Évolution de WisdomTree Cybersecurity à l’ère de l’IA

Publié le 26 octobre 2026

Elvira Kuramshina
Associate Director, Quantitative Research

Points clés

- Une nouvelle ère du risque cyber : L’IA générative a d’ores et déjà transformé l’économie de la cybercriminalité ; aujourd’hui, les modèles d’IA les plus avancés inaugurent une nouvelle ère de risques et stimulent la demande. La méthodologie de l’indice WisdomTree Team8 Cybersecurity UCITS a été adaptée pour tenir compte de cette évolution.
- L’IA redéfinit ce qui doit être sécurisé : Avec l’essor de l’IA générant de nouveaux vecteurs d’attaque et des postes de dépenses inédits en cybersécurité, les moteurs de croissance du secteur se transforment. Cela exige donc une révision des critères de sélection et de pondération appliqués aux entreprises.
- Trois évolutions méthodologiques : d’abord, un Focus Score enrichi, intégrant plusieurs signaux ; ensuite, un Growth Score tourné vers l’avenir ; enfin, une formule de pondération à la fois claire et modulable. L’ensemble vise à mieux capter le potentiel de la cybersécurité à l’ère de l’IA.
- Des bases identiques, mais des choix plus affirmés : l’univers initial, la structure centrale et l’expertise du partenaire Team8 demeurent, tandis que la répartition du portefeuille privilégie désormais des sociétés à l’ancrage cybersécurité renforcé et au potentiel de croissance plus prononcé.
- La cybersécurité, pilier essentiel : alors que l’IA s’impose progressivement dans toute l’économie numérique, l’indice se concentre sur les segments affichant la demande la plus soutenue.

La cybersécurité a de tout temps opposé attaquants et défenseurs dans une course permanente ; désormais, l’intelligence artificielle (IA) vient en bouleverser la cadence. Ces dernières années, l’IA générative a bouleversé l’économie de la cybercriminalité : les attaques sont devenues à la fois plus rapides et plus fréquentes, tandis que les défenseurs disposent désormais d’outils plus puissants pour détecter les menaces et y répondre. Les avancées récentes des modèles d’IA de pointe marquent le début d’une nouvelle ère. Avec l'adoption croissante de l’IA au sein des systèmes d’entreprise, de nouveaux actifs apparaissent, nécessitant une protection spécifique : modèles, jeux de données d’entraînement, agents autonomes ou encore identités machine. La cybersécurité reste une opportunité, mais les moteurs de croissance et de différenciation qu’elle recèle changent. Avec le concours de notre partenaire expert Team 8, nous examinons ce que ces évolutions impliquent pour le secteur.

Ces dernières années, le secteur s'est distingué par l'essor d'une sécurité cloud-native, axée sur l'identité et intégrant l'intelligence artificielle. Aujourd'hui, il évolue dans un contexte où les capacités des modèles avancés, l'émergence d'agents autonomes, les identités machines et de nouvelles surfaces d'attaque prennent une place croissante, sans oublier que les systèmes d'IA eux-mêmes requièrent désormais des protections particulières. Pour accompagner cette transition, il faut adopter une approche en mesure de s'ajuster aux secteurs où l'IA sera le principal moteur de la demande à venir. Notre méthodologie s'appuie sur des signaux mis à jour, tirés d'analyses d'experts plus poussées pour guider la sélection et la pondération des entreprises. L'univers d'investissement et le cadre de référence, eux, demeurent inchangés.

Pourquoi l'opportunité liée à la cybersécurité évolue

Le paysage des menaces informatiques se complexifie, et ce, sur plusieurs fronts à la fois. Le rapport Global Threat Report 2026 de CrowdStrike révèle qu'un intrus eCrime a réussi, dans le scénario le plus rapide, à passer de l'accès initial au mouvement latéral en à peine 27 secondes, preuve que les défenseurs disposent d'une marge d'erreur extrêmement réduite. Le nombre d'assaillants est lui aussi en hausse. On observe une augmentation de 49 % en un an du nombre de groupes de ransomware actifs. Pendant ce temps, le coût de l'échec ne cesse d'augmenter. Selon IBM, le coût moyen d'une violation de données dans le monde s'élève à 4,99 millions de dollars.

