'éducation de chacun pour le moins conséquent.

Il convient donc de faciliter la compréhension des outils de management de la cybersécurité. Pour y parvenir, l'un des remèdes structurants est, sans conteste, celui de la sensibilisation en augmentant notamment le parcours pédagogique des utilisateurs. Des questionnaires construits ou enrichis par l'IA peuvent ainsi retracer plusieurs points consécutifs à l'usage de la technologie (utilisation de la base de connaissance, temps d'exposition, niveau de criticité des éléments utilisés…)

L'acculturation des collaborateurs semble constituer un élément clé de la réussite de l'utilisation de la technologie au sein de l'entreprise, a fortiori des IA. Cet effort peut notamment être réalisé au moyen de l'intelligence artificielle elle-même en tant qu'appui. Les outils LLM peuvent en effet formuler des conseils et des préconisations pertinentes.

L'idée est donc, selon les experts d'EuroCloud et Numeum, de favoriser l'acculturation en formant les utilisateurs en continu par des moyens simples (comme la gamification par exemple). Ces derniers doivent ainsi être sensibilisés aux enjeux relatifs à la technologie et aux points mentionnés dans la partie abordant les risques. Pour y parvenir, un leadership fort doit être instauré dans l'entreprise ou auprès des clients concernés. Par exemple, un e-mail douteux doit automatiquement créer un état d'alerte chez le possesseur d'une boîte électronique, une mise à jour d'OS réalisée rapidement, une alerte de sécurité traitée avec célérité.

Cette acculturation par la gamification peut tout à fait être réalisée de manière continue, par exemple au moyen d'outils utilisant l'IA proposant des parcours personnalisés pour chaque type de poste, de fonction, de profil, avec à la clé des recommandations spécifiques relatives à la cybersécurité. De nombreux professionnels proposent dès à présent des interfaces simples d'utilisation pour véritablement « accueillir » tous les profils, sans instaurer de barrière de compréhension. Ces services s'accompagnant généralement de contenus qualitatifs et simples rappelant que des outils sont à la portée de l'ensemble des collaborateurs.

L'IA semble donc constituer un réel levier dans l'accompagnement vers un niveau de maturité cyber satisfaisant.

Vers de nouveaux concepts de défense

L'intelligence artificielle, sous toutes ses formes, représente un moyen de générer de nouveaux concepts de défense ou de la génération de prévention d'incident. Aussi, une IA peut dans certains cas détecter plus rapidement qu'un humain la nature d'une cyber-attaque, la comprendre et potentiellement la parer ou récupérer les données perdues.

Dans cette optique, cette technologie va amener de nouvelles capacités d'analyse. On pense notamment à l'extension des bases de sécurité dans l'écosystème de l'IA, en tirant parti des protections de l'infrastructure sécurisée par défaut. On pense également à l'extension de la détection et de la réponse (D&R) aux menaces de

façon à intégrer l'IA dans l'univers des menaces d'une organisation pour surveiller les entrées et les sorties des systèmes d'IA génératifs. Et cela, afin de détecter les anomalies et d'utiliser les renseignements sur les menaces voire d'anticiper les attaques.

De même, l'IA peut servir à l'automatisation des défenses pour suivre le rythme des menaces existantes et nouvelles afin de répondre plus largement et plus rapidement aux incidents de sécurité. Le management des risques cyber portant sur l'IOT pourrait grandement bénéficier des avancées en matière d'IA.

Aussi, elle est en mesure d'agir pour harmoniser les contrôles au niveau de la plateforme pour garantir une sécurité cohérente, notamment en étendant les protections sécurisées par défaut aux plateformes d'IA et ce en intégrant des contrôles et des protections dans le cycle de vie du développement logiciel.

Enfin, elle est utile en matière d'adaptation des contrôles pour ajuster les mesures d'atténuation et créer des boucles de rétroaction plus rapides pour le déploiement de l'IA grâce à des techniques comme l'apprentissage par renforcement, basé sur les incidents et le retour des utilisateurs.

Restaurer la confiance

L'utilisation de l'IA peut permettre in fine d'établir un niveau de confiance suffisant pour développer des outils nouveaux. Ce potentiel de confiance nouvelle, permise par l'apport de la technologie, va indubitablement générer des gains en termes de productivité. Le constat est également particulièrement pertinent en ce qui concerne les IA destinés à l'audit : dans ce secteur, la technologie vient littéralement en renfort de la dimension humaine du conseil apportée par un professionnel, avec un gain de temps et d'efficacité important.

