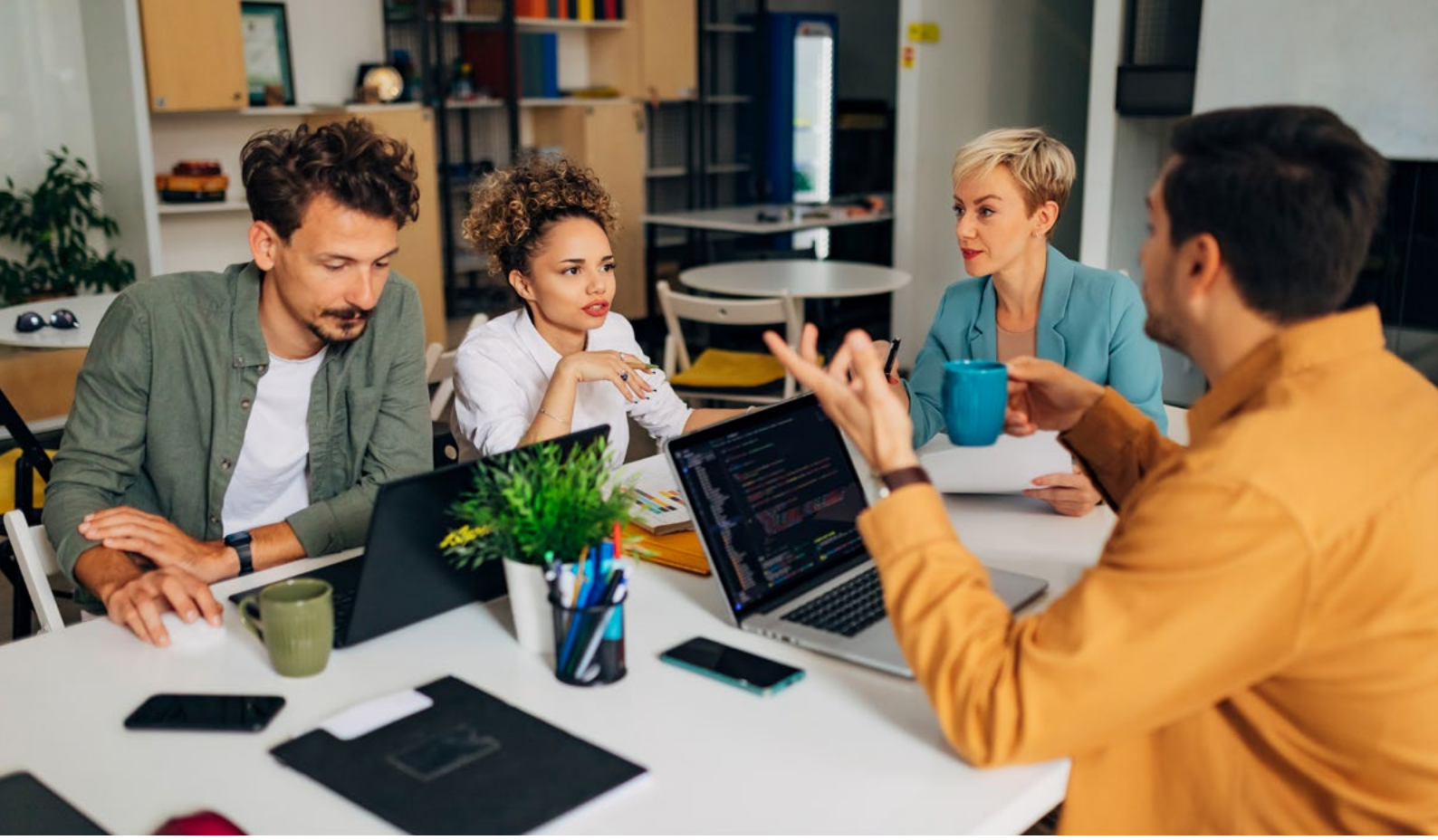


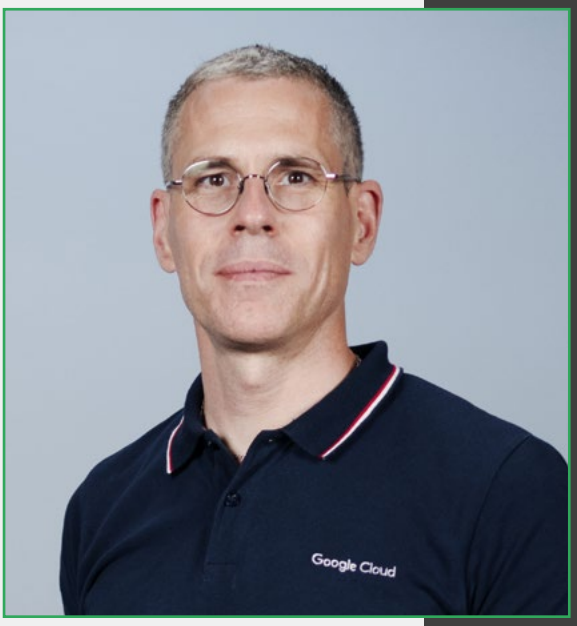
Google Cloud

Interview

CYBERSÉCURITÉ

Comment les PME se mettent à la page avec les solutions Google

