keyrus
make data matter

OPSKY
INFRASTRUCTURE AT SCALE

Le maillon faible de la cybersécurité

Sensibilisez vos équipes. Dédiabolisez la prévention.

www.keyrus.com

Le maillon faible de la cybersécurité

Sensibilisez vos équipes. Dédiabolisez la prévention.

L'ère numérique, bien qu'offrant des occasions sans précédent, expose également les entreprises à des risques cybernétiques considérables. La cybersécurité s'impose comme un enjeu majeur pour les organisations de toutes tailles, particulièrement les PME et ETI qui se trouvent souvent moins bien équipées face à ces menaces. Les attaques informatiques, de plus en plus sophistiquées et fréquentes, peuvent avoir des conséquences dévastatrices : pertes financières, atteinte à la réputation, interruption des activités, et dans certains cas, licenciements forcés.

Au cœur de cette problématique se trouve un élément souvent négligé : le facteur humain. Les statistiques révèlent que 95% des incidents de sécurité sont liés à des erreurs humaines, soulignant l'importance capitale de la sensibilisation et de la formation des employés. La technologie seule ne suffit pas à garantir une protection efficace ; il est essentiel de créer une culture de la cybersécurité au sein de l'organisation.

Les défis sont multiples : comment sensibiliser efficacement le personnel aux bonnes pratiques de sécurité ? Comment transformer chaque employé en première ligne de défense contre les cybermenaces ? Comment équilibrer les investissements entre solutions technologiques et formation humaine ? Ces questions se posent avec d'autant plus d'acuité que les conséquences d'une attaque réussie peuvent être dramatiques, avec un coût moyen estimé à 130 000 euros pour une PME.

Face à ces enjeux, une approche holistique de la cybersécurité s'impose, intégrant à la fois des solutions techniques avancées et une stratégie de sensibilisation adaptée. Il s'agit non seulement de protéger les systèmes d'information, mais aussi de former et de responsabiliser chaque membre de l'organisation pour créer un écosystème résilient face aux menaces cybernétiques.

Image et image de couverture générées par **Midjourney** avec la consigne : *« Portrait of an average office employee acting proactively for security enforcement and against cyberattacks and cyber-criminality. --ar 38:125 --style raw --cref https://s.mj.run/41SQk2SljHE --stylize 600 --v 6 »*

Transformation digitale et cybersécurité

La transformation numérique des entreprises, impulsée par l'adoption massive de technologies digitales et l'exploitation des données, a bouleversé les modes de fonctionnement traditionnels. Ce virage vers des systèmes interconnectés, des applications dématérialisées et des infrastructures cloud a offert de nouvelles occasions pour améliorer l'efficacité opérationnelle, mais a également accru les risques en matière de cybersécurité. Les entreprises doivent aujourd'hui faire face à des menaces de plus en plus sophistiquées et ciblées.

Les cyberattaques prennent des formes variées, parmi lesquelles certaines sont devenues particulièrement fréquentes et dangereuses. Le ***phishing***, par exemple, cette technique frauduleuse par laquelle des attaquants se font passer pour une entité de confiance, généralement via des emails ou des messages, afin de tromper les utilisateurs et leur soutirer des informations sensibles, telles que des identifiants ou des coordonnées bancaires. Bien que cette méthode soit relativement simple, elle est extrêmement efficace et reste l'une des plus répandues.

Un autre type de menace courante est celle des ***ransomwares*** (ou rançongiciel). Il s'agit de logiciels malveillants qui prennent en otage des systèmes ou des données en les chiffrant, puis exigent une rançon pour en restituer l'accès. Les entreprises ciblées par des ransomwares se retrouvent souvent dans une situation délicate, pour ne pas dire insupportable : payer la rançon sans aucune garantie de récupérer leurs données ou leurs accès, ou tenter de restaurer leurs systèmes...

