préparez-vous à l'inconnu

gardez la maîtrise face à l'agilité des cybermenaces

Your business technologists. **Powering progress**

Atos

Nouvelles menaces, nouvelles approches

Votre activité est de plus en plus dépendante d'un monde ultraconnecté. Comment réduire les risques et protéger votre société tout en respectant la conformité ? Se préparer à l'inconnu de manière efficace nécessite une autre approche de la sécurité ou se faire accompagner par un partenaire sécurité de confiance.

Maintenir une position de marché demande un énorme investissement : maîtriser les coûts, gérer la croissance et la fidélisation des clients, stimuler l'innovation. Préserver la sécurité de l'information est essentiel. Vous avez déjà pensé à la mise en place de solutions. Toutefois, connaissez-vous la nature et l'étendue des cybermenaces, qu'elles soient actives et malveillantes ou qu'elles découlent de pertes ou de compromissions accidentelles ? Êtes-vous en mesure de prévoir, de comprendre et d'éliminer les cybermenaces actuelles et futures ? Êtes-vous capable d'adopter les comportements et de développer les compétences qui vous permettront d'y faire face à l'avenir ?

D'après Atos, l'écrasante majorité des entreprises, peut-être la vôtre, ne possède pas les compétences essentielles pour se confronter aux cybermenaces actuelles ou futures, alors que c'est primordial. Ces sociétés ne sont pas qualifiées en matière de *patchs* de serveurs, de connaissance des *Advanced Persistent Threats* ou en matière d'offres relatives aux logiciels malveillants. Nombre de nos clients se rendent compte que rester au fait des derniers risques et innovations de sécurité est une tâche immense. Au lieu d'être attentif aux préoccupations de vos clients vous assistez probablement à des présentations de fournisseurs de sécurité, vous étudiez l'effet de la dernière faille de sécurité ou vous découvrez que vous n'avez pas respecté la conformité suite à une perte de données client. Dans le pire des cas, vous pouvez laisser vos DPI (droits de propriété intellectuelle) s'échapper au profit d'une autre entreprise ou d'un État-nation. Cette situation est susceptible de nuire à votre réputation ou de vous infliger une pénalité financière importante.

Préparez-vous aux cybermenaces à l'ère de l'entreprise « connectée et mobile »

Les solutions de sécurité simples, telles que les pare-feux, ne sont pas assez flexibles, ni suffisantes pour vous protéger des menaces complexes d'aujourd'hui, qu'elles soient malveillantes ou qu'elles découlent d'une exposition accidentelle. En interne, votre entreprise, toujours connectée doit pouvoir fonctionner de manière plus souple. Vous ne pouvez pas restreindre l'accès aux ressources d'entreprise à vos bureaux ou via des technologies spécifiques, car les collaborateurs ont besoin d'un accès constant et fiable aux informations et aux services. On assiste de plus en plus à ce que les analystes appellent la « consumérisation et la dépérimétrisation de l'informatique ». Cela permet à l'entreprise d'être agile et au personnel d'être satisfait. Pour ce faire, l'entreprise s'expose davantage au cyberespace, et donc au risque.

Dans cet environnement, vous devez être préparé à l'inconnu. À cet effet, il vous faut un partenaire de confiance disposant de compétences, d'outils éprouvés et de spécialistes expérimentés pour vous protéger des attaques d'aujourd'hui.

Atos est ce guide. Notre ensemble de solutions de sécurité de bout en bout vous permet de mieux prévoir et d'éliminer de nouvelles incursions, sans jamais interrompre votre activité principale. Nous améliorons votre protection contre les menaces tandis que vous et votre personnel vous concentrez sur ce que vous faites le mieux : votre métier. Nous apportons à nos clients une tranquillité d'esprit tout en leur permettant d'exercer leur activité efficacement dans un monde qui exige de la flexibilité.

Notre savoir-faire reconnu

Atos a plus de 25 ans d'expérience dans la fourniture de solutions et services de sécurité robustes, complets et adaptés aux entreprises de tous les secteurs d'activité. Nous avons une capacité éprouvée à fournir des solutions aux sociétés et entreprises selon des exigences de sécurité extrêmement rigoureuses. Notre travail pour le Comité International Olympique (CIO) est un exemple clair de cette capacité à prévoir et gérer les cybermenaces tout en assurant des opérations fluides et réussies.