Quatre questions à Patrice Puichaud



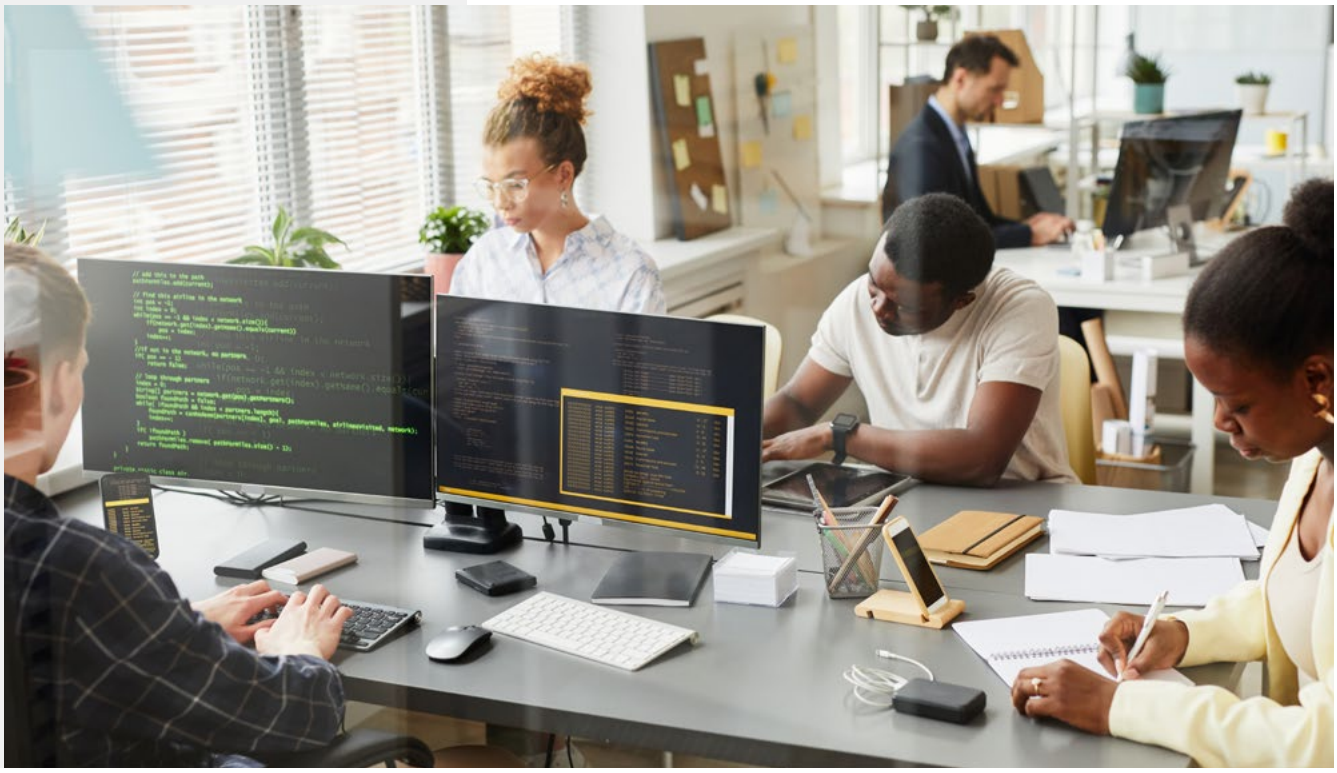
Patrice Puichaud,
Responsable sécurité
Google Cloud France.