L'IA façonne désormais les deux aspects de la compétition. D'une part, cela a ouvert une nouvelle surface d'attaque. D'après les analyses menées par Check Point, près d'une requête sur 80 envoyée à une IA générative met en jeu des données sensibles. De son côté, IBM chiffre à environ 6 millions de dollars le coût moyen d'une violation liée à une attaque par inversion de modèle d'IA. En revanche, l'IA s'avère être un atout important pour les défenseurs. Selon l'analyse d'IBM, les organisations ayant largement intégré l'IA et l'automatisation à leurs opérations de sécurité réalisent en moyenne une économie de 1,93 million de dollars par violation. Cette dualité fait émerger une catégorie spécifique de dépenses en matière de sécurité, orientée vers la protection des modèles, des données d'entraînement, des agents autonomes et des identités machine. L'arrivée récente de modèles de pointe aux capacités cyber avancées en est sans doute la meilleure illustration.

Graphique 1 : L'IA devient à la fois une nouvelle surface d'attaque et un nouvel outil pour les cybercriminels comme pour les cyberdéfenseurs.

Plus de 90 organisations	1 sur 80 des requêtes GenAI	6 millions de dollars
Des acteurs malveillants se sont servis d'outils GenAI légitimes, détournés par l'injection d'instructions malveillantes, pour produire des commandes visant à dérober identifiants et cryptomonnaies (CrowdStrike).	Expose des données sensibles aux attaquants (Check Point)	Le coût moyen mondial d'une violation liée à une attaque par inversion de modèle d'IA, reflétant la difficulté croissante de protéger les données d'entraînement et les informations sensibles (IBM).

56%	7,5 % des requêtes GenAI	1,93 million $
D'augmentation des attaques exploitant l'IA, qu'il s'agisse d'usurpations d'identité via deepfake ou de logiciels malveillants pilotés par l'intelligence artificielle (IBM)	Incluent des informations sensibles ou privées (Check Point)	D'économies générées par une adoption accrue de l'IA et de l'automatisation dans le domaine de la sécurité, comparativement aux organisations qui n'y ont pas recours (IBM)

Source : CrowdStrike, « Global Threat Report » publié en février 2026. IBM, « X-Force Threat Intelligence Index 2026 ». IBM, « Cost of a Data Breach Report 2026 ». Check Point, « AI Security Report 2025 ».

La diffusion limitée de la version Preview de Claude Mythos par Anthropic, puis le lancement du Project Glasswing avec une cinquantaine de partenaires, ont constitué un moment charnière. Ils ont mis en lumière une nouvelle capacité des IA avancées à détecter des vulnérabilités à grande échelle. En l'espace d'un mois à peine, les partenaires ont relevé plus de 10 000 vulnérabilités classées comme graves ou critiques. L'AI Security Institute du Royaume-Uni, qui a examiné Mythos Preview en avril 2026, a estimé que ces capacités présentaient un double usage : elles soulèvent d'importants défis en matière de sécurité, tout en ouvrant la voie à des avancées significatives dans le secteur de la défense. Avec l'arrivée prochaine de modèles plus performants, il a été soutenu qu'il est essentiel d'investir dès maintenant dans la cybersécurité.

Présentation de la méthodologie de réponse

La méthodologie s'adapte à l'évolution des opportunités en cybersécurité à travers trois nouveautés : un Focus Score enrichi, intégrant plusieurs signaux ; un Growth Score à visée prospective ; et une formule de pondération à la fois transparente et modulable. Ensemble, ils s'attachent à cerner comment la demande en cybersécurité évolue, ainsi qu'à repérer les entreprises les plus susceptibles d'en profiter.