La plateforme SIEM d'Atos a traité **plus de 255 millions** de messages d'alerte lors des Jeux Olympiques

Sur ces messages bruts, **4,5 millions** d'événements significatifs ont été identifiés

Le SIEM a identifié des incidents internes pour **5 324** d'entre eux à transmettre au SOC

Sur ces incidents internes, **686** ont fait objet d'une escalade à l'équipe sur site pour action

Lors des Jeux Olympiques 2012 de Londres et de Sotchi en 2014, **0** incident de sécurité n'a affecté le déroulement de la compétition en direct

Statistiques sur les systèmes informatiques, les informations de sécurité et la gestion des événements relatifs aux jeux.

« Avec le soutien d'Atos, le système d'information des Jeux Olympiques de Londres 2012 a été bien conçu, construit et utilisé : les résultats des compétitions ont pu être vus et lus par plus de personnes que jamais auparavant ».

Jeux Olympiques de Londres : - quatre milliards de téléspectateurs - zéro atteinte à la sécurité

En tant que partenaire informatique mondial du Comité International Olympique, nous avons conçu, intégré et géré les multiples systèmes d'information de tous les Jeux Olympiques depuis 2002.

Ces évènements constituent un défi non seulement en matière de sécurité, mais également en gestion de projet. Combien de vos projets connaissent des retards ? Les dates de début et de fin des Jeux Olympiques ne peuvent pas être modifiées : chaque événement doit commencer exactement à l'heure prévue. Atos a systématiquement respecté chaque délai requis par les compétitions pour assurer un déroulement extrêmement précis du point de vue de l'informatique et de la sécurité.

À Londres en 2012, avec plus de quatre milliards de téléspectateurs tout appareil confondu, partout, à tout moment, les menaces du cyberespace ont atteint leur plus haut niveau jamais enregistré. Il s'agissait des premiers « jeux sociaux » avec un niveau sans précédent d'activité sur les réseaux sociaux, ce qui a engendré de nouvelles sources de cybermenaces inconnues. Cependant, grâce à notre approche, nous nous sommes assurés qu'aucune menace connue ou inconnue n'affectait le déroulement normal des Jeux Olympiques, ni ne menaçait les informations essentielles.