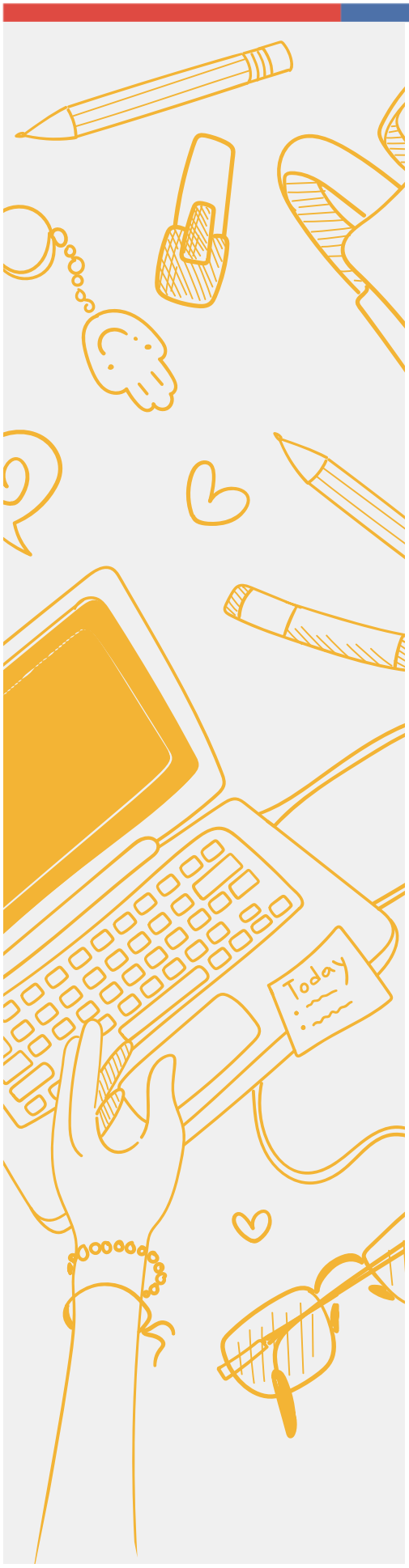
Toute entreprise est susceptible de faire l'objet d'une cyberattaque. Pour des sociétés de taille modeste, PME en tête, une cyberattaque peut même représenter une question de vie ou de mort, et nombreuses sont celles qui ne s'en relèvent pas. Dès lors, comment déployer les bons outils qui les protègeront tout autant que les grands groupes ?
Éléments de réponse avec **Patrice Puichaud**, Responsable sécurité Google Cloud France.

Quelles ont été les évolutions récentes en matière de cyberattaques ? Quelles sont les principales menaces auxquelles font aujourd'hui face les entreprises ?

Patrice Puichaud. Au cours des deux dernières décennies, le paysage des cyberattaques n'a pas fondamentalement changé. Le « top 3 » des typologies de menaces les plus fréquentes est le même qu'il y a vingt ans. On retrouve tout d'abord l'hameçonnage, ou phishing ; ensuite, l'usurpation d'identité, et notamment les vols de données utilisateurs ; enfin, les rançongiciels, ou ransomwares.