Un Focus Score enrichi, multi-signal

Score de concentration = Portée de la cybersécurité + Leadership en matière de produits + Thèmes prioritaires

Jusqu'à présent, le Focus Score était déterminé à partir d'un unique critère : l'appartenance de l'entreprise à la catégorie Broad Focus ou Narrow Focus. Désormais, il repose sur la combinaison de trois signaux

à la fois complémentaires et interprétables, additionnés entre eux. Chacune met en lumière une facette particulière du positionnement d'une entreprise sur le plan de la cybersécurité :

- **Portée de la cybersécurité (40 %)** privilégie les entreprises aptes à satisfaire les besoins sur une large palette de segments du marché, au lieu de s'appuyer sur un nombre limité de solutions. On considère qu'une entreprise possède un Broad Focus lorsqu'elle affiche une forte exposition à au moins la moitié des thèmes liés au développement de la cybersécurité. Les entreprises dites à Narrow Focus, présentant une forte exposition à au moins un thème, demeurent éligibles. Ainsi, les spécialistes continuent d'intégrer l'univers d'investissement.
- **Leadership produit (30 %)** prend en compte aussi bien la profondeur que la portée. Team8 analyse les produits de cybersécurité selon des catégories de solutions bien définies et met en avant les entreprises dont les produits se distinguent comme leaders dans leur segment, y compris lorsque leur présence sur le marché reste limitée à une échelle plus réduite. La stratégie peut ainsi orienter l'exposition vers des entreprises capables de répondre à une demande émergente, grâce à des savoir-faire distinctifs.
- **Les thèmes prioritaires (20 % ou 30 %)** ciblent des domaines où la demande en cybersécurité est appelée à croître rapidement. Une entreprise atteint 20 % dès lors qu'au moins la moitié de son exposition porte sur ces thèmes ; ce taux passe à 30 % si elle figure aussi parmi les leaders en matière de produits. Les thèmes prioritaires du moment sont la **Sécurité de l'IA**, qui englobe les solutions destinées à protéger les systèmes d'IA eux-mêmes ; la **Sécurité intelligente**, où l'IA et l'automatisation sont mises à profit pour accélérer et adapter les réponses en matière de sécurité ; et un **Monde sans périmètre**, qui met l'accent sur la gestion des identités et des accès, un défi qui prend de l'ampleur à mesure que les agents d'IA multiplient les identités machines. Ces thématiques ne sont pas immuables ; elles sont susceptibles d'évoluer au fil des avancées technologiques et de la transformation des vecteurs de menace.

Un Growth Score prospectif

Le Growth Score actualisé évalue dans quelle mesure une entreprise est susceptible de tirer profit de la demande en cybersécurité, en se fondant sur l'évolution anticipée de son chiffre d'affaires. Il procède à l'anticipation dès que des données fiables sont accessibles, en appliquant une hiérarchie claire : la priorité va d'abord au taux de croissance annuel composé (TCAC) du chiffre d'affaires sur deux ans ; à défaut, il retient l'estimation sur un an, et, si moins de cinq analystes fournissent des projections, il se rabat sur la croissance effectivement enregistrée au cours des douze derniers mois.

Les entreprises sont ensuite classées en comparaison avec l'ensemble de l'univers éligible à la cybersécurité, plutôt qu'en fonction de seuils de croissance prédéfinis. Ainsi, les seuils évoluent en fonction des conditions du marché et du rythme propre au cycle de la cybersécurité. Les 20 % d'entreprises les moins bien classées sont écartées. Les sociétés restantes sont ensuite réparties en quatre groupes distincts, auxquels est attribué un facteur de pondération propre à chacun :

- **Croissance rapide et taille (1,5x) :** sociétés affichant une forte progression, dont le chiffre d'affaires sur la période écoulée se classe parmi les dix plus élevés du groupe à croissance rapide et dépasse la médiane de l'ensemble. Le groupe est limité à 10 entreprises.
- **Croissance rapide (1,2x) :** entreprises affichant une progression supérieure à la médiane de l'ensemble.
- **En croissance (1x) :** entreprises enregistrant une croissance inférieure ou égale à la médiane.
- **En croissance et en ralentissement (0,8x) :** entreprises appartenant aux 40 % les moins bien notées sur le critère de croissance, mais dont la croissance récente s'est révélée supérieure aux prévisions des analystes, signe que la dynamique faiblit.