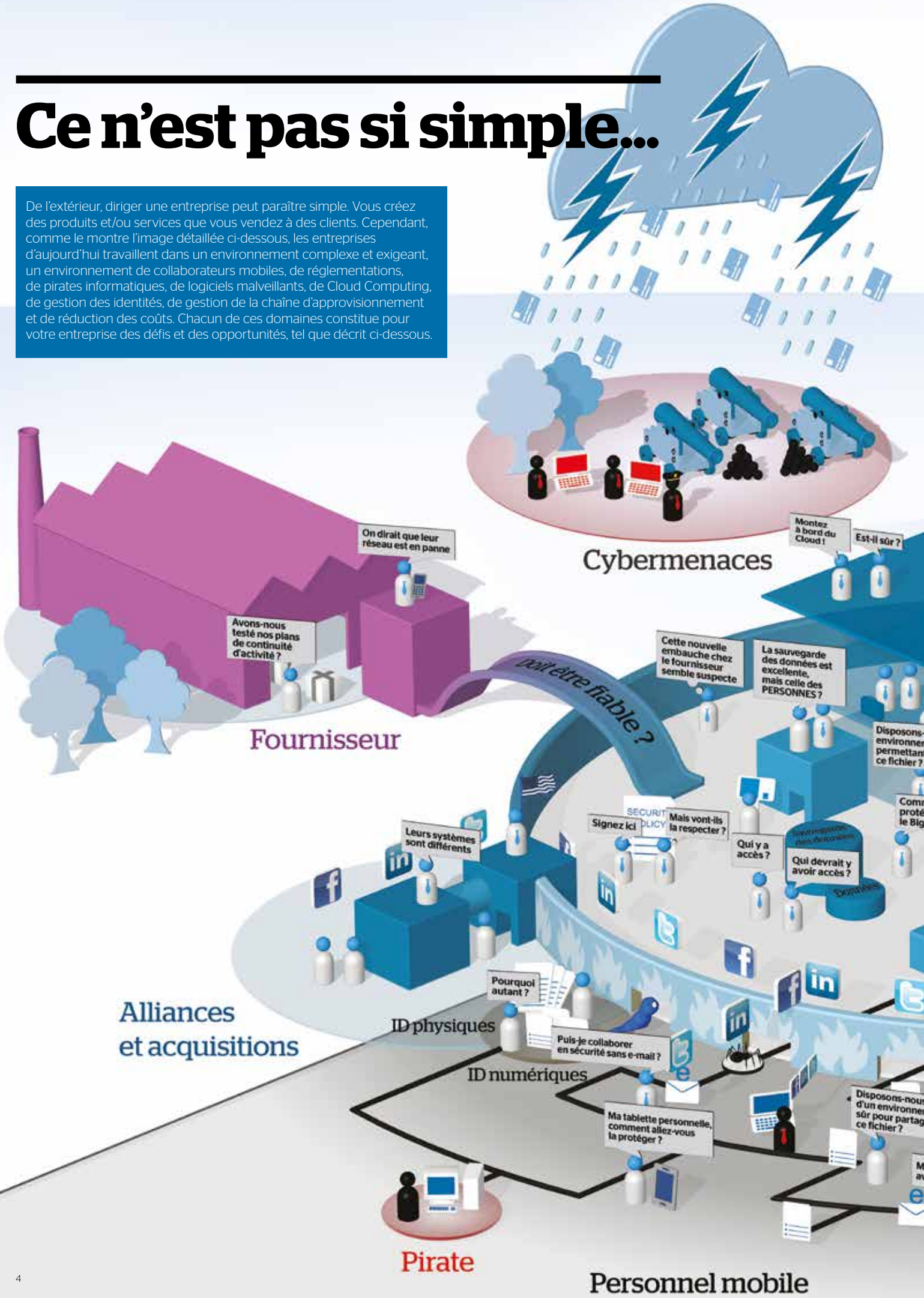
Notre méthode

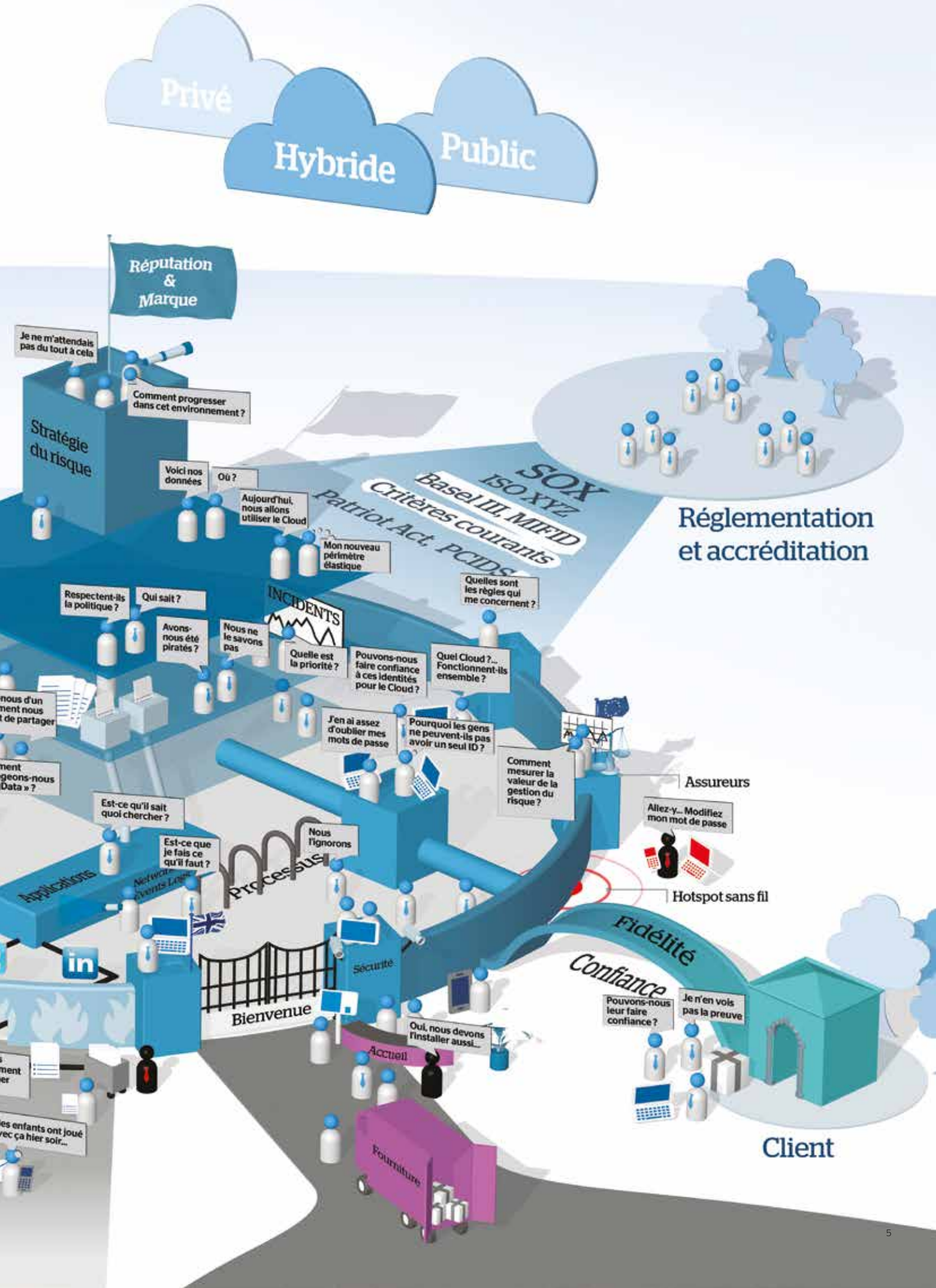
Nous avons réutilisé la démarche que nous avions adoptée lors des Jeux précédents tout au long du cycle de vie du projet. Nous avons mis en place une architecture informatique qui a permis d'assurer une sécurité permanente dans les systèmes informatiques. Cette approche comprenait notre service *Security Information Event Management* (SIEM) géré par notre solution *Atos High Performance Security* (AHPS), associant les connaissances approfondies de nos experts de la sécurité à un centre de sécurité opérationnel (SOC) dédié 24 heures sur 24 et 7 jours sur 7. Ce service, spécialement conçu pour les Jeux Olympiques, peut réagir aux menaces en temps réel 24 heures sur 24, 7 jours sur 7 et permet une analyse à posteriori (forensics). Les événements douteux sont analysés et corrélés sur la base de leur profil de risque, et sont immédiatement signalés aux responsables concernés lorsqu'il apparaît clairement qu'ils appartiennent à une catégorie de risque élevé. Cette solution, en association avec des politiques de sécurité et des procédures comportementales cohérentes, réduit les risques d'interruption des activités par de « fausses alarmes ». Elle permet également de donner une vision d'ensemble et de prendre conscience de l'exposition aux risques pour anticiper une situation critique sur l'architecture informatique.

À Londres en 2012 et à Sotchi en 2014, lors des Jeux Olympiques les plus sociaux et les plus exposés aux cybermenaces à ce jour, notre approche a permis de garantir qu'aucune menace n'endommagerait l'informatique ni n'affecterait la compétition.

Ce n'est pas si simple...

De l'extérieur, diriger une entreprise peut paraître simple. Vous créez des produits et/ou services que vous vendez à des clients. Cependant, comme le montre l'image détaillée ci-dessous, les entreprises d'aujourd'hui travaillent dans un environnement complexe et exigeant, un environnement de collaborateurs mobiles, de réglementations, de pirates informatiques, de logiciels malveillants, de Cloud Computing, de gestion des identités, de gestion de la chaîne d'approvisionnement et de réduction des coûts. Chacun de ces domaines constitue pour votre entreprise des défis et des opportunités, tel que décrit ci-dessous.