L'humain au centre de tout

Les experts de Numeum et d'EuroCloud estiment que l'apport de l'intelligence artificielle peut et doit représenter un progrès social. En termes d'emploi, la technologie peut par exemple permettre à des personnes éloignées du numérique de venir y travailler, de par sa relative facilité d'utilisation, susceptible de créer de nouveaux concepts de croissance.

Un profil de type Bac+2 ou +3 pourrait ainsi devenir IA Cyber Analyst afin de diffuser, maîtriser la technologie dans une entreprise ou chez un client. Ces profils n'ont pas besoin d'être nativement techniques. En ce sens, l'IA générative représente un avantage en termes de ressources humaines dans la mesure où beaucoup plus d'individus auront accès à ces métiers nouveaux.

Une opportunité également de montrer ce que la technologie apporte réellement et concrètement aux hommes et aux femmes. Loin de la Science-fiction est des théories futuristes utopiques, l'IA peut éclairer de nouvelles idées, accompagner le développement professionnel et personnel d'une personne, contribuer à relever le défi des compétences et renforcer le niveau de maturité global français en matière de cybersécurité.

Risques et opportunités de l'IA en cybersécurité

Risques de l'IA en cybersécurité :

Sophistication croissante des attaques, notamment de phishing

Création de nouvelles vulnérabilités en cas d'utilisation non autorisée de l'IA par les collaborateurs

Amélioration de la rapidité de la détection et de la réponse aux incidents de sécurité.

Augmentation des attaques automatisées

Opportunités de l'IA en cybersécurité :

Perfectionnement de la sensibilisation et de l'acculturation des utilisateurs

Automatisation de certains systèmes de défense

Supervision améliorée, notamment en matière d'IoT

MÉTHODOLOGIE NUMEUM CAMP CYBER

Numeum a rassemblé une quarantaine d'experts en cybersécurité et en intelligence artificielle issus de ses entreprises adhérentes pendant une demi-journée, autour de deux ateliers thématiques : « *Comment l'intelligence artificielle est susceptible de créer de nouvelles menaces pour le management des risques cyber* », et « *Comment l'intelligence artificielle est susceptible de renforcer le management des risques cyber, et le niveau global de maturité cyber ?* »

La diversité des points de vue exprimés par les RSSI et les experts en intelligence artificielle de haut niveau issus de représentants d'éditeurs de logiciels, d'ESN et d'entreprises de conseil en cybersécurité adhérentes de Numeum a permis d'aborder l'ensemble des thématiques relatives à l'IA et à la Cybersécurité, le tout au sein d'un cadre serein. Chacun a ainsi pu s'exprimer librement autour de la double problématique relative aux conséquences positives et négatives de l'apport de l'intelligence artificielle dans la gestion des risques cyber.

Une compilation des notes issues de ces échanges a ensuite été réalisée, et retravaillée pour aboutir à la présente synthèse, diffusée à l'ensemble de l'écosystème.

REMERCIEMENTS

REMERCIEMENTS

Numeum tient à remercier particulièrement EuroCloud, co-organisateur du Numeum Camp, les membres-experts de la commission cybersécurité de Numeum présents lors de cet évènement, Neuflize, partenaire-financeur des Numeum Camp et le Hub Institute, qui a contribué à l'organisation des échanges.

Ont gracieusement contribué aux échanges : Kevin Smouts, Zygon, Sébastien Sivignon, Custocy, Arnaud Jumelet, Microsoft, Etienne de Séréville, IBM, Francois Lorek, Trax solutions, Yan Richard, SoSafe, Frédéric Daurelle, SalesForce, Yves Chedru, Huawei Cloud Europe, Frédéric Cetlin, AFD Tech, Thomas Gayet, Scovery, Eric Melki, InfoClip, Marc Bothorel, Marc-Antoine Ledieu, Avocat, Cédric Mora, Amazon Web Services, Michel Poujol, Sopra Steria, Louis Naugès, Wizy.io, Olivier Lys, Qorum'SecurNum, Nolwenn le Ster, Capgemini, Pierre-Guillaume Gourio-Jewell, Opensezam.

OURS

- Directrice de la publication : Véronique Torner
- Conception et coordination : Nolwenn Le Ster, Paul Pastor, Olivier Robillart
- Rédaction : Olivier Robillart
- Création graphique : Laura Pineau
- Crédits photos : IStock
- Réalisé et édité par Numeum, 22-28 rue Joubert, 75009 Paris, 2024.