D'autres formes de cyberattaques incluent **les attaques par déni de service** (**DDoS**), où les attaquants surchargent les systèmes informatiques ou réseaux d'une entreprise par un flot massif de requêtes, rendant ces systèmes inaccessibles. **Les intrusions réseau**, qui consistent à pénétrer dans un système informatique non autorisé pour en voler des données ou y introduire des logiciels malveillants, sont également très courantes. Enfin, **les exploitations de vulnérabilités logicielles**, où des cybercriminels profitent de failles non corrigées dans des applications ou des systèmes d'exploitation, constituent une menace persistante.

Ces menaces augmentent ce que l'on appelle **la surface d'attaque** d'une entreprise, c'est-à-dire l'ensemble des points d'entrée potentiels qu'un attaquant peut exploiter pour pénétrer un système. Plus une entreprise utilise de technologies interconnectées — qu'il s'agisse d'applications cloud, de l'Internet des objets (IoT) ou de dispositifs mobiles — plus sa surface d'attaque s'étend. Chaque nouveau dispositif ou service numérique représente une porte potentielle pour les cybercriminels, créant ainsi un défi supplémentaire pour les équipes chargées de la sécurité.

Image générée par **Midjourney** avec la consigne : *« https://s.mj.run/m2Zv2lWCK7E Economical impact of cyber criminality. --ar 3:2 --style raw --stylize 600 --v 6. »*

Dans ce contexte, la cybersécurité est devenue une priorité stratégique pour les entreprises. Protéger leurs systèmes, données et infrastructures est essentiel pour garantir non seulement la confidentialité et l'intégrité des informations, mais aussi la continuité des opérations. **Une attaque réussie peut entraîner des pertes financières conséquentes, des interruptions d'activité, ainsi qu'une détérioration de la réputation, parfois irréparable**.

Impact économique et social des cyberattaques

Que dire de l'impact ? sinon qu'il est conséquent... Les PME et ETI sont particulièrement vulnérables et peuvent subir des répercussions économiques et sociales considérables et dévastateurs.

- **Pertes financières directes** : les cyberattaques peuvent engendrer des pertes financières immédiates et substantielles.

Ces pertes se manifestent sous diverses formes, notamment le vol direct de fonds. Dans le cas d'attaques par rançongiciel, les entreprises peuvent se voir contraintes de verser des sommes considérables pour récupérer leurs données critiques. De plus, l'interruption de l'activité due à l'indisponibilité des systèmes informatiques peut entraîner un manque à gagner significatif, paralysant les opérations quotidiennes et impactant directement le chiffre d'affaires.

- **Coûts de remédiation élevés** : à la suite à d'une cyberattaque, les entreprises font face à des coûts de remédiation souvent sous-estimés et pourtant considérables. Ces dépenses comprennent la restauration complète des systèmes informatiques, parfois nécessitant une reconstruction intégrale de l'infrastructure IT. S'y ajoutent les frais liés aux enquêtes forensiques, essentielles pour comprendre l'étendue de l'attaque, identifier les failles exploitées et prévenir de futures intrusions. Enfin, le renforcement urgent de la sécurité implique des investissements imprévus dans de nouveaux outils et solutions, grevant davantage le budget de l'entreprise déjà fragilisée.

« Une attaque réussie peut entraîner des **pertes financières** conséquentes, des **interruptions d'activité**, ainsi qu'une **détérioration de la réputation**, parfois irréparable. »