Tout d'abord, **le phishing**, qui est très courant. Ces attaques – visant à attirer quelqu'un vers un site Internet frauduleux – étaient assez mal faites durant de nombreuses années, mais sont à présent bien plus crédibles, du fait de l'intelligence artificielle générative. Celle-ci permet de créer du contenu multimodal (texte, audio, voire vidéo), peu cher et très performant. C'est bluffant, notamment ce qui a trait au deepfake – je pense que nous avons tous vu ces vidéos mettant en scène des personnes célèbres à qui l'on fait dire ce qu'elles n'ont jamais dit. Les attaques par phishing se nourrissent également de ce type d'intelligence artificielle et peuvent cibler absolument tout le monde. Ensuite, on





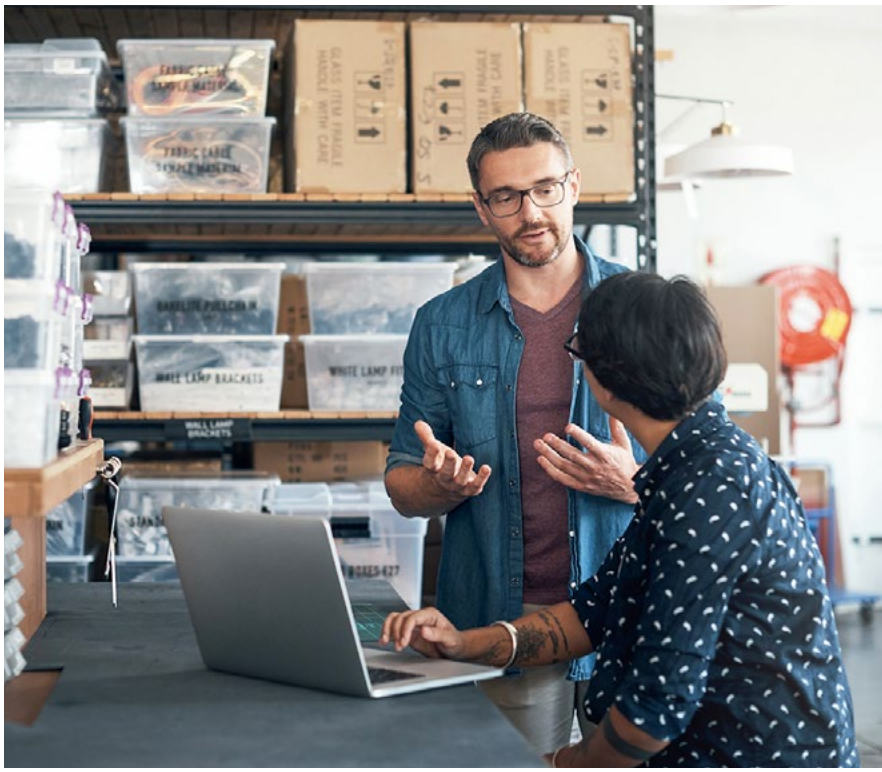
- retrouve **l'usurpation ou vol d'identité**, effectuée via des mots de passe trop faibles, ou des services en ligne. Dans ces cas-là, ce qui intéresse les hackers est de revendre les données subtilisées à des clients qui les exploiteront. Viennent enfin **les ransomwares**. Auparavant, il s'agissait surtout de hackers qui chiffraient vos données et exigeaient une rançon pour les déchiffrer. Désormais, ils menacent de divulguer publiquement des photos ou des données personnelles (c'est le « shaming ») et cela peut vous mettre dans une situation délicate.

  À ces trois types d'attaques assez standards, j'en rajouterai deux, plus techniques. D'une part **l'exploitation de vulnérabilités** ; c'est lorsque vous utilisez des logiciels n'ayant pas été fixés ou patchés, et donc vulnérables ; une faille dont les hackers se serviront pour attaquer. D'autre part les **mauvaises configurations** de solutions cloud, qui présentent donc un risque de sécurité élevé.

  Ces attaques, surtout les trois premières, sont susceptibles de toucher tout type d'entreprise, quels que soient son secteur et sa taille.

> “Ces attaques (surtout le phishing ; l'usurpation ou vol d'identité ; les ransomwares), sont susceptibles de toucher tout type d'entreprise, quels que soient son secteur et sa taille.”

Pour les petites et moyennes entreprises, précisément, les chiffres sont alarmants : environ 80 % des PME attaquées ne s'en relèvent pas. Comment celles-ci peuvent-elles alors capitaliser sur les forces des géants du numérique comme Google et être aussi bien protégées que les grands groupes ?



