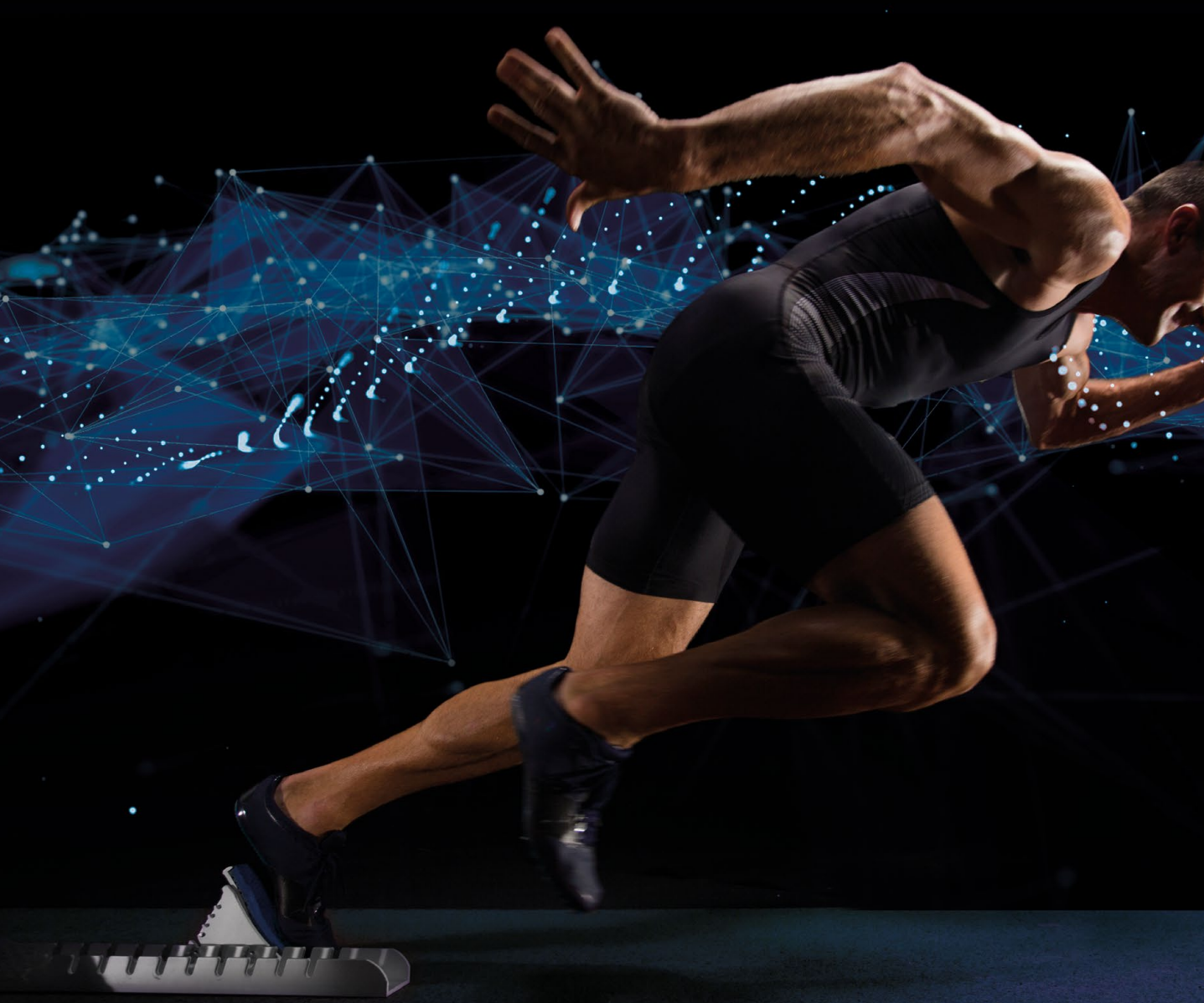
8 minutes pour
garder le contrôle

Ctrl

Cyberdefense | Editions

Menace quantique
Anticipez le tsunami technologique.