Privé
Hybride
Public
Réputation & Marque
Je ne m'attendais pas du tout à cela
Comment progresser dans cet environnement ?
Stratégie du risque
Voici nos données
Où ?
Aujourd'hui, nous allons utiliser le Cloud
Mon nouveau périmètre élastique
SOX
ISO XYZ
Basel III, MIFID
Critères courants
Patriot Act, PCIDSS
Réglementation et accréditation
Respectent-ils la politique ?
Qui sait ?
Avons-nous été piratés ?
Nous ne le savons pas
INCIDENTS
Quelle est la priorité ?
Pouvons-nous faire confiance à ces identités pour le Cloud ?
Quel Cloud ?... Fonctionnent-ils ensemble ?
Quelles sont les règles qui me concernent ?
J'en ai assez d'oublier mes mots de passe
Pourquoi les gens ne peuvent-ils pas avoir un seul ID ?
Comment mesurer la valeur de la gestion du risque ?
Assureurs
Allez-y... Modifiez mon mot de passe
Hotspot sans fil
Est-ce qu'il sait quoi chercher ?
Est-ce que je fais ce qu'il faut ?
Nous l'ignorons
Applications
Processus
Sécurité
Bienvenue
Accueil
Oui, nous devons l'installer aussi...
Fidélité
Confiance
Pouvons-nous leur faire confiance ?
Je n'en vois pas la preuve
Client
Fourniture

Découverte des principales menaces

Dans l'environnement actuel, il est nécessaire de comprendre et de compenser les risques qui peuvent affecter le plus votre entreprise et ce dans les cinq domaines clés : clients, cybermenaces, cloud, mobilité, gouvernance.

Clients

C'est la raison d'être de votre entreprise. Sur cette image détaillée, les clients n'ont qu'une place réduite. D'une certaine façon, les autres activités peuvent être considérées comme une « diversion » de votre objectif principal : fidéliser et augmenter votre clientèle. Ces « diversions » ne sont pourtant pas sans importance : votre entreprise dans son ensemble peut en dépendre. Les organismes de réglementation peuvent considérer votre système non conforme, les pirates peuvent voler des données privées inestimables et les réseaux peuvent tomber en panne. En outre, de nouvelles demandes surviennent tous les jours. Par exemple, les clients d'aujourd'hui exigent un accès de n'importe où, à tout moment, sur n'importe quel appareil. Ils veulent une application pour cela.

De plus, une atteinte à la sécurité peut avoir des conséquences désastreuses pour votre image de marque, le cours de l'action et la fidélisation de vos clients. Plus vous rendez vos informations accessibles, plus vous vous exposez aux risques. La bonne nouvelle, c'est que votre société n'est pas seule. Aujourd'hui, Atos fournit des services de sécurité à des clients du monde entier qui, tout comme vous, se trouvent dans des environnements exigeants.

Nous fournissons des services de sécurité à des réseaux, identités, adresses et applications sécurisés au niveau mondial. Nous offrons la plus large gamme de solutions de gestion des identités de l'industrie, y compris nos propres solutions biométriques et de cartes à puces ainsi que notre propre logiciel de gestion des identités et des accès DirX.

Au Royaume-Uni, plus de 18 millions de citoyens utilisent nos services *via* le portail du gouvernement, que ce soit pour une demande de permis de conduire ou le dépôt de leurs déclarations d'impôts. Le système est alimenté par la capacité de transaction unique d'Atos, qui assure un traitement sûr et optimal à 99,99 % pour les demandes les plus exigeantes. Ce système gère près de 500 000 transactions liées aux impôts lors des journées les plus chargées. Pour Siemens, l'un de nos autres clients, nous gérons 800 000 adresses IP et plus de 40 000 serveurs. Ces deux clients d'Atos se trouvent dans des environnements probablement comparables au vôtre ; si nous pouvons les soutenir à une telle échelle, nous sommes convaincus de pouvoir le faire pour vous aussi.

« Le portail du gouvernement est un atout majeur du gouvernement... Avec plus de 18 millions d'utilisateurs, il est devenu un élément central de la prestation d'e-Services du secteur public pour les citoyens comme pour les entreprises. Pour obtenir ce résultat, nous nous sommes concentrés sur la qualité du service fourni à nos clients tout en restant à la hauteur des exigences changeantes, afin de nous assurer que le portail du gouvernement est bien positionné pour l'avenir et reste au cœur de l'agenda gouvernemental pour la transformation ».