80%

des PME attaquées ne s'en relèvent pas.

Patrice Puichaud. Ce qu'il faut bien avoir en tête, c'est qu'une PME n'a pas vocation à avoir des employés spécialisés en cybersécurité. Ces PME font donc appel à des experts pouvant les guider et les aider en la matière. Les entreprises fournissant des services de sécurité (MSSP) ou de détection et réponse (MDR) identifient ainsi les potentielles attaques et les contrent.

Par ailleurs, les PME peuvent implémenter des outils, assez simples, pour se défendre ou réduire leur surface d'attaque et leurs vulnérabilités. En la matière, ce que nous proposons chez Google est unique. Notre credo : pour vous protéger, quelle que soit la taille de votre entreprise, vous pouvez utiliser les mêmes outils que nous utilisons chez Google, et ce dans un cadre professionnel autant que personnel. Lorsque vous utilisez Workspace ou un ordinateur Chromebook – très populaire auprès des étudiants par exemple – vous bénéficiez de l'ensemble des moyens de sécurité proposés par Google.

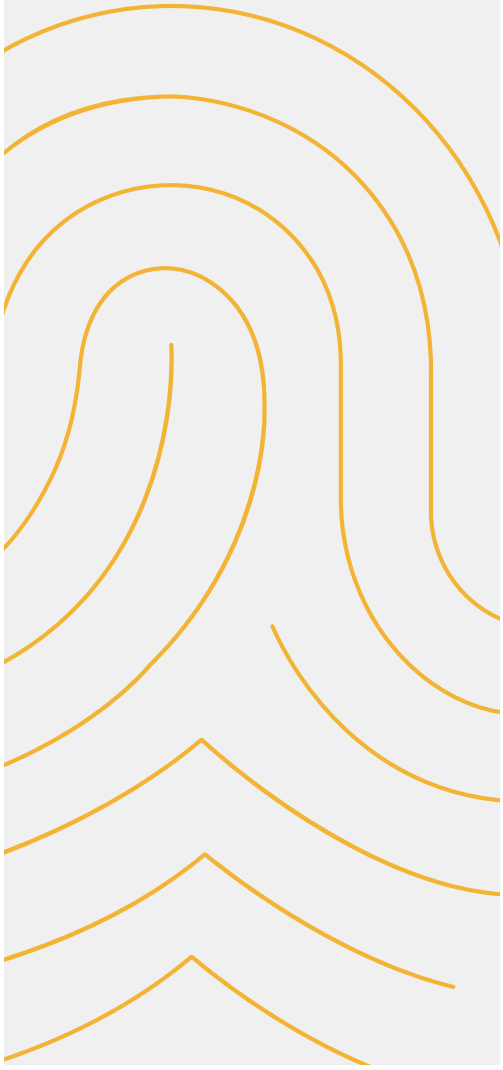
Justement, pour les entreprises, quels avantages concrets y a-t-il à déployer les outils Google comme Chromebook et Workspace ?

Patrice Puichaud. Je repartirai des trois typologies d'attaques que je citais plus haut – phishing, usurpation d'identité et ransomware – pour montrer ce que les outils Google sont capables de faire à ces sujets.

LE PHISHING

Concernant le phishing tout d'abord : si vous utilisez Gmail, vous êtes d'emblée protégé par un outil performant, propre à Workspace. Le nombre de spams ou d'emails malveillants que vous pouvez recevoir est extrêmement réduit. Pour votre navigation sur le Web, vous bénéficiez d'une deuxième protection, intégrée au navigateur Chrome : SafeBrowsing, qui tire profit de la riche base de connaissances de Google. Celle-ci est capable d'identifier les sites frauduleux, du fait de sa connaissance très approfondie d'Internet. On se sert donc de cela pour bâtir une base de données mise à jour en temps réel, à laquelle les navigateurs ont accès.

> Nous proposons de renforcer la sécurité avec des clés physiques d'authentification, répondant au standard FIDO.