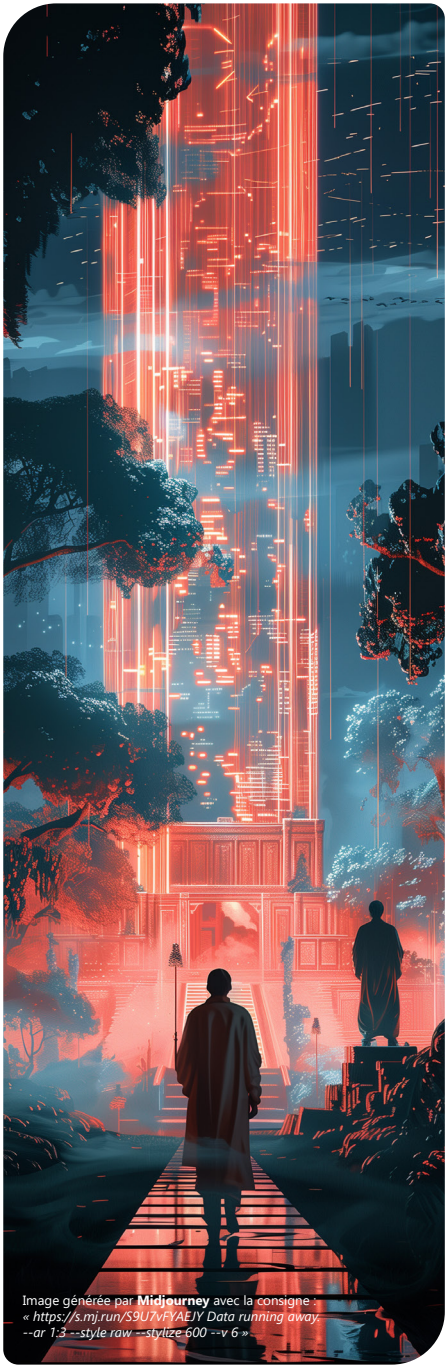


Image générée par **Midjourney** avec la consigne : *« https://s.mj.run/S9U7vFYAEJY Data running away. --ar 1:3 --style raw --stylize 600 --v 6 »*

- **Perte de productivité et de revenus** : l'arrêt temporaire des opérations pendant la phase de remise en état des systèmes entraîne une perte directe de revenus. Même après la reprise partielle des activités, l'utilisation de solutions de contournement ralentit considérablement les processus de travail, affectant l'efficacité globale. Cette période d'instabilité peut également entraîner la perte d'opportunités commerciales.
- **Fuite de données sensibles** : la compromission des données sensibles représente l'un des risques les plus graves pour les PME et ETI victimes de cyberattaques. Cette fuite peut concerner les informations personnelles et financières des clients, exposant l'entreprise à des poursuites judiciaires et à une perte de confiance. Les secrets industriels et la propriété intellectuelle, souvent au cœur de la valeur ajoutée de l'entreprise, peuvent être dérobés, mettant en péril les avantages concurrentiels durement acquis. La perte de brevets, de designs ou d'autres actifs immatériels peut avoir des conséquences désastreuses sur la compétitivité et la pérennité. Bref, s'il ne fallait retenir qu'un chiffre de ce désastre, ce serait celui-ci : 41% des sociétés attaquées ne récupèrent pas 100% des données violées.
- **Atteinte à la réputation** : l'impact d'une cyberattaque sur la réputation d'une entreprise peut être durable et profond, et notamment sur la force morale du ou des dirigeant(s). La perte de confiance des clients et des partenaires commerciaux, suite à la divulgation de l'incident, peut entraîner une érosion rapide de la base clientèle. Les PME et ETI, souvent ancrées dans un tissu économique local, peuvent subir une couverture médiatique négative disproportionnée, amplifiant les dommages réputationnels. Cette atteinte à l'image de marque peut rendre extrêmement difficile l'attraction de nouveaux clients ou partenaires, créant un cercle vicieux qui entrave la croissance et la reprise post-incident.
- **Risques juridiques et réglementaires** : les ennuis débarquant toujours en escadrille, comme disait un ancien président, les conséquences juridiques et réglementaires d'une cyberattaque peuvent être lourdes, exposant les entreprises à des amendes potentiellement élevées pour non-respect des obligations légales en matière de protection des données, notamment dans le cadre du RGPD en Europe.

