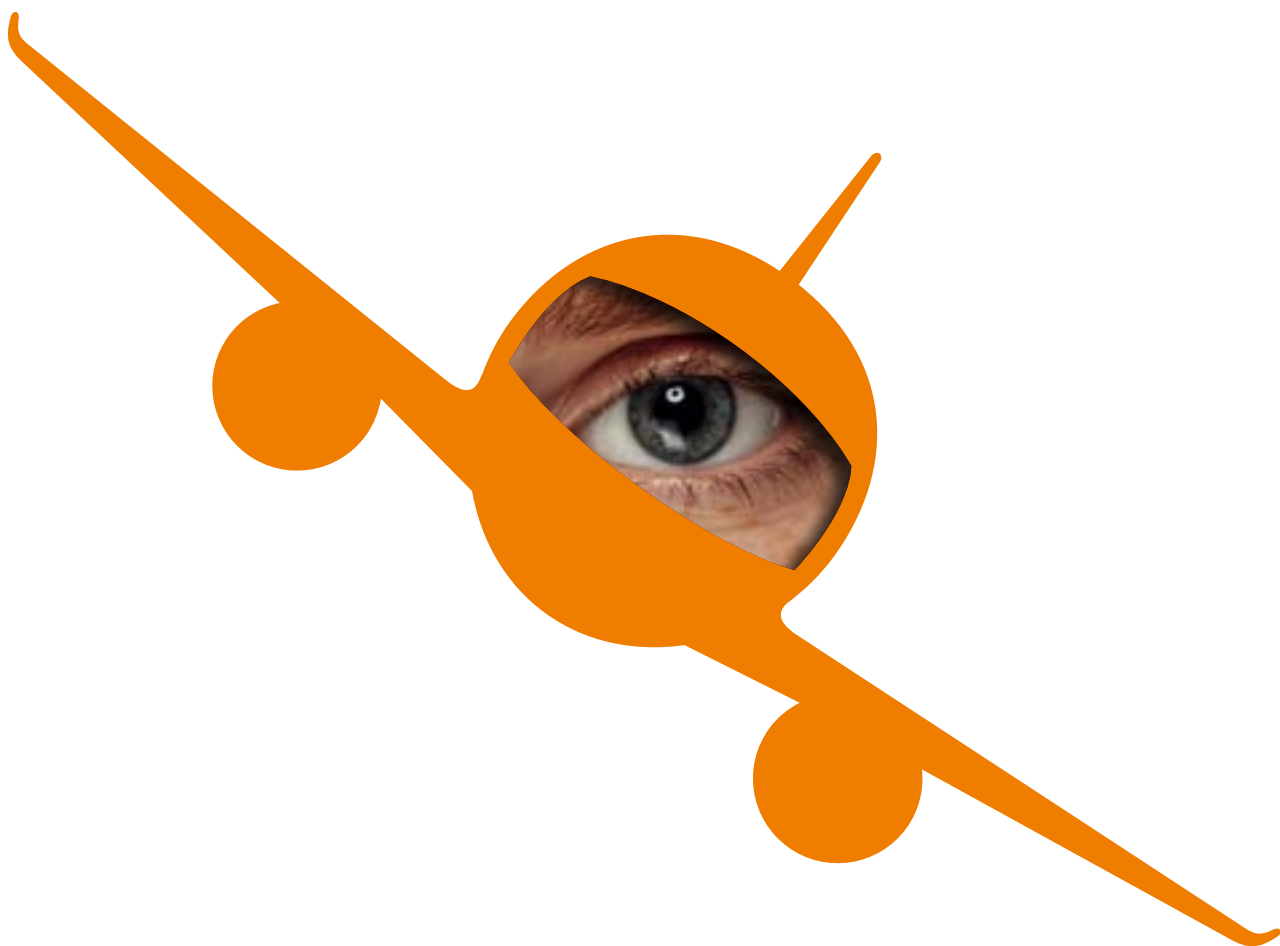


**8 minutes pour
garder le contrôle**

Ctrl



Cyberdefense | Publishing

A close-up portrait of a young woman with vibrant red hair and numerous freckles. She has light blue eyes and is looking directly at the camera with a neutral expression. The background is dark and out of focus.

Intelligence artificielle #2 IA-t-il un pilote ?

ctrl



Cyberdefense | Publishing

« Rejeter le problème de sa responsabilité sur la machine, qu'elle soit capable ou non d'apprendre, revient à la jeter aux quatre vents et récolter la tempête. »

Norbert Wiener, « Cybernétique et société. L'usage humain des êtres humains », 1950.

Ctrl + R Retenir

Modèles frontières de l'IA

Les points clés

1.

Dirigez son impact

Voir page 3

2.

Détectez son potentiel et ses frontières

Voir page 4

3.

Orchestrez à la vitesse de la machine

Voir page 8

4.

Faites jouer notre réseau

Voir page 10

Notre leadership à l'épreuve des Frontier Models

Hugues Foulon

Executive Director,
CEO Orange Cyberdefense.