Ctrl



orange Cyberdefense | Editions

« L’avenir appartient à ceux qui préparent le présent. » Eleanor Roosevelt

Ctrl + R Retenir

La menace quantique
Les grandes étapes

1. Anticipez le **Q-Day**

Voir page 3

2. Maîtrisez les risques de l’ère **post-quantique**

Voir page 4

3. Adoptez la **crypto-agilité**

Voir page 8

4. Amorcez votre processus de **migration**

Voir page 10

Q-Day : êtes-vous prêt ?

Hugues Foulon
Directeur Exécutif,
CEO Orange Cyberdefense

2025 a été désignée comme étant l'année du quantique par les Nations Unies.

Si notre attention est tournée aujourd'hui sur l'évolution fulgurante de l'IA, il est impératif de relever dès à présent le challenge que ce nouveau paradigme représente, pour la sécurité et la résilience des organisations. On estime que **d'ici 2030-2035,** l'informatique quantique aura la puissance de calcul nécessaire pour casser une partie de la cryptographie actuelle, utilisée pour protéger les flux de communication, de transactions et de données.

Bien comprendre les enjeux de la menace quantique est donc une étape importante en matière de **gestion des risques.** Pour les chefs d'entreprise, anticiper l'émergence du **« Q-Day »** relève d'une véritable prise de conscience. Afin d'assurer la pérennité des flux d'information sécurisés, y compris les plus critiques, un processus de migration en faveur de la cryptographie post-quantique doit être amorcé au plus tôt. Une fois de plus, Orange Cyberdefense est là pour accompagner les entreprises à entamer cette transition dès aujourd'hui et construire ensemble une société numérique plus sûre.

Ce document a été conçu pour vous partager les premières clés de compréhension en matière de cybersécurité, afin de vous aider à déchiffrer les grandes étapes de la migration vers la cryptographie post-quantique. ■

Anticiper l'émergence du « Q-Day » relève d'une véritable prise de conscience. ”

La cryptographie est l'un des fondamentaux invisibles de la cybersécurité. Elle permet la confidentialité et l'intégrité de nos communications, données et identités numériques. Imaginez cependant qu'un jour elle ne soit plus assez robuste pour protéger vos données…

Bienvenue dans l'ère post-quantique

Vivien Mura
Chief Technology Officer,
Orange Cyberdefense.

La cryptographie assure la confidentialité et l'authenticité des données et des échanges, au niveau d'un poste informatique ou mobile, sur le réseau d'une entreprise, sur Internet et entre plusieurs organisations. Lorsque les standards sont respectés et correctement implémentés, il est extrêmement difficile de la compromettre avec les moyens actuels. Typiquement, les capacités de calcul d'un ordinateur classique nécessiteraient des milliers voire des millions d'années pour compromettre des systèmes cryptographiques à clés publiques de type « RSA » ou « ECC ».

Or, des ordinateurs quantiques pourraient un jour exploiter des algorithmes déjà modélisés comme celui de Shor, voire d'autres encore plus performants, pour remettre en cause ces fondements et casser une clé en quelques heures, voire en quelques minutes. On parle de menace quantique.

Se protéger de la menace quantique : un enjeu actuel

Le risque ? Des attaquants ayant récupéré aujourd'hui des données chiffrées, au moyen d'attaques informatiques, pourraient à l'avenir les déchiffrer en utilisant l'informatique quantique. Un tel scénario, connu sous le nom de « Store now, decrypt later », fait peser un risque important sur les données et les communications, dont la confidentialité s'étend sur plusieurs années.

Plusieurs révélations, à commencer par celles d'Edward Snowden en 2013, montrent que des puissances étatiques se livrent à de telles pratiques. Pour les domaines d'activité sensibles comme le secteur bancaire, la défense ou la santé, cette perspective est intolérable. Les prévisions quant à la réalisation de cette menace dépendent notamment des avancées de la recherche, dont certains résultats peuvent ne pas être divulgués.

Les experts estiment qu'une rupture technologique ouvrant la voie à la menace quantique pourrait survenir d'ici 5 à 10 ans.

De nombreux acteurs publics et privés - leaders de l'industrie numérique et startups - sont engagés dans une course pour surmonter les obstacles techniques inhérents à la fabrication de telles machines. Les experts estiment qu'une rupture technologique pourrait voir la menace quantique se réaliser d'ici 5 à 10 ans.