Équipe eDelivery du gouvernement du Royaume Uni

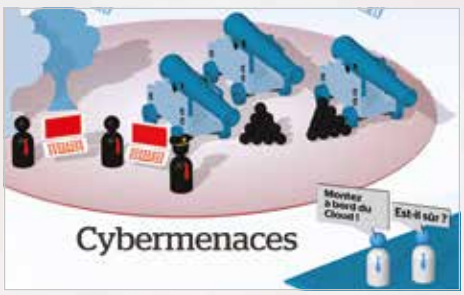
Cybermenaces

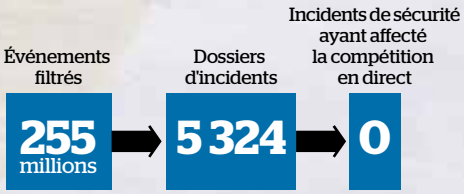
Les virus peuvent sembler d'une autre époque et, par rapport aux menaces d'aujourd'hui, relativement faciles à maîtriser. Les pirates d'aujourd'hui utilisent des logiciels malveillants sophistiqués vendus en ligne, qui se perfectionnent au fil du temps et qui restent difficiles à détecter. Ils ciblent votre patrimoine, sont persistants et parfois financés par des gouvernements étrangers ou de grandes organisations de crime organisé. La valeur en jeu n'a jamais été aussi importante : *Deep Packet Inspection* (DPI) d'entreprise, informations de cartes de crédit, e-mails du gouvernement et même conception de systèmes d'armes. Aucun opérateur de services ne peut garantir une sécurité totale, mais Atos fournit des services de sécurité et SIEM à plusieurs des entreprises les plus en vue au monde.

Atos High Performance Security (AHPS) a été développé par nos experts sécurité de renommée mondiale pour servir vos enjeux, sur la base de notre expérience de protection des systèmes pour les Jeux Olympiques et Paralympiques. Cet événement planétaire constitue une cible de tout premier choix pour les pirates du monde entier ; et pourtant, à ce jour, ils n'ont jamais réussi à déjouer la sécurité informatique qu'Atos a déployée pour le CIO.

AHPS ne repose pas seulement sur des antivirus et des pare-feux, mais utilise des techniques SIEM avancées pour d'abord identifier les comportements et les activités nominaux, avant de se concentrer sur les activités véritablement suspectes. AHPS constitue une défense moderne contre les plus grandes menaces d'aujourd'hui et notamment les menaces persistantes avancées (APT).

Comme l'illustre le schéma de droite, AHPS permet à Atos de filtrer les millions événements potentiellement dangereux pour ne garder qu'un ensemble gérable d'incidents. AHPS résout ceux, dans ce dernier lot, qui pourraient réellement menacer la sécurité afin d'obtenir zéro incident et aucune perturbation de l'activité.





Chiffres réels des Jeux Olympiques 2012 de Londres

« En déployant sa solution de gestion de l'information et des événements de sécurité (SIEM), Atos a pu gérer de manière efficace et efficiente le grand nombre d'événements de sécurité informatique enregistrés lors des Jeux Olympiques 2012 de Londres, afin de garantir l'absence de perturbation dans l'infrastructure informatique des Jeux ».

Jean-Benoit Gauthier
Directeur des technologies et de l'information - CIO

Cloud Computing, l'informatique en nuages

Le Cloud est fait pour durer et va progresser de manière exponentielle. Si votre société ne l'utilise pas, c'est peut-être pour des questions de sécurité. Le Cloud, modèle de computing et de stockage toujours connecté avec des données accessibles de n'importe où, pose nombre de nouvelles questions liées à la sécurité. Atos a constaté que les entreprises avaient des inquiétudes légitimes concernant la protection de leurs données et de leurs informations dans les environnements Cloud.

Pour lutter contre les menaces et les obstacles susceptibles de surgir au sein du Cloud, le service d'évaluation de la sécurité d'Atos vous garantit :

- l'identification de vos problèmes de sécurité et de conformité ;
- l'information sur les obligations légales et réglementaires relatives au Cloud pour votre secteur d'activité ;
- la transparence sur le rapport entre vos coûts et les risques commerciaux.

Notre objectif est de vous aider à clarifier les choses en vous fournissant des rapports et des tableaux de bord objectifs. Votre société pourra ensuite prendre des décisions commerciales pertinentes, basées sur les faits et non sur le battage publicitaire des fournisseurs.