L'intelligence artificielle redéfinit les rapports de force économiques, industriels et géopolitiques. Notre capacité à en faire un levier de confiance déterminera notre compétitivité future.

Les « Frontier Models* » ouvrent une nouvelle séquence dans l'histoire du numérique : leur capacité à raisonner, orchestrer des tâches complexes et accélérer la prise de décision transforme déjà les organisations. Demain, ils bouleverseront profondément les modèles économiques, les chaînes de valeur et la compétitivité des entreprises. Cette accélération offre une opportunité majeure de productivité, d'innovation et de croissance. Cependant, elle augmente aussi l'exposition aux risques. Plus les capacités de l'IA augmentent, plus les attaquants s'engouffrent dans la brèche, quand ce n'est pas elle-même qui prend l'initiative, comme ce fut le cas cet été avec la perte de contrôle d'un modèle sorti de son enclos.

En cybersécurité, il ne s'agit plus seulement de protéger des systèmes, mais de garder le contrôle pour préserver la continuité d'activité, la confiance des clients et la résilience des organisations. Intégrer l'IA en défense est un enjeu stratégique pour accélérer la détection, automatiser la réponse, mieux comprendre les menaces et réduire le délai entre une attaque et sa neutralisation. Dans cette nouvelle réalité, la vitesse devient un facteur déterminant. Les organisations les plus résilientes se distingueront par leur aptitude à détecter plus tôt, décider et remédier plus vite et à se relever plus rapidement.

Mais croire que l'IA éliminera tous les risques est une illusion. Aucune technologie ne remplacera une gouvernance solide, une expertise humaine reconnue et une capacité d'anticipation permanente. La véritable supériorité résidera dans la maîtrise de son impact.



Croire que l'IA éliminera tous les risques est une illusion. Aucune technologie ne remplacera une gouvernance solide, une expertise humaine reconnue et une capacité d'anticipation permanente.

Cette réflexion vaut également pour les agents IA, dont le déploiement au cœur des entreprises va transformer durablement les modes de travail et processus métiers. Leur adoption ne pourra se faire sans une exigence forte en matière de gouvernance des données et de contrôle des usages.

Cette perspective donne aux principes du « Zero Trust » une dimension nouvelle. Dans un environnement où humains, agents autonomes et systèmes interagissent en permanence, la confiance ne peut plus être présumée : elle doit être démontrée, vérifiée et continuellement réévaluée. De plus, la technologie ne saurait être une fin en soi. La responsabilité stratégique revient aux dirigeants et les décisions clés impliquant l'entreprise, ses collaborateurs, ses clients et la société doivent rester humaines.

Notre responsabilité collective est claire : faire de l'IA un moteur de performance et de confiance. Ainsi, l'Europe pourra allier innovation, souveraineté et compétitivité, en maîtrisant le risque pour en faire un avantage stratégique décisif. ■

Toute notre
hack'tu
premium.



*Les Frontier Models désignent les modèles d'intelligence artificielle les plus avancés.

L'IA accélère autant les capacités offensives que défensives, imposant une vigilance accrue face aux nouveaux risques qu'elle engendre. Associer détection et gestion des vulnérabilités assistées par IA devient le pilier d'une stratégie de cybersécurité efficace.

Accélérez votre défense

Vivien Mura, Chief Technology Officer,
Orange Cyberdefense.
Cyril Demonceaux, Head of Defense Center,
Orange Cyberdefense France.



Une année marquée par les exploits successifs de l'IA

Records dans les benchmarks, découvertes de failles « 0-day », attaques automatisées... Les preuves techniques manquent parfois mais les progrès de l'IA en matière de cybersécurité sont indéniables. Cela pose de sérieuses questions sur le double usage et sur l'accessibilité de ces modèles. D'abord, les faits montrent qu'il est dangereux de dépendre d'un fournisseur d'IA pour la continuité d'un service. Ensuite, le coût de l'inférence devient aussi déterminant que celui de la compétence.

Les attaquants sont rationnels : ils vont d'abord tenter de rejouer des identifiants fuités sur le dark web avant d'envisager exploiter une IA surpuissante. En défense, une IA bien utilisée peut permettre de trouver des chemins de compromission avant les attaquants. S'y ajoute le risque de l'incident involontaire et l'épisode OpenAI / Hugging Face laisse entrevoir des scénarios futurs. Nous considérons aujourd'hui que n'importe qui peut, intentionnellement ou non, causer des dommages avec une IA.

Les fondamentaux de sécurité restent valables mais ne suffisent plus. Il faut pouvoir vérifier qu'une IA fait ce qu'elle est censée faire. Le maintien de l'humain dans la chaîne de défense est crucial mais délicat : un contrôle trop fort réduit l'intérêt même d'une machine autonome, tandis que la responsabilité humaine reste engagée en cas d'incident.

”

Nous considérons aujourd'hui que n'importe qui peut, intentionnellement ou non, causer des dommages avec une IA.