Une formule de pondération transparente

Poids final = poids égal × facteur Focus × facteur Growth

Chaque entreprise démarre avec une pondération égale. Ce poids de départ est ensuite multiplié par deux coefficients, l'un provenant du Focus Score, l'autre du Growth Score. Les résultats obtenus sont alors recalibrés pour que l'ensemble du portefeuille atteigne un total de 100 %.

Le **facteur Focus** est égal à 1 additionné au Focus Score de la société. Chaque signal confère un bonus spécifique : la portée peut offrir jusqu'à 40 %, le leadership produit jusqu'à 30 %, et l'exposition au thème prioritaire, 20 % ou parfois 30 %. Ainsi, une société peut se retrouver surpondérée à hauteur de 100 % avant que le facteur Growth ne soit appliqué.

Le **facteur Growth** modifie ensuite la pondération selon le groupe de croissance auquel appartient l'entreprise : il surpondère les sociétés en Croissance rapide et montée en puissance, tandis qu'il sous-pondère celles en Croissance en ralentissement.

L'approche se distingue par sa transparence ; à chaque biais correspond un signal précis. Elle est également modulaire, puisque les facteurs Focus et Growth opèrent indépendamment l'un de l'autre et peuvent être appréhendés séparément. Les pondérations respectent par ailleurs les exigences de concentration, de liquidité et de capitalisation boursière propres à l'indice, garantissant ainsi la constitution d'un portefeuille à la fois diversifié et investissable.

Continuité du portefeuille au cœur

Pour mettre en lumière l'effet de la méthodologie révisée par rapport à l'ancien portefeuille, nous confrontons le portefeuille cible élaboré pour le rééquilibrage d'octobre 2026, selon les règles actualisées, aux pondérations de l'indice en vigueur en mars 2026.

Le cœur du portefeuille reste similaire. Sept des dix principales positions du nouveau portefeuille figuraient déjà parmi les dix premières en mars. Quant aux trois premières, CrowdStrike, Palo Alto Networks et

Fortinet, elles présentent chacune une pondération identique de 7,68 %. Les dix premières représentent ensemble 58,99 % du portefeuille.

Graphique 2 : Top 10 de la stratégie optimisée après le rééquilibrage d'octobre 2026

Nom de la société	Poids	Classification Growth	Facteur Focus Weight
CrowdStrike Holdings, Inc.	7,68 %	Croissance rapide et montée en puissance	2,00
Palo Alto Networks, Inc.	7,68 %	Croissance rapide et montée en puissance	2,00
Fortinet, Inc.	7,68 %	Croissance rapide et montée en puissance	2,00
Zscaler, Inc.	6,15 %	Croissance rapide et montée en puissance	1,60
Rubrik, Inc.	6,15 %	Croissance rapide et montée en puissance	1,60
Varonis Systems, Inc.	4,92 %	Croissance rapide	1,60
Netskope, Inc.	4,92 %	Croissance rapide	1,60
Cloudflare, Inc.	4,61 %	Croissance rapide et montée en puissance	1,20
Datadog, Inc.	4,61 %	Croissance rapide et montée en puissance	1,20
Elastic NV	4,61 %	Croissance rapide et montée en puissance	1,20
Top 10 total	**58,99 %**		

Source : WisdomTree. À partir de la composition cible établie pour le rééquilibrage de l'indice WisdomTree Team8 Cybersecurity UCITS, après la clôture des marchés le 23 octobre 2026. **Il n'est pas possible d'investir directement dans un indice. Les performances passées ne garantissent pas les résultats futurs ; tout investissement comporte un risque de perte de valeur.**

Le principal changement concerne la répartition des pondérations. Le nouveau portefeuille privilégie davantage les sociétés affichant une position renforcée en cybersécurité, leur attribuant des pondérations supérieures au sein des trois catégories du Focus Score, notamment dans Leadership produit et Thèmes prioritaires, où leur part s'avère plus marquée. En matière de croissance, une pondération plus élevée est

accordée aux entreprises affichant une Croissance rapide et montée en puissance, alors que les 20 % de l'univers les moins performants selon le Growth Score ne reçoivent aucune pondération.

