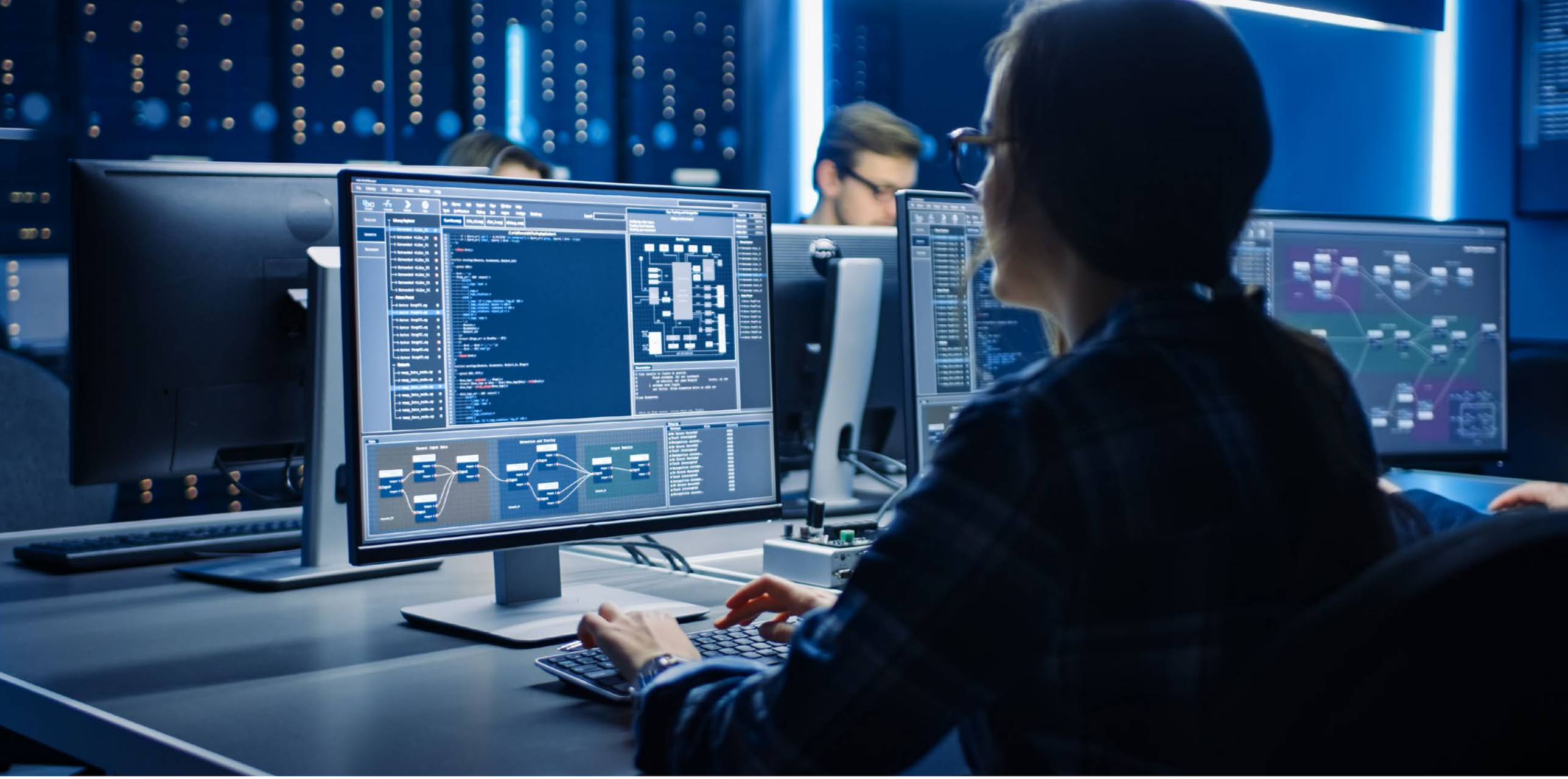


Sécurité et résilience : une priorité essentielle

Les solutions Alcatel-Lucent Enterprise pour le secteur public

Alcatel·Lucent Enterprise

Livre blanc

Sommaire

| Présentation

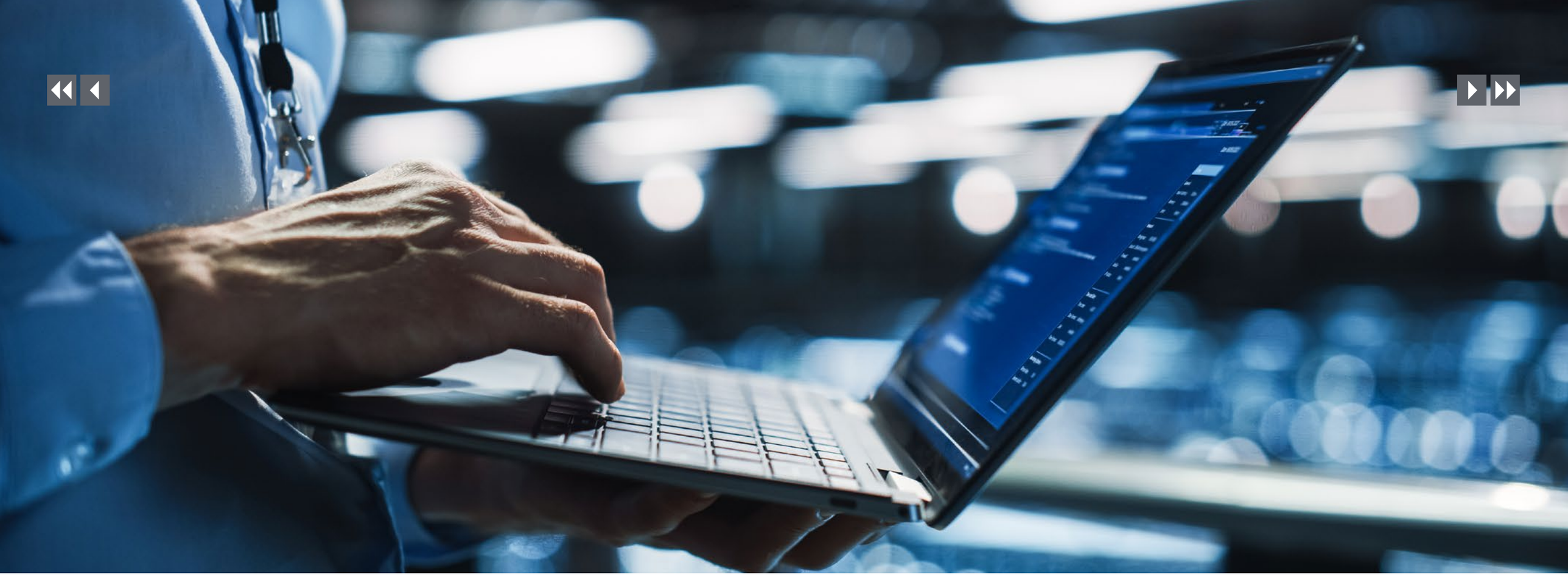
| Pourquoi la collaboration entre les technologies de l’information et les technologies opérationnelles est-elle essentielle

| Des infrastructures réseau résilientes et sécurisées

| Rendre les infrastructures de communications résilientes

| Protéger les personnes et les équipements

| Souveraineté et sécurité des données



Présentation

Face aux défis mondiaux croissants et à l'augmentation des cyberattaques, les authorités doivent donner la priorité à la gestion des risques, sauvegarder les infrastructures critiques et protéger les citoyens. De janvier à décembre 2024, l'ANSSI a traité 218 incidents cyber affectant les collectivités territoriales, soit une moyenne de 18 incidents par mois[1]. L'objectif est la reprise d'activité le plus rapidement, quelle que soit la situation et que les citoyens et leurs données soient en sécurité. Dans le climat mondial actuel, il est plus important que jamais de maintenir la sécurité, la souveraineté des données et de garantir la disponibilité des services.

La transformation numérique du secteur public

Ces dernières années, la transformation numérique des services publics s'est accélérée, offrant à un nombre croissant de citoyens un accès aux services en ligne. La transformation numérique a également permis aux agents de travailler en tout lieu. Les services publics sont de plus en plus contraints d'accélérer davantage la transformation numérique. Selon un article de Deloitte, 77% des services publics affirment que les initiatives de transformation numérique lancées pendant la pandémie ont déjà un impact positif sur leurs organisations.