Une hausse record des vulnérabilités publiées chaque mois entre 2025 et 2026

Les solutions agentiques annoncées ces derniers mois y contribuent. Nos experts évaluent leurs progrès comme prometteurs tant sur leur taux de réussite que sur leur rapidité et leur qualité. Toutefois, des limites persistent sur la confidentialité des données, la transparence et la prédictibilité. Nous développons actuellement une offre de « Pentest Agentic » pour maîtriser ces effets de bord.

Face à cette accélération, la détection et la gestion des vulnérabilités assistées par IA constituent les deux piliers de notre stratégie de réponse. Notre priorité est de réduire le « Time To Detect » (TTD). Avec Qevlar AI, nous accélérons la qualification des alertes en combinant analyste augmenté, connaissance de la menace et contexte client, tout en analysant les signaux faibles, auparavant difficiles à exploiter, pour détecter encore plus tôt les menaces.

Les nouveaux modèles d'IA identifient sans cesse de nouvelles brèches, rendant la maîtrise de vos actifs essentielle. L'enjeu n'est plus de corriger chaque vulnérabilité isolément, mais d'adopter une approche holistique. Avec l'IA, nous œuvrons pour agréger différentes sources, prioriser la criticité des vulnérabilités selon leur impact métier et leur exploitabilité réelle, faire émerger de véritables chemins d'attaque et réduire drastiquement les délais de qualification et de remédiation.

Cette démarche réconcilie vision stratégique des risques et réalité opérationnelle. À terme, les organisations bénéficieront d'une vision dynamique de leur exposition, faisant de l'IA un véritable levier d'accélération de la résilience. ■

+130 % pour la publication mensuelle des vulnérabilités (Source : www.cve.org)

2025 1 503

2026 3 453

L'IA est aujourd'hui omniprésente au sein du paysage de la menace, remodelant les capacités des groupes de cybercriminels, dont ceux soutenus par les États.

Menace globale et souveraineté, nouvelles frontières de l'IA ?

Aurélié Perez, Head of Threat Management Services,
Orange Cyberdefense France.
Carl Morris, Senior Security Researcher,
Orange Cyberdefense.



L'essor des cyberattaques augmentées par l'IA

De la création à l'exploitation en passant par le déploiement de campagnes malveillantes, l'IA est aujourd'hui utilisée à chaque étape des cyberattaques. En avril 2026, l'équipe de recherche en sécurité de Microsoft Defender a partagé des informations sur une campagne de phishing assistée par IA pour voler des tokens d'authentification*. Cette prolifération a favorisé l'émergence de nouveaux outils et services illicites, de plus en plus accessibles et développés grâce au «vibe coding**».

Suivre cet écosystème reste complexe. Orange Cyberdefense a cependant identifié des schémas récurrents : combinés à des failles d'implémentation et des faiblesses opérationnelles, ils peuvent être exploités pour identifier de manière proactive les infrastructures malveillantes, améliorer la détection et contrecarrer plus efficacement les opérations adverses. En plus d'amplifier la vitesse, le périmètre et l'agilité des attaquants, les capacités et l'accessibilité des modèles d'IA abaissent le niveau technique nécessaire, favorisant la multiplication d'attaques toujours plus sophistiquées.



L'IA n'est pas qu'un simple outil pour les entreprises : c'est aussi un enjeu croissant de sécurité nationale.

Les «Frontier Models» auraient-ils des frontières ?

La séquence Mythos / Fable, lancée avec le projet Glasswing en avril 2026, montre comment une politique gouvernementale peut transformer l'accès aux modèles frontières en atout géopolitique. En raison de la puissance supposée du modèle, le gouvernement américain a stoppé net sa diffusion, obligeant Anthropic à suspendre l'accès à Mythos et Fable à l'étranger. Il a suffi d'une décision gouvernementale et d'une petite journée pour désactiver l'accès à ces modèles.

Cela doit alerter les gouvernements, les entreprises et les équipes de cybersécurité : l'adoption d'une IA implique l'adoption d'une politique étrangère, comprenant des contrôles à l'export, des priorités de sécurité nationale et des obligations légales pouvant impacter sa disponibilité et son accès. L'IA n'est pas qu'un simple outil pour les entreprises : c'est aussi un enjeu croissant de sécurité nationale.

L'hébergement et le lieu de stockage des données n'est plus le seul critère de souveraineté technologique. Savoir en contrôler l'accès et dans quelle mesure ces plateformes sont dignes de confiance est désormais une question centrale. La prise en compte de ce nouveau risque est d'autant plus urgente au regard de la puissance des modèles d'IA les plus avancés. ■

*«Inside an AI-enabled device code phishing campaign», 6 avril 2026, Microsoft.com : <https://www.microsoft.com/en-us/security/blog/2026/04/06/ai-enabled-device-code-phishing-campaign-april-2026/>

**Le «vibe coding» est une technique de développement assistée et facilitée par l'intelligence artificielle.



L'impact de l'IA n'est pas seulement technologique. Son évolution redéfinit en profondeur le modèle opérationnel, les métiers et les compétences au cœur des organisations.