Graphique 3 : Comparaison entre l'ancienne et la nouvelle stratégie pour les groupes Focus et Growth

Groupes	Nouveau poids WCBR	Ancien poids WCBR
Focus Score		
Portée de la cybersécurité	27,14 %	24,33 %
Leadership produit	56,54 %	49,03 %
Thèmes prioritaires	84,19 %	76,42 %
Growth Score		
Croissance rapide et montée en puissance	49,16 %	41,82 %
Croissance rapide	25,03 %	25,50 %
En croissance	9,01 %	20,54 %
Croissance en ralentissement	16,80 %	7,99 %
20 % inférieurs	0 %	4,15 %

Source : WisdomTree. Les nouveaux poids WCBR s'appuient sur les positions cibles établies pour le rééquilibrage de l'indice WisdomTree Team8 Cybersecurity UCITS, une fois les marchés fermés le 23 octobre 2026. Les anciens poids WCBR sont ceux fixés comme cibles lors du rééquilibrage prévu en mars 2026. **Il n'est pas possible d'investir directement dans un indice. Les performances passées ne garantissent pas les résultats futurs ; tout investissement comporte un risque de perte de valeur.**

En résumé

La cybersécurité forme l'un des piliers essentiels de l'économie numérique et de l'intelligence artificielle ; or, la demande qui en découle se trouve aujourd'hui transformée par les avancées de l'IA. La méthodologie révisée maintient l'univers actuel, la structure centrale ainsi que le partenaire expert, tout en ajustant les critères de sélection et de pondération des entreprises pour mieux accompagner l'évolution de la demande.

Team8 Disclaimer: This Article represents the opinions of Team8 Labs Inc. ("Team8") and is for informational purposes only. You should not treat any opinion expressed by Team8 as a specific inducement to make an investment in any security, but only as an expression of Team8's opinions. Team8's statements

and opinions are subject to change without notice. Team8 is not registered as an investment adviser under the Investment Advisers Act of 1940, as amended (the “Advisers Act”), and relies upon the “publishers’ exclusion” from the definition of investment adviser under Section 202(a)(11) of the Advisers Act. As such, the information contained in this Article does not take into account any particular investment objectives, financial situation or needs and is not intended to be, and should not be construed in any manner whatsoever as, personalized investment advice. The information in this Article is provided for informational and discussion purposes only and is not intended to be, and shall not be regarded or construed as, a recommendation for a transaction or investment or financial, tax, investment or other advice of any kind by Team8. You should determine on your own whether you agree with the information contained in this Article. Certain of the securities referenced in this Article may currently, or from time to time, be constituents of an index developed and maintained by WisdomTree Investments, Inc. using data provided by Team8, which has been or will be licensed for a fee to one or more investment funds. In addition, certain officers or employees of Team8 or funds or other persons or entities affiliated or associated with Team8 may hold shares of, be officers or directors of, or otherwise be associated with some or all of the issuers of the securities referenced in this Article or included in such index. Team8 expressly disclaims all liability with respect to any act or omission taken based on, and makes no warranty or representation regarding, any of the information included in this Article.

INFORMATIONS IMPORTANTES

Le présent document a été rédigé par WisdomTree et ses sociétés affiliées. Il ne constitue en aucun cas une prévision, une recherche ou un conseil en investissement, ni une recommandation, une offre ou une sollicitation d'achat ou de vente de titres ou bien d'adoption d'une quelconque stratégie d'investissement. Les opinions exprimées correspondent à la date de publication du document et peuvent varier selon les circonstances. Les informations figurant dans les présentes, y compris toute opinion qui y est exprimée, proviennent de sources exclusives et non exclusives. De ce fait, aucune garantie n'est donnée quant à l'exactitude ou à la fiabilité des informations. En outre, WisdomTree, toute société affiliée, un de leurs dirigeants, employés ou agents rejettent toute responsabilité en cas d'erreurs ou d'omissions (y compris la responsabilité envers toute personne pour cause de négligence). L'utilisation des informations contenues dans le présent document est laissée à la seule discrétion du lecteur. **La performance passée ne constitue pas une indication fiable des performances futures.**