Le personnel mobile

Le personnel d'hier utilisait des postes fixes et des ordinateurs portables verrouillés et renforcés, qui pouvaient généralement, comme l'environnement d'entreprise, être préservés des logiciels non approuvés. Aujourd'hui, non seulement les collaborateurs sont mobiles et en plus ils travaillent en mode collaboratif « ouvert ».

Vos collaborateurs transportent leurs adresses favorites, visitent des sites Web non testés, leur système d'exploitation préféré s'appelle *« Ice Cream Sandwich »* et ils téléchargent des applications non testées (susceptibles de divulguer vos données confidentielles à des serveurs non approuvés). Les utilisateurs utilisent sur leurs outils de travail plusieurs réseaux sociaux populaires et on peut les entendre débattre bruyamment des bénéfices d'Android par rapport à Apple. Comment une entreprise peut-elle fonctionner normalement et en toute sécurité dans ce nouvel environnement ?

Il n'y a pas de réponse simple, mais Atos fournit une suite complète de services de sécurité aux sociétés qui rencontrent ces problèmes. Nous travaillons avec plusieurs fournisseurs de logiciels de sécurité pour appareils mobiles, notamment *Citrix/Zenprise et Good Technology.*

Nos services de sécurité s'adaptent constamment pour répondre aux toutes dernières menaces. À ces fins, nous travaillons en étroite collaboration avec Intel/McAfee et avec des fournisseurs de sécurité de « prochaine génération » tels que Verdasys et FireEye. Les appareils ne pouvant plus être verrouillés, le comportement et les activités doivent être surveillés et gérés avec attention pour éviter des pertes de données sensibles. Les menaces immédiates doivent être traitées avec des moyens de défense qui ne reposent pas uniquement sur des signatures, mais sur des logiciels de test sûrs pour examiner leur comportement.

Les informations provenant des différents appareils de sécurité de la société doivent être intégrées et harmonisées, comme nous le faisons avec AHPS, pour comprendre exactement ce qui se passe dans un environnement informatique. Et comme toujours, le comportement des employés et l'activité d'entreprise doivent être guidés par une politique de sécurité d'entreprise diffusée et comprise par toutes les parties concernées.

Gouvernance et conformité

C'est pourquoi la conformité, la réglementation et la gouvernance n'ont jamais été aussi importantes. L'environnement de travail n'étant plus aussi « renforcé » qu'auparavant, la gouvernance doit faire l'objet d'une attention renouvelée.

La gouvernance et la conformité peuvent affecter presque chaque aspect de votre entreprise, y compris sa marque, sa réputation et jusqu'à son existence même. De plus en plus d'atteintes de non-conformité et de confidentialité ont pour conséquence le paiement de lourdes amendes et un contrôle des médias.

Atos aide les sociétés à comprendre les menaces et à se mettre en conformité. Nos spécialistes sont expérimentés en matière de politiques et d'accréditation de sécurité, de gestion des identités, PCI DSS, ISO27001, conformité et certification HIPAA, formation de sensibilisation à la continuité et à la sécurité des opérations.

En matière d'intégration, de conseil, de services et de systèmes gérés, nous comptons parmi nos clients des agences gouvernementales dans le monde entier et avons donc développé une expertise dans l'analyse et le déploiement de services informatiques qui respectent les normes reconnues au niveau international. Nous sommes expérimentés dans le domaine de la fourniture de solutions de conformité dans chaque secteur, des gouvernements à la distribution jusqu'aux produits pétroliers et aux services financiers. Nous nous associons à EMC2/RSA pour les différentes parties de cette offre.

Chaque secteur peut avoir ses exigences réglementaires propres et uniques. Les spécialistes d'Atos peuvent vous aider à déterminer comment respecter au mieux les règlementations de votre secteur particulier sans dépasser votre budget.

Pourquoi choisir Atos ?

La gestion de la cybersécurité et de la conformité de vos opérations, c'est le cœur de métier d'Atos. Notre expérience sur tous les marchés et la compréhension des processus métiers et des modèles de fonctionnement propres à l'industrie nous permettent de vous fournir la solution dont vous avez besoin tout en réduisant vos coûts. Nous vous permettons d'en faire davantage en prenant moins de risques.