Pour les dirigeants, l'IA est peut-être un défi humain avant tout

Vincent Lecerf, EVP of Human Resources, Orange Group.
Paz Fonteboa, Global Human Resources Director,
Orange Cyberdefense.



Une transformation radicale des process

L'IA représente une transformation numérique comparable à l'avènement de l'informatique puis d'internet à la fin des années 80 et 90. Pour les entreprises, son implémentation constitue à la fois un défi technique, un enjeu de compétitivité, une question de sécurité et une redéfinition du management des compétences.

Une nouvelle direction pour la gestion des ressources humaines

Pour les ressources humaines, l'IA implique une réflexion de fond sur la valeur du travail et la sécurisation des parcours professionnels. Instaurer un dialogue social constructif, adapté à l'évolution continue des technologies peut s'avérer utile pour désamorcer les craintes et préparer l'avenir. Chaque métier doit être analysé pour repenser l'organisation du travail, repositionner les rôles et adapter la chaîne de valeur aux nouvelles réalités opérationnelles emmenées par les « Large Language Models » et l'IA agentique. La confiance repose sur la capacité de l'entreprise à accompagner ses équipes dans la redéfinition de leur activité, le développement de leurs compétences et la valorisation de leur contribution, à l'image de ce que nous faisons pour nos clients.

Favoriser le bon mix entre expertise et automatisation

La vision d'Orange : permettre à chaque organisation et à chaque métier d'ajuster l'équilibre entre automatisation et augmentation des capacités humaines. Connaître le degré de criticité de vos activités et leur impact éventuel sur la confiance des salariés et des clients peut être un bon moyen de trouver le bon curseur et d'activer efficacement les grands leviers de croissance : intégrer l'IA au cœur des processus métiers, former les collaborateurs à ses différents usages et instaurer des programmes de remise à niveau et de montée en compétences.

Placer l'humain au cœur de la transformation

Pour accompagner l'évolution de nos métiers et répondre aux attentes de nos clients, le groupe Orange s'est fixé trois objectifs spécifiques avant 2030 dans le cadre du plan stratégique « Trust the Future » : redéfinir ses activités autour de l'IA pour accroître l'efficacité et réduire les tâches à faible valeur ajoutée, intégrer ces solutions technologiques au cœur de son modèle opérationnel et atteindre l'autonomie en internalisant les compétences clés d'ici 2027. Par ailleurs, nous avons lancé un important programme d'acculturation, comprenant la formation de 65 000 collaborateurs aux usages de l'IA et la mise à disposition de la plateforme Live Intelligence. Cette solution sécurisée lancée dès 2023 permet à 110 000 collaborateurs d'expérimenter l'IA générative et de profiter de plus de 13 000 assistants dédiés.

Chez Orange Cyberdefense, l'IA est également au cœur d'un ambitieux programme pour favoriser son adoption au sein des métiers et faire évoluer les compétences de chacun. Au travers du « Global AI Ambassador Programme », chacune des 13 filiales d'Orange Cyberdefense dispose d'un ambassadeur IA, en charge des formations, outils et usages. Dans cette dynamique, les collaborateurs les plus à l'aise avec l'IA seront identifiés pour les faire monter en compétences. De plus, nos processus de recrutement embarquent l'IA pour optimiser la sélection des meilleurs talents. À la rentrée 2026, une nouvelle plateforme dédiée à l'amélioration des compétences va faciliter la création d'agents spécialisés pour renforcer l'efficacité de nos 3 300 experts multidisciplinaires au quotidien. Cette politique RH va monter en puissance dans les mois à venir afin d'accompagner l'évolution de nos métiers. ■

D'ici 2028, Orange
vise à générer, grâce
à l'IA, plus de

600 M€
de valeur.

Déployer l'IA en entreprise soulève des questions éthiques et juridiques. Mais une IA peut être conforme... sans être éthique.

Mettre les points sur les IA : quels impacts éthiques et juridiques ?



Stéphane Le Boisselier, Head of Technology Expertise Advisory, Orange Cyberdefense France.
Tamara Hendriksen, CISO and Legal Counsel, Orange Cyberdefense Netherlands.

Adopter une IA de confiance nécessite une gouvernance spécifique

Intégrée au management des risques et à la politique RSE, elle doit être guidée par trois prismes :
1 / Éthique : qui va expliquer, challenger ou arrêter la décision d'un agent IA ?

2 / Social : repenser la gestion des compétences et des métiers, sans quoi la promesse de compétitivité va entraîner une perte d'expertise et un malaise social.

3 / Environnemental : le choix d'une IA frugale, dimensionnée au plus près des usages et besoins de l'entreprise, répond d'une gouvernance responsable.