La puissance de calcul quantique pourrait initialement être réservée à des entités disposant de moyens importants. Cependant, son industrialisation et son accessibilité via des modèles « as a service » pourraient accélérer cette disponibilité pour d'autres usages : optimisation industrielle, recherche pharmaceutique et intelligence artificielle. Ce développement pourrait aussi permettre à la cybercriminalité, considérée comme l'une des criminalités les plus importantes de notre époque, de s'en emparer pour déchiffrer des données volées, les revendre ou bien les exploiter lors d'intrusions (phishing, données d'authentification). Ce risque pourrait entraîner une pression importante sur les organisations, qui, à défaut d'anticiper la menace, pourraient devoir agir en urgence, le jour où la protection de leurs données sensibles ne serait plus assurée par la cryptographie actuelle.

Les solutions pour anticiper la menace

Les autorités recommandent d'adopter de nouveaux algorithmes cryptographiques, notamment basés sur les réseaux euclidiens, reconnus comme suffisamment robustes face à la menace quantique. Des algorithmes « post-quantiques » (« PQC ») ont été sélectionnés et leur normalisation a commencé. Leur intégration au sein des protocoles et des produits se fait progressivement, permettant une migration vers ces nouveaux standards. Les organismes les plus exposés doivent planifier cette transition pour protéger leurs ressources sensibles dans les délais. C'est une opération longue et complexe, nécessitant une cartographie des systèmes à migrer, une priorisation des tâches à mener, des tests, benchmarks et déploiements en concertation avec les fournisseurs.

5 min.

C'est le temps qu'il a fallu à la dernière puce quantique de chez Google pour effectuer un calcul complexe, qui aurait pris plus de 10 000 000 000 000 000 000 000 000 000 années à un superordinateur actuel.*

Les infrastructures de gestion de clés « PKI » devront généralement migrer vers le post-quantique, ce qui peut prendre plusieurs années. Le projet requiert des compétences en cybersécurité et cryptographie pour définir les mesures à mettre en œuvre au niveau des systèmes d'information et de la chaîne d'approvisionnement. L'expertise doit être à la pointe, tant sur le plan scientifique que technique, pour mener ces opérations avec méthode et rigueur, en utilisant des outils maîtrisés et sans introduire de nouveaux risques.

Un chemin incontournable mais vertueux

Se protéger de la menace quantique constitue un nouvel enjeu, s'ajoutant aux défis actuels en cybersécurité. La transition vers la cryptographie post-quantique s'inscrit dans une approche globale de gestion des risques et de conformité aux nouveaux standards.

Les algorithmes actuels, dits pré-quantiques, seront progressivement dépréciés, et tout l'écosystème, des concepteurs aux utilisateurs, devra investir pour respecter ces nouvelles normes. L'évolution des standards, l'hybridation et des tests de performance sont nécessaires.

La menace quantique est sérieuse mais prévisible : l'histoire montre que l'anticipation permet de renforcer la sécurité. C'est un défi collectif, une opportunité de réviser les pratiques et d'adopter une cryptographie plus évolutive. Cela permet aussi de mieux évaluer l'exposition aux risques cyber, en utilisant des outils d'évaluation automatique. La migration peut s'intégrer dans une démarche de modernisation, par exemple vers une architecture Zero Trust ou vers des solutions « SASE » (Secure Access Service Edge). Les organisations qui agiront à temps auront un avantage stratégique dans les années à venir. ■

*Source : https://blog.google/technology/research/google-willow-quantum-chip/

Ctrl + R Retenir

Cryptographie post-quantique : les dates clés

1980 Paul Benioff propose le concept d'ordinateur quantique, basé sur une publication d'Alan Turing datant de 1936.

1984 Charles Bennett et Gilles Brassard proposent le premier protocole de cryptographie quantique, sous le nom de BB84.

1994 Peter Shor invente le premier algorithme quantique, remettant en question la cryptographie classique.

1996 Lov Grover invente un algorithme quantique qui réduit significativement le niveau de sécurité des clés symétriques.

2001 IBM démontre le potentiel de l'algorithme de Shor pour casser certains systèmes de cryptographie.

2017 Le NIST* lance un processus de standardisation des algorithmes de cryptographie post-quantique.

2024 Le NIST standardise les premiers algorithmes post-quantiques.

2025 Avec l'accompagnement Quantum Safe Migration, Orange Cyberdefense accompagne les organisations pour assurer leur migration vers la cryptographie post-quantique.