Un acteur clé de la cybersécurité

Chez Atos, tous les experts de la sécurité actualisent constamment leurs connaissances et leurs meilleures pratiques *via* une participation active aux forums nationaux et internationaux. En tant qu'entreprise, nous sommes l'un des membres fondateurs de l'IISP, *Institute of Information Security Professionals*. Nous sommes également membre de nombreuses organisations indépendantes créées pour rassembler fournisseurs, opérateurs et organismes de réglementation afin de définir des normes et un travail sur les réglementations, notamment :

- *International Cyber Security Protection Association* (ICSPA), qui lutte contre la cybercriminalité et la formation au pilotage ;
- *European Cyber Security Protection* Association, qui aide l'industrie à se protéger ;
- *Security and Defence Agenda*, qui se consacre aux défis de la politique de sécurité ;
- *European Security Round Table* (ESRT), qui traite des problèmes de sécurité européens ;
- la *Cloud Security Alliance* (CSA) ;
- *l'Agence nationale pour la sécurité des systèmes d'information* (ANSSI) ;
- Et bien entendu, notre longue liste de clients dans les secteurs industriels saura vous prouver que nous sommes un fournisseur d'une excellente fiabilité.

Préparez-vous à l'inconnu dès aujourd'hui

Le monde d'aujourd'hui comporte des cybermenaces potentielles que vous ne voyez peut-être pas vous-même. Pour les traiter, il vous faut plus qu'une solution de sécurité. Vous devez chercher un partenaire de sécurité digne de confiance et sur lequel vous pouvez compter.

Pour découvrir pourquoi Atos est peut-être le partenaire dont vous avez besoin, contactez-nous maintenant à l'adresse security@atos.net.

Et pourquoi ne pas assister à l'un de nos ateliers d'évaluation ou d'innovation ? Vous y découvrirez comment nous avons aidé d'autres entreprises à faire face à de nouveaux types d'expositions et vous en apprendrez davantage sur les meilleures pratiques en matière de cybersécurité.

Vous pouvez également déposer une demande de consultation gratuite, telle que l'*Atos Security Scan*. Lors de ces séances, nous pouvons évaluer l'état actuel de votre système de sécurité et déterminer s'il est adapté par rapport aux menaces actuelles et émergentes.

Le temps est venu d'agir

Quoi que vous fassiez, n'attendez pas que votre entreprise soit la cible d'une cyberattaque pour prendre des mesures afin d'améliorer votre protection. De nouvelles attaques ont lieu chaque jour et de nouvelles menaces émergent à un rythme préoccupant.

Atos est organisé pour les comprendre en temps réel et est prêt à vous aider à répondre aux menaces connues et inconnues de la cybersphère. Pourquoi ne pas nous laisser appliquer notre approche à votre entreprise ?

Aujourd'hui, aucune autre solution sur le marché ne concurrence son caractère complet et sa rentabilité. Avec Atos comme partenaire de confiance, votre entreprise peut continuer à repousser les limites, à innover et à distancer la concurrence tout en étant assurée que sa sécurité est entre les meilleures mains. Quoi que le futur vous réserve, votre entreprise est en sécurité avec nous.

À propos d'Atos

Atos SE (Société Européenne), acteur international des services informatiques avec un chiffre d'affaires annuel de 8,6 milliards d'euros et 76.300 collaborateurs dans 52 pays, fournit à ses clients du monde entier des services de conseil & d'intégration de systèmes, d'infogérance et des services transactionnels par l'intermédiaire de Worldline, le leader européen et un acteur mondial dans les services de paiement. Grâce à son expertise technologique et sa connaissance industrielle, Atos sert ses clients dans différents secteurs : Industrie, distribution & transports, Secteur public & santé, Services financiers, et Télécoms, médias & services aux collectivités.

Atos déploie les technologies qui accélèrent le développement de ses clients et les aident à réaliser leur vision de l'entreprise du futur. Atos est le partenaire informatique mondial des Jeux Olympiques et Paralympiques. Le Groupe est coté sur le marché NYSE Euronext Paris et exerce ses activités sous les noms d'Atos, Atos Consulting, Worldline et Atos Worldgrid.

Pour plus d'informations : atos.net.

Pour plus d'informations, contactez : fr.directionmarketing@atos.net