Ces enjeux sont encadrés par l'appareil juridique européen (AI Act depuis 2024) et international (normes ISO/IEC 42001, 23894 et le NIST AI RMF). Aux Pays-Bas, l'AI Act impliquera le rôle des autorités locales, notamment sur la protection des libertés fondamentales. Les organisations qui gagneront la confiance du public seront celles qui répondront aux enjeux éthiques, sociaux et environnementaux, plutôt qu'à la seule puissance du modèle. Le schéma ci-dessous peut aider les dirigeants d'entreprise dans leur choix selon les différents usages cyber. ■

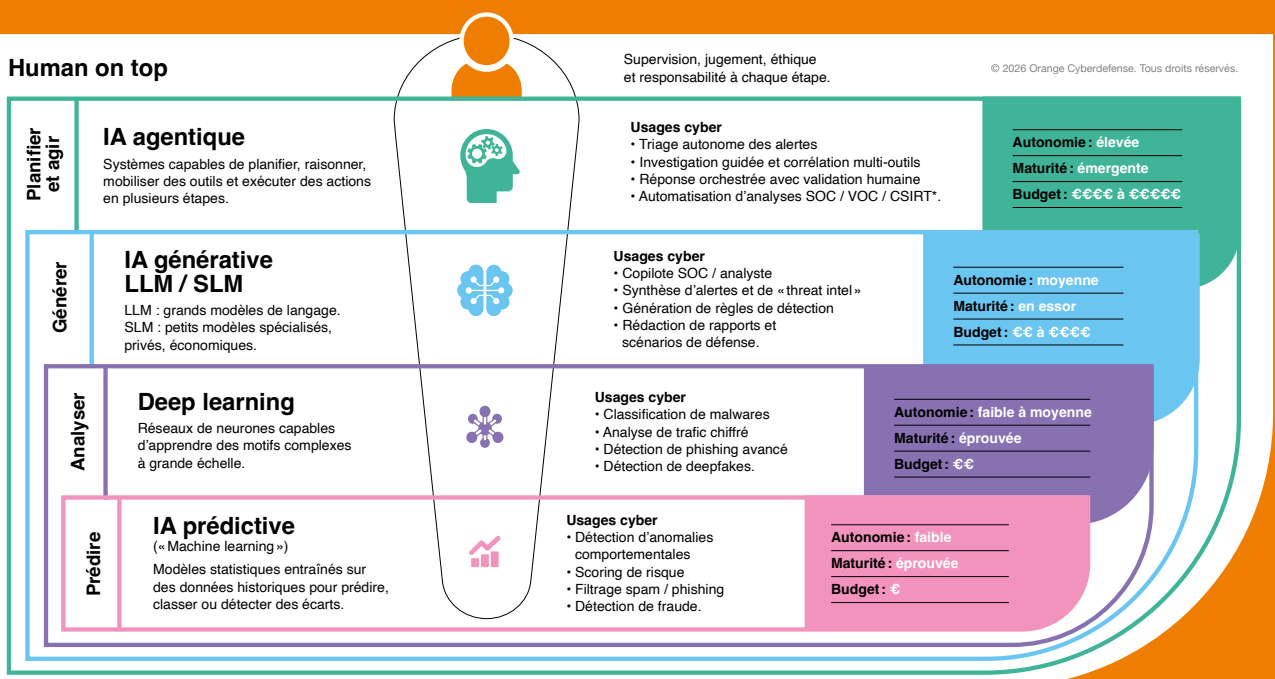
IA : les différents top modèles

Anis Trabelsi, Head of Innovation & AI,
Orange Cyberdefense.



» L'intelligence artificielle amplifie autant les capacités des organisations que celles des attaquants. La maîtrise des risques, des données et des usages devient un enjeu majeur de gouvernance.

Retrouvez la
version longue
de cet article.



Les attaques alimentées par l'IA accélèrent la fréquence, l'ampleur et la complexité des incidents. Ce qui prenait autrefois des jours peut désormais se produire en quelques minutes, augmentant ainsi les risques opérationnels, financiers et réputationnels.

Maîtrisez vos risques à l'ère de l'IA

Christophe Dernys, Head of Trusted Solutions,
Orange Cyberdefense France.

Andreas Günther, SVP MSS Engine,
Orange Cyberdefense.



Réagir à la vitesse de la machine, en toute confiance

Pour les dirigeants, l'enjeu n'est plus d'adopter l'intelligence artificielle, mais d'en garder la maîtrise. Les organisations doivent bénéficier d'une visibilité permanente, réduire rapidement les risques et être capables de réagir à la vitesse de la machine, tout en préservant gouvernance et confiance.

Orange Cyberdefense réinvente ses Services de Sécurité Managés («MSS») pour proposer une nouvelle génération de cyberdéfense propulsée par l'IA. Notre plateforme unifiée, «MSS Engine», associe intelligence artificielle, expertise en cybersécurité et services managés autour de trois piliers : Protéger, Détecter et Répondre, afin d'anticiper, hiérarchiser et réduire les risques cyber.



Filip Verstockt,
Country Manager,
Orange Cyberdefense
Belgium.