2030-2035 Le Q-Day

Une estimation de la date à laquelle les ordinateurs quantiques pourraient casser le chiffrement numérique actuel.

*National Institute of Standards and Technology.

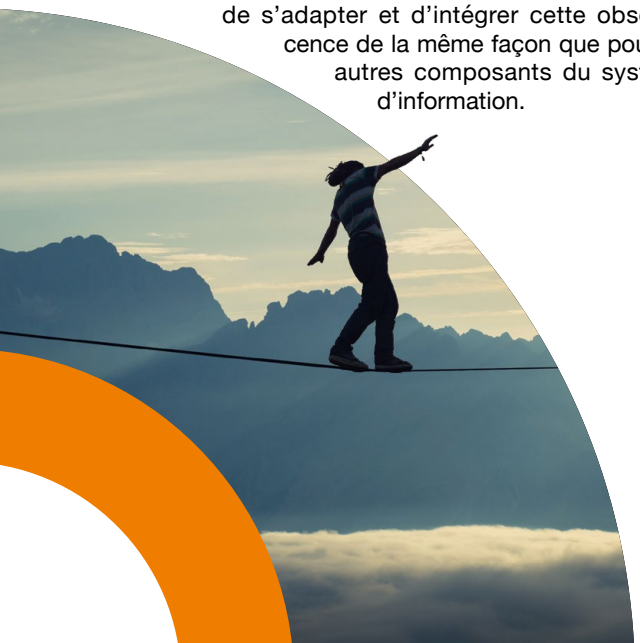
Face à la menace quantique, la capacité d'adapter rapidement les algorithmes cryptographiques est essentielle pour sécuriser les flux de communication. Focus sur l'importance de la crypto-agilité pour relever le défi de la cryptographie post-quantique.

Êtes-vous plutôt crypto-fragile ou crypto-agile ?

Louis-Alexis Brenac
Directeur de l'Expertise - Conseil & Audit,
Orange Cyberdefense.

Qu'est-ce que la crypto-agilité ?
La crypto-agilité désigne l'ensemble des moyens techniques et organisationnels qui permettent à une entreprise de pouvoir modifier les algorithmes cryptographiques utilisés par leurs systèmes d'information. La crypto-agilité permet en somme de faire face aux nouvelles menaces et aux prochaines évolutions technologiques.

Pourquoi cette notion est-elle importante ?
L'émergence de la menace quantique nous montre que les algorithmes cryptographiques ne sont pas immuables et peuvent eux aussi devenir obsolètes. La crypto-agilité permet de s'adapter et d'intégrer cette obsolescence de la même façon que pour les autres composants du système d'information.



> **Notre approche intègre la crypto-agilité afin de garantir la résilience des systèmes face à l'évolution des standards cryptographiques.**

Quelle réponse Orange Cyberdefense peut-elle apporter ?
Nous accompagnons les organisations dans l'anticipation de la menace quantique. Notre approche intègre la crypto-agilité afin de garantir la résilience des systèmes face à l'évolution des standards cryptographiques.

En quoi la crypto-agilité peut-elle bénéficier aux organisations ?
La menace quantique doit servir de prise de conscience pour un problème plus vaste encore : nous avons construit nos systèmes d'information sans agilité cryptographique.

Face à la menace quantique, il faut remédier au problème à sa source et s'assurer que le travail réalisé sur les 5 prochaines années ne doive pas être repris de zéro lorsque les standards de demain deviendront obsolètes à leur tour. ■

L'ABC DU PQC

Votre cyber glossaire

Ctrl + R Retenir

Algorithme cryptographique

Une suite d'instructions mathématiques utilisée pour sécuriser les flux de données en chiffrant le message, qui demeure illisible sans la clé appropriée pour les lire.

Cryptographie

La science et les techniques de sécurisation des données et des communications. La cryptographie comprend des méthodes symétriques, asymétriques et des fonctions de hachage pour protéger l'information contre toute tentative d'accès non autorisé.

ECC

Ensemble des techniques cryptographiques à courbes elliptiques, notamment utilisées pour la signature électronique et l'échange de clé.

NIST

L'Institut national des normes et de la technologie (« National Institute of Standards and Technology ») est une agence américaine dédiée au développement et à la standardisation technologique.