Les entreprises peuvent également faire face à des poursuites judiciaires de la part de clients ou de partenaires affectés par la fuite de données, entraînant des coûts supplémentaires en frais de justice et en éventuels dédommagements. La gestion des aspects légaux post-incident, incluant les notifications obligatoires aux autorités et aux personnes concernées, ajoute une charge financière et administrative significative. Et c'est sans parler du sentiment de honte que peuvent ressentir les PME contraintes à ce genre d'exercice

- **Impact sur l'emploi** : les répercussions d'une cyberattaque sur l'emploi au sein des PME et ETI peuvent être sévères et durables : 1 PME sur 5 qui se fait attaquer doit licencier. En effet, face aux difficultés financières prolongées suite à l'attaque, certaines entreprises peuvent être contraintes de procéder à des licenciements pour réduire leurs coûts opérationnels. Même en l'absence de licenciements directs, l'instabilité financière peut conduire à un gel des embauches et des augmentations salariales, affectant la capacité de l'entreprise à attirer et retenir les talents nécessaires à sa reprise et à son développement futur.
- **Stress et démotivation des équipes** : à l'instar du poids moral sur les épaules des dirigeants et du management, l'impact psychologique d'une cyberattaque sur les employés ne doit pas être sous-estimé. Le personnel IT, en première ligne pour gérer la crise, subit une pression intense et un stress considérable, augmentant les risques d'épuisement professionnel. L'ensemble des employés peut ressentir une anxiété accrue concernant la sécurité de leurs propres données personnelles et professionnelles, ainsi que des inquiétudes quant à l'avenir de l'entreprise et à la stabilité de leur emploi. Cette atmosphère d'incertitude et de perturbation opérationnelle peut conduire à une baisse significative du moral et de la productivité, affectant la capacité de l'entreprise à se remettre rapidement de l'attaque.

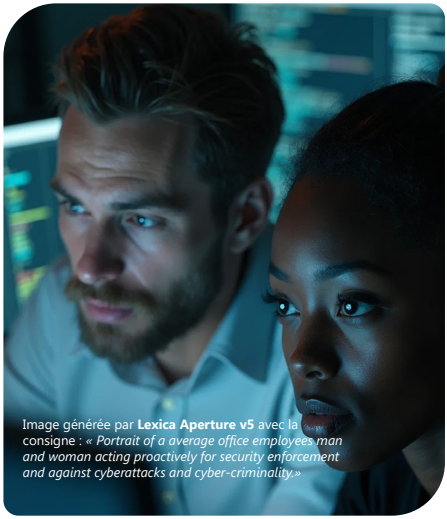


Image générée par **Lexica Aperture v5** avec la consigne : *« Portrait of a average office employees man and woman acting proactively for security enforcement and against cyberattacks and cyber-criminality.»*

- **Risque de fermeture de la société** : s'il n'y a pas de consensus clair sur le pourcentage exact d'entreprises qui ferment à la suite d'une cyberattaque, plusieurs sources indiquent un impact significatif. En effet, le risque de défaillance d'une entreprise augmente d'environ 50% dans les 6 mois suivant un incident cyber. Pour les entreprises françaises spécifiquement, une étude a observé une augmentation de 80% du risque de défaillance dans les 3 mois après l'annonce d'un événement cyber.

Pourtant, malgré l'ampleur de ces menaces, nombreuses sont les entreprises qui peinent encore à développer des stratégies de cybersécurité robustes. De plus, souvent perçue comme une démarche complexe et coûteuse, la prévention est trop fréquemment négligée, au profit de solutions réactives.

Cependant, face à l'évolution constante et rapide des techniques d'attaque, cette approche défensive ne suffit plus. Il est désormais impératif de passer à une stratégie proactive, impliquant non seulement la mise en place de technologies de pointe, mais aussi **une sensibilisation accrue des employés aux enjeux de la sécurité informatique**. Car le maillon faible, il est humain !

Les vulnérabilités humaines : le maillon faible de la cybersécurité

Il ne faut jamais sous-estimer l'importance du facteur humain. En effet, malgré les dispositifs de sécurité les plus avancés, les comportements des utilisateurs peuvent compromettre l'intégrité des systèmes et des données. Les cybercriminels exploitent fréquemment les failles humaines, car elles constituent souvent le chemin le plus aisé pour accéder aux informations sensibles.