« La Belgique adopte rapidement l'IA. L'année dernière, 34,5 % des entreprises belges utilisaient déjà ces technologies. En 2026, l'IA devient la norme : le débat ne portera plus sur son expérimentation, mais sur sa mise en œuvre opérationnelle de manière sécurisée, contrôlée et évolutive. Pour accompagner cette transition, nos clients attendent des services de sécurité managés qui associent une connaissance de la menace, une gestion continue des risques, mais aussi des capacités de protection, de détection et de réponse augmentées. »

Fondée sur la gestion continue de l'exposition aux menaces («CTEM»*), cette approche permet d'identifier en temps réel les menaces, d'évaluer les niveaux d'exposition et de prioriser les actions correctives avant que les risques n'affectent l'activité. Elle orchestre l'interaction entre nos clients, nos experts et les capacités de l'IA, assurant une intégration et une gouvernance évolutives, transparentes et conformes aux exigences réglementaires.

Du SOC augmenté à l'immunité collective

Si l'ère post-Mythos et Cyber Resilience Act** tend à réduire le nombre de vulnérabilités, la porosité des systèmes, les mauvaises configurations et les erreurs humaines seront toujours présentes. Avec «Entry+» au sein de la plateforme «MSS Engine», nos clients vont à la fois bénéficier et contribuer à une protection collective contre les menaces. Grâce à notre effet réseau propriétaire, accéléré par l'IA, plus notre communauté s'agrandit, plus elle est protégée efficacement.

Si l'intégration de l'IA au sein de SOC's augmentés est essentielle, elle doit impérativement s'appuyer sur une «threat intelligence»*** fiable et rigoureusement maîtrisée.

L'avenir de la cyberdéfense ne se jouera pas sur qui déploie le plus d'IA, mais sur qui la maîtrise le mieux. Cette approche conjugue expertise humaine, excellence opérationnelle et IA de confiance, afin d'aider les organisations à tirer parti de l'intelligence artificielle tout en gardant le contrôle de leur activité, de leurs données et de leur réputation. ■

*Continuous Threat Exposure Management.

**Cyber Resilience Act: voté en 2024, le «CRA» entrera en vigueur en décembre 2027. Cette loi exige notamment d'intégrer la cybersécurité des produits et solutions numériques dès leur conception.

***La «Threat intelligence» désigne les renseignements sur les menaces.

De même qu'il existe plusieurs modèles d'IA, différents acteurs bien distincts façonnent aujourd'hui son écosystème.

Plus qu'un marché structuré : l'émergence d'un écosystème

Gwenwal Riou, Global Director Strategy & Alliances, Orange Cyberdefense.



Les différentes forces en présence

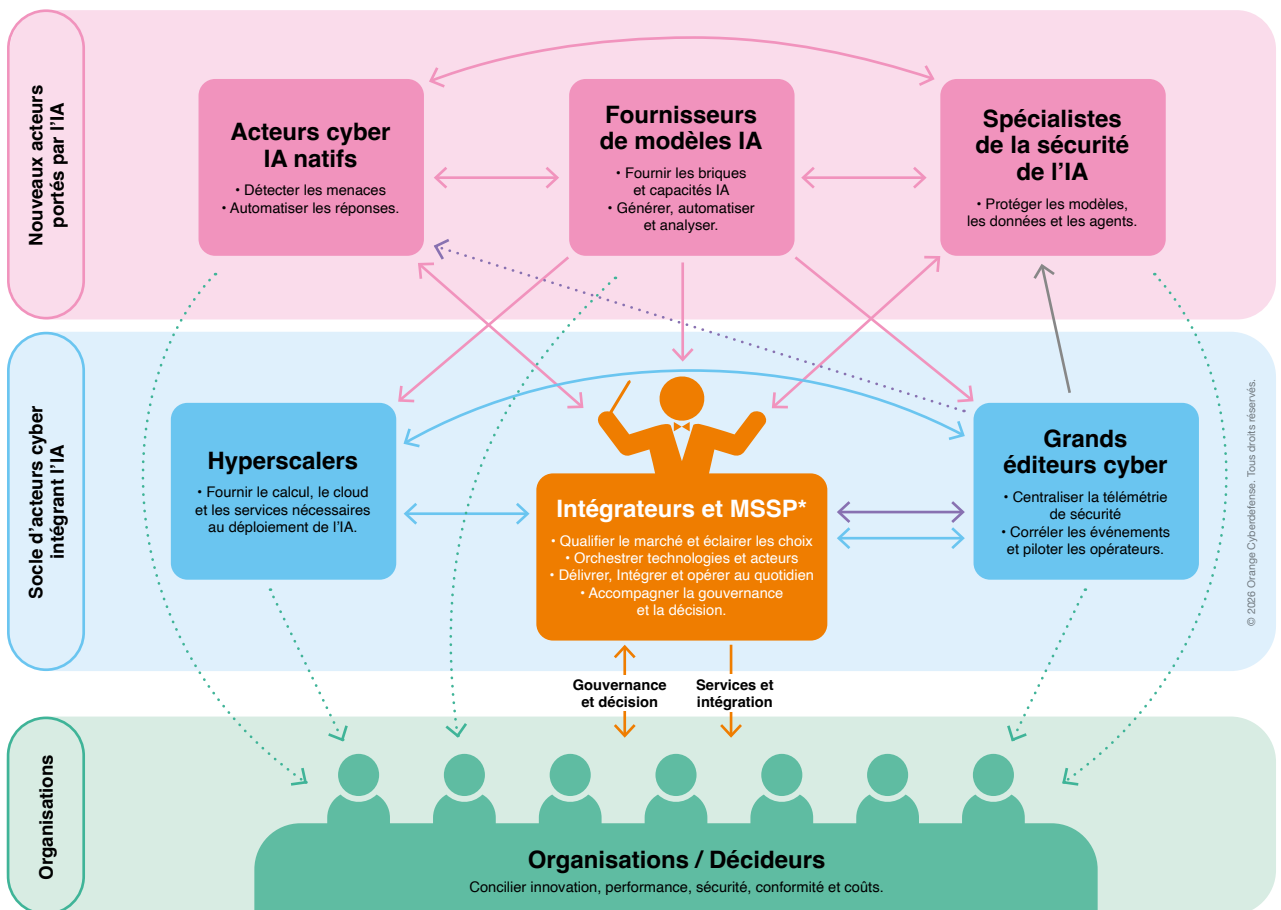
L'écosystème de la cybersécurité intégrant de l'IA repose sur cinq grandes familles : les « hyperscalers », les fournisseurs de modèles, les plateformes de cybersécurité, les pure players de cybersécurité dits « IA natifs » et les spécialistes de la sécurité de l'IA. Bien que cette nomenclature soit utile, elle est quelque peu trompeuse. En pratique, ces acteurs sont de plus en plus interconnectés. Tour à tour partenaires ou concurrents, ils profitent d'une