Ordinateur quantique

Reposant sur des Qubits pouvant combiner les états 0 et 1, un ordinateur quantique est capable de traiter un grand nombre de calculs en parallèle. Sur des applications spécifiques, voire complexes, il peut se révéler beaucoup plus puissant qu'un ordinateur classique.

PQC

La « Cryptographie Post-Quantique » (« Post-Quantum Cryptography ») est un domaine de recherche dédié au développement d'algorithmes cryptographiques suffisamment robustes pour résister aux cyberattaques exploitant les capacités des ordinateurs quantiques.

Q-Day

Une estimation de la date (2030-2035) à laquelle les ordinateurs quantiques pourront casser le chiffrement numérique actuel.

Qubit

Un « quantum bit » ou bit quantique est une unité fondamentale d'information en informatique quantique. A la différence d'un bit informatique classique, dont l'état est soit 0 soit 1, un Qubit peut combiner les deux états.

QKD

La distribution quantique de clés (« Quantum Key Distribution ») est une méthode d'échange de clés qui s'appuie sur les propriétés de la physique quantique pour assurer la sécurité des données lors de l'échange de clés cryptographiques.

RSA

Une paire de clés RSA - nommée d'après Ron Rivest, Adi Shamir et Leonard Adleman – est utilisée pour chiffrer et déchiffrer les données. Elle comprend une clé publique, qui peut être partagée et une clé privée qui doit rester secrète.

SASE

Une architecture cloud combinant sécurité réseau et connectivité (Secure Access Service Edge) pour un accès sécurisé aux applications et données, où que l'utilisateur se trouve.

Shor

L'algorithme de Shor, d'après son inventeur Peter Shor, a été inventé en 1994. Il est capable de factoriser rapidement un grand nombre entier sur un ordinateur quantique. Et c'est cette capacité qui révèle précisément les limites de la cryptographie actuelle.

Zero Trust

L'approche Zero Trust repose sur le principe de ne jamais faire confiance par défaut, même à l'intérieur du réseau, en vérifiant systématiquement l'identité et les permissions des utilisateurs et des appareils.

Les enjeux de sécurité post-quantique cristallisent de nombreuses questions chez les décisionnaires et responsables de la sécurité des systèmes d'information. Voici toutes les clés pour être bien accompagné.

Attendre c'est renoncer : réussir son projet de migration

Benjamin Thomas
Consultant en cybersécurité,
Orange Cyberdefense.

Pourquoi la migration vers un système de cryptographie post-quantique (PQC) est-elle urgente ?
Les algorithmes fondamentaux de sécurité en entreprise seront obsolètes d'ici 2030-2035. Il reste donc moins de 5 ans pour anticiper cette transition et mettre en œuvre des remédiations, notamment l'implémentation de nouveaux algorithmes suffisamment robustes face à la menace quantique. Ce projet, chronophage, doit être lancé rapidement, car des attaques de type « Store now, decrypt later » sont déjà possibles. D'où l'importance de se préparer au plus tôt.

Quelles sont les différentes étapes de cette migration ?
Les premières questions qu'un chef d'entreprise ou un Responsable de la Sécurité des Systèmes d'Information doit se poser sont : « Mon organisation est-elle en danger ? Comment la protéger ? Par où et quand commencer ? ». Après avoir répondu, il est recommandé d'établir une feuille de route budgétisée, de sensibiliser les parties prenantes, et d'entamer un inventaire exhaustif des actifs cryptographiques (clés publiques, privées, certificats, signatures, etc.) pour cartographier leur utilisation et préparer la remédiation. C'est sur cette base qu'il sera possible de réaliser les actions opérationnelles nécessaires.

Quels systèmes d'information sont particulièrement concernés ?
La menace quantique concerne potentiellement tous les systèmes d'information, qu'ils soient directement accessibles depuis internet ou via des accès sécurisés. Les opérateurs d'importance vitale (« OIV »), désignés par la Loi de Programmation Militaire (« LPM »), assurent des services essentiels et doivent être prioritaires, tout comme ceux traitant des données sensibles. Cependant, cette menace concerne toutes les organisations, quelle que soit leur taille. La durée et la difficulté du projet de migration seront proportionnelles à la taille et à la complexité du système d'information. Les organisations avec des systèmes vastes et complexes doivent donc commencer plus tôt.