Les erreurs, la négligence et le manque de formation des employés sont à l'origine d'une grande partie des incidents de sécurité. Selon certaines estimations, jusqu'à 95 % des attaques réussies sont dues à une erreur humaine. Les utilisateurs, sans le vouloir, peuvent ouvrir la porte aux cyberattaques par des actions simples, telles que cliquer sur un lien suspect, utiliser un mot de passe faible ou partager des informations confidentielles sans précaution.

La gestion inadéquate des mots de passe est l'une des vulnérabilités les plus répandues. Beaucoup d'utilisateurs choisissent des mots de passe faciles à mémoriser, mais également faciles à deviner, comme «123456», «motdepasse» ou des informations personnelles comme la date de naissance. De plus, l'utilisation du même mot de passe pour plusieurs comptes amplifie le risque, car une seule compromission peut entraîner l'accès à plusieurs services.

Le *phishing*, ou hameçonnage, dont nous avons parlé précédemment, est par définition la menace qui exploite la confiance et le manque de vigilance des utilisateurs. Les attaquants envoient des emails ou des messages qui semblent provenir de sources légitimes, comme des banques, des fournisseurs de services ou même des collègues. Ces messages incitent les destinataires à fournir des informations sensibles, à cliquer sur des liens malveillants ou à ouvrir des pièces jointes infectées. Malgré les alertes régulières, le phishing reste efficace, car les messages sont de plus en plus sophistiqués et difficiles à distinguer des communications authentiques.

Images générées par **Lexica Aperture v5** avec la consigne : *« Illustration of a woman and a man pulling their hair off, stressed trying to define an appropriate password, in a modern office environment. »*

Image générée par **Midjourney** avec la consigne : « *Happy office employee at a training course about cyber security. Office environment. Light colored walls decorated with symbols representing computer / IT / internet security threats. --ar 3:2 --style raw --stylize 600 --v 6.* »

D'autres comportements peuvent également mettre en danger la sécurité de l'entreprise. **Le partage non sécurisé de documents**, **l'utilisation de supports de stockage amovibles infectés**, ou encore **le téléchargement d'applications non autorisées** sont autant de pratiques risquées. Avec le développement du télétravail, les employés utilisent souvent des réseaux domestiques ou publics moins sécurisés, augmentant ainsi les possibilités d'intrusion.

La négligence est un facteur déterminant. Le simple fait de laisser un poste de travail déverrouillé en l'absence de l'utilisateur, ou de ne pas appliquer les mises à jour de sécurité recommandées, peut ouvrir des brèches exploitables par des personnes malintentionnées. De plus, le manque de sensibilisation aux bonnes pratiques de sécurité de l'entreprise conduit à des pratiques non conformes qui affaiblissent la posture globale de cybersécurité.

Il est donc essentiel de reconnaître que les employés, à tous les niveaux de l'organisation, sont au cœur de la sécurité informatique. La sensibilisation et la formation régulière des équipes sont indispensables pour réduire les risques liés aux vulnérabilités humaines.

Approches innovantes pour améliorer la sécurité

Pour faire face aux nombreuses menaces qui ciblent les entreprises, il est essentiel d'adopter des stratégies de cybersécurité à la fois technologiques et humaines. Opsky, filiale de Keyrus, se spécialise dans l'accompagnement des entreprises en leur proposant des solutions novatrices pour renforcer leur sécurité. L'approche d'Opsky repose sur une combinaison de mesures préventives, d'outils de pointe et de formation des collaborateurs, dans le but de bâtir une sécurité robuste et durable.

L'un des services phares proposés par Opsky est le «**CISOaaS**» (***chief information security officer as a service***). Ce service permet aux entreprises d'accéder à des experts en cybersécurité à la demande, sans avoir besoin de recruter un responsable de la sécurité informatique en interne.