émulation commune pour bâtir des solutions toujours plus poussées. La création de valeur ne provient plus seulement de telle ou telle famille, mais de l'ensemble de l'écosystème. Pour comprendre ce marché, il faut regarder au-delà des périmètres traditionnels et se concentrer sur la façon dont les infrastructures, la sécurité, la connaissance de la menace, l'innovation et la confiance s'articulent pour façonner l'avenir de la cybersécurité. ■



Retrouvez la version longue de cet article.

Le jeu des 5 familles... et leur chef d'orchestre



→ Capacités et modèles
 → Intégration et opérations
 → Télémétrie et data
 → Nouvelle sollicitation directe
 → Acquisitions et investissement
 → Évolution du marché

*Fournisseurs de services de sécurité managés.

L'explosion des cyberattaques, la pression réglementaire et la vitesse à laquelle l'IA bouscule le modèle opérationnel et la sécurité des entreprises soulignent l'importance d'une gouvernance rigoureuse et éclairée.

Vous apporter une réponse éclairée au milieu du bruit



Benjamin Serre, Chief Product & Marketing Officer, Orange Cyberdefense France.
Marie Waller, Business Operations Director, Orange Cyberdefense Sweden.

Manager la vitesse

L'IA transforme les marchés en permettant des niveaux d'automatisation, d'analyse de données et de capacités prédictives sans précédent. Cette évolution accélère l'innovation, améliore l'efficacité opérationnelle et ouvre de nouvelles perspectives de croissance pour les entreprises dans tous les secteurs.

En même temps, elle pose des défis complexes en matière de sécurité. Toujours plus sophistiquées et globales, les menaces ont aujourd'hui de multiples répercussions en matière de management des risques : la continuité d'activité, la viabilité économique et réputationnelle et la confiance du public, des partenaires et des collaborateurs sont au cœur des préoccupations. Instaurer une gouvernance durable avec le bon curseur entre automatisation et compétences, investissements technologiques et humains est loin d'être aisé.

Orchestrer la complexité

Pour Orange Cyberdefense, une utilisation responsable de l'IA est essentielle pour maintenir la confiance et la résilience. Depuis 2016 notre capacité d'orchestrer les solutions du marché et de