Quelles sont les difficultés techniques ou organisationnelles que les RSSI doivent anticiper ?
Il faut d'abord convaincre la Direction : les moyens à déployer peuvent être importants, et ce sujet est rarement prioritaire face à des problématiques plus immédiates (IA, réglementations NIS2 et DORA). Ensuite, il est nécessaire d'acquérir des connaissances spécialisées en sécurité post-quantique ou de s'entourer d'un partenaire expert capable d'apporter une expertise stratégique, organisationnelle et opérationnelle. Réaliser l'inventaire de tous les usages cryptographiques à tous les niveaux de l'organisation, y compris l'écosystème des partenaires, est une autre difficulté. Enfin, des problèmes de compatibilité des algorithmes cryptographiques peuvent surgir : certains systèmes ne supportent pas le changement d'algorithme, nécessitant des mesures de remédiation spécifiques.

Le « Q-Day » nous rappelle qu'aucune mesure de sécurité n'est immuable. ”

Quelles opportunités les organisations pourraient-elles en retirer ?
Au-delà de la menace quantique, il s'agit de devenir crypto-agile pour anticiper les menaces futures. La pérennité des algorithmes cryptographiques n'a jamais été garantie, et le « Q-Day » nous rappelle qu'aucune mesure de cybersécurité n'est immuable. Les systèmes d'information doivent intégrer la crypto-agilité pour permettre le remplacement des algorithmes pré-quantiques… et anticiper autant que possible les prochaines disruptions cryptographiques. ■

Vos prochaines étapes

1. Anticiper au plus tôt votre migration post-quantique

Lancer dès maintenant une évaluation des risques et établir une feuille de route budgétisée pour la transition vers la cryptographie post-quantique.

2. Sensibiliser et mobiliser la Direction

Convaincre la Direction de l'importance de cette migration en soulignant les enjeux et en mobilisant des experts en sécurité post-quantique.

3. Inventorier et cartographier

Réaliser un inventaire exhaustif des actifs cryptographiques (clés, certificats, signatures) et leur utilisation à tous les niveaux de l'organisation, y compris avec les partenaires.

4. Intégrer la crypto-agilité

Adopter une approche flexible permettant de remplacer rapidement les algorithmes obsolètes, en anticipant l'évolution des standards cryptographiques.

Orange Cyberdefense : l'excellence européenne en cybersécurité.

Leader européen de la cybersécurité, Orange Cyberdefense met son expertise au service d'une société numérique plus sûre. Forts de plus de 30 ans d'expérience héritée du groupe Orange, nous fédérons tous les savoir-faire en cyberdéfense : services managés, conseil et intégration. Notre réseau de 36 centres de détection à travers le monde, notre **CERT privé** - le plus important d'Europe - et nos **3 200 experts** répartis dans **12 pays** nous permettent d'offrir des solutions globales, innovantes et intégrées, adaptées aussi bien aux grands groupes qu'aux PME, institutions ou particuliers. Nous créons un maillage de sécurité pour être en phase avec notre mission.

Notre force repose sur l'alliance unique entre expertise humaine, ancrage local et capacités technologiques de pointe. Grâce à nos collaborateurs passionnés et spécialisés dans tous les métiers de la cybersécurité, nous accompagnons la croissance de plus de **50 000 organisations** et protégeons près de **500 000 particuliers.** Présents au plus près de nos clients, dans les régions comme à l'international, nous adaptons nos offres aux spécificités de chaque écosystème, pour répondre aux menaces actuelles sans négliger les enjeux futurs.

Au cœur de notre performance, la **Cyber Threat Intelligence** (CTI) incarne notre capacité à anticiper, éclairer et agir. Entièrement intégrée, autonome et stratégique, elle est notre colonne vertébrale : elle nous permet d'apporter à nos clients une lecture claire de la menace et des analyses actionnables pour y faire face. En combinant technologies avancées, IA, recherche exclusive et connaissance fine des attaquants, nous bâtissons une cybersécurité utile, humaine et résiliente, moteur de confiance et de développement durable pour les entreprises.

Contact

www.orangecyberdefense.com/fr/contact

En savoir +

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

orange Cyberdefense | Editions

Direction de la communication
Orange Cyberdefense
Juin 2025

orangecyberdefense.com

Cyberdefense | Editions