> « Il est impératif de passer à une **stratégie proactive**, impliquant la mise en place de technologies de pointe, et **la sensibilisation accrue des employés** aux enjeux de la sécurité. »

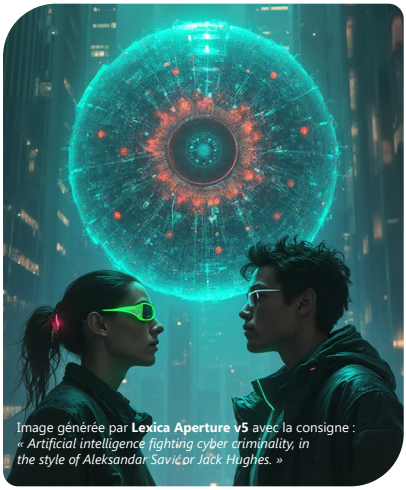


Image générée par **Lexica Aperture v5** avec la consigne : *« Artificial intelligence fighting cyber criminality, in the style of Aleksandar Savić or Jack Hughes. »*

Ce service s'avère particulièrement avantageux pour les PME et ETI qui n'ont pas toujours les ressources nécessaires pour intégrer un expert à plein temps. En externalisant cette fonction, les entreprises peuvent bénéficier d'une expertise sur mesure, alignée sur leurs besoins spécifiques et leurs budgets. Ce service flexible permet une gestion proactive et maîtrisée de la cybersécurité, tout en s'adaptant à la complexité des enjeux numériques.

Opsky mise également sur **la sensibilisation des employés**, un volet essentiel dans toute stratégie de cybersécurité. Elle propose par exemple **des modules de formation interactifs et ludiques** conçus pour capter l'attention et impliquer les participants. Ces formations, d'une durée courte, permettent de sensibiliser les équipes aux risques auxquels elles sont exposées, tout en leur apprenant à adopter les bonnes pratiques.

Traditionnellement, les méthodes de sensibilisation en cybersécurité se limitaient à des séances théoriques, des cours magistraux ou des vidéos explicatives. Bien qu'informatives, ces méthodes manquent souvent d'interactivité et peinent à maintenir l'attention des employés sur le long terme, réduisant ainsi leur efficacité. Face à cette limite, Opsky innove avec de nouvelles approches immersives. Parmi celles-ci figurent des ateliers sous forme de jeux, où les participants peuvent expérimenter de manière ludique des situations de cyberattaque simulée, comme lors d'un escape game, ou participer à des campagnes de phishing intelligentes qui simulent des attaques réelles pour évaluer et améliorer la vigilance des utilisateurs. Opsky utilise également des chatbots éducatifs qui, en temps réel, aident les employés à répondre à des questions de sécurité ou à reconnaître des comportements suspects. Ces méthodes immersives ont montré une efficacité accrue pour ancrer durablement les bonnes pratiques, en rendant l'apprentissage plus concret et engageant.

Parmi les thèmes de formation proposés, on trouve **la gestion des mots de passe**, où les participants, par un jeu consistant à simuler une effraction, découvrent comment créer des mots de passe forts et gérer leur sécurité à l'aide d'outils spécialisés. Un autre module, tout aussi essentiel, est dédié à **la détection des emails de *phishing***. Les employés apprennent à identifier les tentatives d'hameçonnage et à éviter de cliquer sur des liens potentiellement dangereux.

Un autre atelier propose une sensibilisation aux questions de confidentialité des données… ce ne sont malheureusement pas les thématiques sécuritaires qui manquent.

Ces formations sont conçues pour être accessibles à tous les collaborateurs, quel que soit leur niveau de compétence technique, et sont facilement déployables au sein des entreprises. L'objectif est de faire de chaque utilisateur un acteur de la sécurité, conscient des risques et capable de prendre des mesures simples mais efficaces pour éviter les incidents.

En plus des formations, Opsky intègre dans ses services des technologies avancées telles que **l'intelligence artificielle** (IA) et le ***Machine Learning*** (ML) pour renforcer la cybersécurité des entreprises. Ces outils permettent d'analyser d'énormes quantités de données en temps réel et de détecter des comportements anormaux, avant même qu'une attaque ne survienne. L'utilisation de l'IA permet ainsi d'anticiper les menaces, de réagir rapidement et de combler les failles avant qu'elles ne soient exploitées par des cybercriminels. C'est une approche résolument proactive qui garantit une protection continue et optimale.