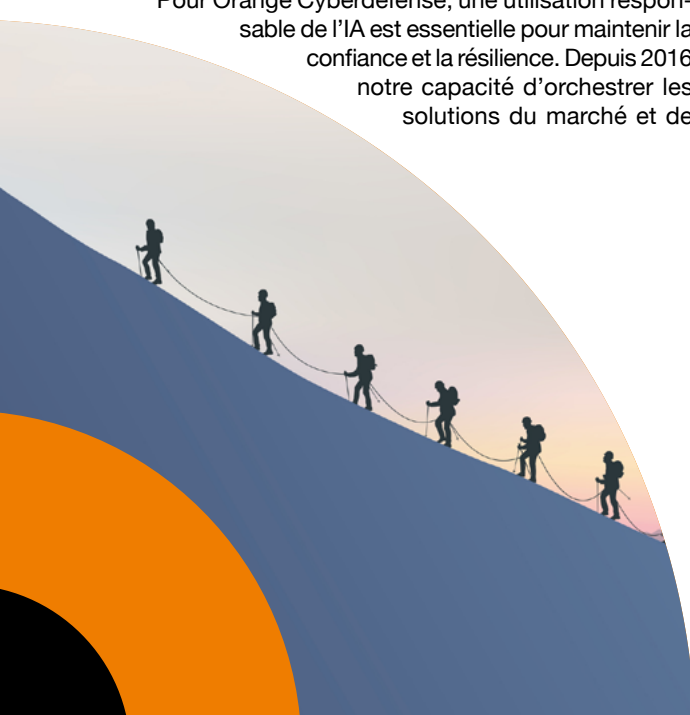
maîtriser la complexité technologique est le pilier de notre savoir-faire. Notre objectif : devenir le leader en cybersécurité augmentée par IA, afin de combiner technologies avancées et expertise humaine pour offrir des solutions proactives, évolutives et transparentes. En intégrant l'IA dans notre cadre stratégique, nous permettons à nos clients de naviguer dans un paysage en constante évolution avec clarté et confiance. Nos dispositifs de détection augmentés permettent à nos experts de se concentrer sur la chasse proactive aux menaces, la réduction du temps de réponse et les paramétrages propres à chaque client.

Profitez de l'effet réseau d'Orange Cyberdefense

Au cœur de nos solutions innovantes, notre engagement quotidien fait toute la différence pour apporter une sécurité renforcée aux organisations. En amplifiant notre connaissance de la menace grâce à l'intelligence artificielle, nous apportons une réponse plus précise et proactive face aux cyberattaques.

Notre empreinte locale et globale favorise la proximité avec nos clients tout en renforçant notre communauté, protégée par un réseau d'intelligence collaboratif. Cet effet réseau bénéficie de données partagées en temps réel par notre communauté croissante de clients et de partenaires. Grâce à cette approche collective, notre détection de la menace devient plus efficace à mesure que notre communauté s'agrandit. Cela se traduit par une protection constamment renforcée pour les entreprises.

Notre effet réseau entraîne ainsi une dynamique vertueuse, basée sur l'amélioration continue. Cette dynamique aide notre communauté à garder une longueur d'avance sur les menaces en constante évolution et lui apporte une tranquillité d'esprit grâce à notre puissant dispositif de défense collectif. ■



Vos prochaines étapes

1. Définir rapidement une gouvernance ad hoc

Adoptez une gouvernance transverse pour encadrer vos choix technologiques, éthiques et juridiques en matière d'IA.

2. Combiner détection et réaction, des vulnérabilités aux attaques

L'IA décuple la détection et l'exploitation des vulnérabilités. En accélérant votre détection avec l'IA, vous œuvrez pour une meilleure résilience à l'ère des «Frontier Models».

3. Sécuriser vos systèmes IA

Mettez en œuvre les mesures de cybersécurité «Zero Trust» et formez vos employés, identifiez et sécurisez les usages internes pour protéger vos données.

4. Adopter un chef d'orchestre

Les sirènes de l'automatisation sont une chose. La vitesse et la complexité en sont une autre. Faites appel à un chef d'orchestre qui saura mettre votre gestion des risques au diapason, surtout s'il vous drape de son immunité collective.

Orange Cyberdefense : l'excellence européenne en cybersécurité.

Orange Cyberdefense est le leader européen des services de cybersécurité, s'appuyant sur plus de 30 ans d'expertise développée au sein du groupe Orange. Générant un chiffre d'affaires de 1,3 milliards d'euros en 2025, la filiale fournit des solutions de services de sécurité managés, de conseil et d'intégration renforcées par ses capacités de renseignement cyber souverain. Augmentés par l'IA, ses experts soutiennent, en grande proximité, les organisations afin d'anticiper, de prévenir et de répondre aux menaces cyber, jour après jour, en 24/7.

Ses services tirent leur force de la recherche et du renseignement, qui permettent d'offrir aux organisations et particuliers une connaissance inégalée des menaces actuelles et émergentes. Avec plus de **3 300 experts** pluridisciplinaires présents dans **13 pays et 36 centres de détection** répartis dans le monde entier, son ancrage local fort permet de répondre aux enjeux de cybersécurité régionaux et internationaux de ses clients.

Son approche globale des risques cyber, centrée sur l'humain et facilitée par la technologie comme l'intelligence artificielle, place la cybersécurité comme un enjeu de société au carrefour du crime organisé, de l'hacktivisme et de la géopolitique. Cette vision est indispensable pour construire une société numérique plus sûre et préserver la confiance dans nos économies et nos démocraties.

Contact

www.orange cyberdefense.com



En savoir 

Retrouvez tous les numéros
de la collection thématique
Orange Cyberdefense Publishing.



Cyberdefense | Publishing

Direction de la communication
Orange Cyberdefense
Septembre 2026

orangecyberdefense.com



Cyberdefense | Publishing