L'USURPATION D'IDENTITÉ

Pour l'usurpation d'identité, il existe aujourd'hui des moyens fiables renforçant cette identité numérique. Le mot de passe ne suffit plus, même l'authentification à double facteur (par exemple par SMS) trouve aujourd'hui ses limites du fait des attaques du type « l'homme du milieu » (man in the middle). Pour pallier cela, nous proposons de renforcer la sécurité avec des clés physiques d'authentification, répondant au standard FIDO. Nous encourageons tous nos clients, mais également des personnes sensibles à titre individuel (journalistes, politiciens), à utiliser ces clés. Chez Google, tous les collaborateurs sont dotés d'une clé Titan et ne peuvent accéder à leurs outils de travail sans cela. Par ailleurs, le gestionnaire de mots de passe de Chrome permet de générer des « passkeys ». Plutôt que d'avoir des mots de passe trop faibles, pas assez robustes, on aura donc des phrases très longues, plus sécurisées. Bien sûr, il n'est pas nécessaire de connaître cette phrase, il vous suffit de vous authentifier pour y avoir accès.

LES RANSOMWARES

Pour les ransomwares enfin, quel que soit le système d'exploitation que vous utilisiez, vous pouvez être visé par une attaque, via une pièce jointe frauduleuse, un partage de réseau ou un fichier sur une clé USB. Cela génère un exécutable sur votre machine, qui va chiffrer vos données pour vous extorquer une rançon. Néanmoins, si vous utilisez Chromebook, et donc Chrome OS, vous ne pouvez pas être victime de ce type d'attaque. Historiquement, il n'y a jamais eu d'attaque de ce genre sur ce système d'exploitation. Pour terminer, je citerai les Google Docs, documents partagés en ligne. Ceux-ci ne peuvent pas être chiffrés par un ransomware traditionnel, quand bien même vous utiliseriez un système d'exploitation qui n'est pas Chrome. Et s'ils devaient être attaqués, vos Google Docs ne seraient pas chiffrés, et vous pourrez continuer à les utiliser normalement.

Comment les technologies Google capitalisent-elles sur les dernières innovations, notamment l'IA ?

Patrice Puichaud. L'IA est prisée des hackers depuis très longtemps, la réelle nouveauté est l'IA générative dont je parlais plus tôt. Il est donc primordial que, côté défense, nous puissions tirer parti de cela aussi. Cela consistera par exemple à simplifier les outils techniques pour que les responsables sécurité de nos clients puissent se les approprier plus facilement. Bien sûr, pour maîtriser ce sujet de bout en bout, il faudra toujours être un expert en cybersécurité, c'est indéniable. En revanche, accompagner celles et ceux en charge du support aux niveaux 1 et 2, les aider à trier toutes les alertes qu'ils reçoivent, à comprendre le contexte d'une alerte, c'est possible avec l'intelligence artificielle générative. Grâce à celle-ci, on croisera plusieurs sources d'information pour résumer en un paragraphe les meilleures décisions stratégiques conseillées. De plus, l'IA peut également coder les actions techniques découlant de ces décisions, même si vous n'êtes pas familier avec les langages de programmation. L'idée, ici, est de pouvoir se concentrer sur les alertes bien réelles et dangereuses.

Peu d'acteurs dans le monde possèdent, comme c'est le cas pour Google, la totalité des moyens nécessaires pour créer de l'intelligence artificielle. Le matériel, tout d'abord : il s'agit des processeurs spécifiques aux serveurs ou des data centers. Les données, ensuite : former des grands modèles linguistiques (LLM) requiert de larges volumes de données, ce qui n'est pas à la portée de tout le monde… Les logiciels, par ailleurs : plusieurs modèles d'IA utilisés en LLM proviennent de chez Google et sont disponibles en open source. La connaissance, enfin, puisque chez Google nous bénéficions d'experts en cybersécurité. Google a donc toutes les cartes en main pour proposer de l'IA très pointue. Pour ce qui est plus précisément de la cybersécurité, nous proposons un assistant virtuel, Duet AI, afin d'aider les non-experts.

“Pour ce qui est plus précisément de la cybersécurité, nous proposons un assistant virtuel, Duet AI, afin d'aider les non-experts.”