Opsky propose une offre complète de ***CISO as a Service*** (**CaaS**), permettant aux entreprises, des PME aux Grands Comptes, de gérer efficacement leur cybersécurité tout en maîtrisant leurs coûts. Ce service managé est conçu pour accompagner les organisations dans la gestion de leurs enjeux de sécurité, tout en offrant une flexibilité adaptée à leurs besoins spécifiques. Le modèle CaaS d'Opsky repose sur une approche modulaire, allant de la définition de la stratégie de sécurité (*Build*) à la gestion opérationnelle des systèmes (*Run*).

Grâce à ce service, Opsky prend en charge la gouvernance de la sécurité, la gestion des incidents, la surveillance des vulnérabilités et la mise en conformité réglementaire, des aspects cruciaux pour les grandes entreprises qui doivent souvent se conformer à des réglementations strictes, telles que le RGPD, les directives NIS, DORA ou PCI DSS. En externalisant cette fonction à Opsky, les Grands Comptes peuvent bénéficier d'une expertise de haut niveau, sans avoir à recruter un responsable de la sécurité à temps plein, tout en répondant à leurs besoins de gestion multi-sites et à l'échelle internationale.

Opsky assure également **la résilience** et **la continuité** d'activité en cas de cyberattaque, en mettant en place des plans de continuité (PCA/PRA) et des mesures proactives pour prévenir et atténuer les risques. Pour les grandes entreprises, souvent confrontées à des infrastructures complexes et à une multiplicité d'actifs à protéger, ces services sont essentiels pour garantir une disponibilité continue des systèmes critiques.

Le service CaaS inclut également des actions concrètes telles que **la gestion des incidents de sécurité**, **l'analyse de risques**, **la rédaction de politiques de sécurité**, ainsi que **la sensibilisation des collaborateurs** via des outils interactifs et des simulations avancées. En combinant expertise technique et accompagnement personnalisé, Opsky permet à ses clients, qu'ils soient des Grands Comptes ou des entreprises de taille intermédiaire, de renforcer leur posture de sécurité tout en assurant une gestion optimisée des coûts liés aux investissements en cybersécurité.

Article co-écrit par Keyrus, ChatGPT-4o, Claude, Mistral, Perplexity et Gemini

Image générée par **Lexica Aperture v5** avec la consigne : *« Artificial intelligence fighting cyber criminality, in the style of Aleksandar Savić or Jack Hughes. »*

Vous avez trouvé cette lecture utile ?

Vous aimerez sûrement aussi :

DecSecOps Spéciales

Sécurisez votre code comme un commando

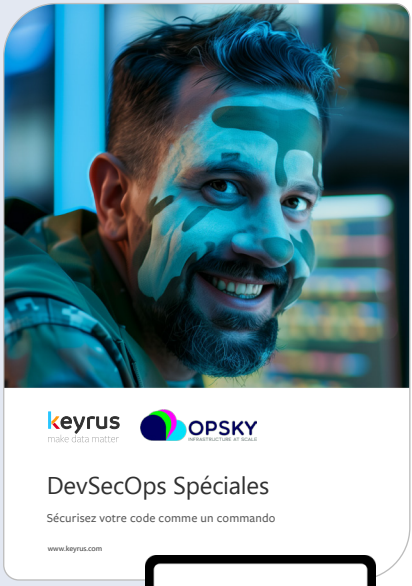
Cet ebook traite de l'approche DevSecOps, qui combine le développement (Dev), les opérations (Ops) et la sécurité (Sec) en un processus intégré. Il met en avant l'importance de cette méthodologie pour améliorer la qualité des logiciels, accélérer les cycles de développement, renforcer la sécurité et optimiser les coûts. Le DevSecOps permet de briser les silos traditionnels entre les équipes, favorisant une collaboration continue et l'utilisation d'outils automatisés. Bien que cette approche présente des défis tels que la gouvernance et le manque de compétences, l'ebook propose des solutions pour une mise en œuvre réussie, illustrées par des études de cas pratiques

Quelles sont les 3 idées principales ?

1. **Intégration continue de la sécurité** : le DevSecOps intègre la sécurité dès le début du processus de développement logiciel, assurant ainsi une protection robuste contre les menaces tout au long du cycle de vie du logiciel. Cette approche proactive permet de détecter et de corriger les vulnérabilités dès les premières phases de développement, réduisant les risques et les coûts liés aux failles de sécurité découvertes en fin de cycle.

2. **Collaboration inter-équipes et automatisation** : on brise les silos traditionnels entre les équipes de développement, d'opérations et de sécurité, favorisant une collaboration fluide et continue. En utilisant des méthodologies agiles et des outils automatisés, les entreprises peuvent réaliser une intégration et un déploiement continus, améliorant ainsi l'efficacité, la qualité et la rapidité du développement logiciel.

3. **Avantages stratégiques et opérationnels** : l'approche DevSecOps permet d'améliorer la qualité des logiciels, d'accélérer les cycles de développement, de renforcer la sécurité des applications, d'optimiser l'utilisation des ressources et de promouvoir des pratiques durables.



SCAN ME

keyrus

make data matter

Acteur international du conseil et des technologies, Keyrus a pour mission de donner du sens aux données, en révélant toute leur portée, notamment sous un angle humain.

Parce que ce ne sont pas tant les données elles-mêmes qui importent, mais les opportunités que nous pouvons développer en les apprivoisant vraiment, nous nous efforçons constamment de comprendre les objectifs que nos clients souhaitent atteindre. Nous explorons et mesurons les comportements, nous les comprenons et les traduisons en un résultat concret. Nous donnons un sens aux réalités que les données portent afin d'aider nos clients à prendre des décisions plus efficaces.

Les données, qu'elles soient grandes, petites, humaines, complexes, historiques ou prospectives, n'ont de sens que lorsqu'elles sont utilisées pour développer les expériences, affiner la compréhension du quotidien et prendre les meilleures décisions.

Notre proposition de valeur est fondée sur cinq grands groupes de services, chacun comprenant des offres multiples :

- **Automatisation et intelligence artificielle** : nous fournissons à nos clients les moyens d'améliorer leur productivité et leur précision sur l'ensemble de leurs processus, afin de se concentrer sur le travail à plus forte valeur ajoutée.
- **Expérience numérique centrée sur l'humain** : la relation avec les clients et l'engagement des collaborateurs constituent deux des plus grands contributeurs au succès global des entreprises. Nous aidons les entreprises à imaginer et à créer des expériences numériques multimodales et fluides pour atteindre leurs objectifs.
- **Mise en œuvre des données et des analyses** : les données sont une clé incontestable du succès pour les entreprises. Lorsqu'elles sont utilisées intelligemment, elles ouvrent des opportunités uniques pour faire face aux défis actuels et futurs. Nous permettons aux organisations de déployer tout le potentiel de leurs données : nous mettons la science des données au profit du développement de l'entreprise.
- **Cloud et sécurité** : le Cloud et les plateformes numériques ont le potentiel de révolutionner la façon dont les données sont transformées en valeur, tout en portant l'extensibilité et la flexibilité à un niveau supérieur. Nous sécurisons l'ensemble de vos données et veillons à ce qu'elles soient protégées et confidentielles.
- **Transformation et innovation** : pour prospérer dans l'écosystème actuel, chaque entreprise doit non seulement accélérer sa transformation numérique, mais aussi acquérir des compétences pour stimuler son adaptabilité, sa résilience et sa compétitivité. Nous aidons nos clients à se transformer avec succès pour développer un meilleur futur.

S'appuyant sur l'expérience cumulée de plus de 3 500 collaborateurs et présent dans 27 pays sur 4 continents, Keyrus est l'un des principaux experts internationaux en matière de données, de conseil et de technologie.

Pour en savoir plus : **www.keyrus.fr**

Jean-Philippe CLAIR
Directeur Marketing, Communication & Expérience client
jean-philippe.clair@keyrus.com