Alcatel-Lucent Enterprise travaille avec des services publics du monde entier et reconnaît l'importance de protéger les citoyens, les opérations et les bâtiments contre les risques cybernétiques et physiques. Nos solutions prennent en compte la sécurité et la confidentialité des données à chaque étape du processus de conception et sont construites avec des options résilientes pour s'adapter à chaque type d'organisation. Ce livre blanc fournit des informations sur la résilience et la sécurité de vos solutions de communications, de cloud et de réseau proposées par ALE.

1 CERT-FR : Collectivités territoriales - Synthèse de la menace, https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-002/
2 https://www2.deloitte.com/uk/en/insights/industry/public-sector/government-digital-transformation-strategy.html.

Pourquoi la collaboration entre les technologies de l'information et les technologies opérationnelles est essentielle

Avant de regarder comment améliorer la résilience et la sécurité voyons comment la relation entre les technologies de l'information et les technologies opérationnelles a évolué. Dans le passé, les équipes informatiques et opérationnelles ne collaboraient pas étroitement, chacune avait ses propres fonctions et responsabilités. Ces deux mondes convergent aujourd'hui et doivent travailler ensemble. Les équipes informatiques et opérationnelles qui ne connaissent pas les activités des uns et des autres, ou qui ne sont pas coordonnées et ne collaborent pas entre elles, mettent en péril l'ensemble de l'organisation.

Considérons, par exemple, le grand nombre d'objets connectés qui sont rapidement déployés dans de nombreux services publics et villes intelligentes. Lorsque le service informatique n'est pas informé de la mise en œuvre de nouveaux objets connectés par l'équipe opérationnelle, il ne peut pas s'assurer que ces appareils sont conformes aux politiques de sécurité de l'organisation. Les objets connectés sont dotés de niveaux de cybersécurité très variables. Ils peuvent ne pas être équipés des mécanismes de protection les plus récents, ou leurs capacités peuvent ne pas avoir été pleinement mises en œuvre. Ces appareils informatiques « fantômes » non autorisés peuvent utiliser n'importe quel logiciel et être infectés par des virus et des programmes malveillants. S'ils ne sont pas contrôlés, ils peuvent facilement introduire de nouvelles vulnérabilités et de nouveaux vecteurs d'attaque dans le réseau. Nous assistons aujourd'hui à l'émergence d'une collaboration IT/OT nécessaire pour assurer la sécurité et la résilience des réseaux.

Des infrastructures réseau résilientes et sécurisées

L'infrastructure réseau fait partie intégrante des activités des organismes gouvernementaux et des services publics. L'interruption ou les perturbations des services réseau peuvent avoir de graves conséquences en raison de la nature sensible des informations contenues dans les réseaux des services publics ou régaliens. Ainsi, la résilience et la sécurité sont une priorité. Des réseaux fiables et sécurisés sont essentiels pour permettre aux authorités de fournir des services efficaces, de protéger les informations sensibles et de garantir le bon déroulement des opérations.

Les solutions d'infrastructure réseau d'ALE sont résilientes et vont au-delà de ce qu'offrent de nombreux autres fournisseurs de technologie. Nous intégrons la sécurité dans nos solutions dès les premières étapes de la conception, sans coûts de licence supplémentaires.

6 meilleures pratiques pour sécuriser vos infrastructures réseau

1. **Adopter une stratégie de sécurité Zero Trust** La macro et la micro segmentation de votre réseau sont essentielles pour maintenir une infrastructure résiliente. Une approche progressive de la micro-segmentation garantit une bonne mise en œuvre et prévient les perturbations.
2. **Envisager d'adopter une solution de Shortest Path Bridging (SPB)** pour la redondance et la sécurité, car cette approche réachemine dynamiquement le trafic en utilisant plusieurs chemins en cas de défaillance, tout en créant un réseau efficace et conteneurisé. SPB renforce la sécurité grâce à l'encapsulation MAC-in-MAC, qui élimine les adresses IP afin d'empêcher les attaques par usurpation d'adresse IP ou par analyse des paquets.
3. **Envisager d'exploiter les capacités du châssis virtuel pour améliorer la fiabilité dans les zones critiques.** Cela permet la redondance et la résilience du réseau, tout en prenant en charge les mises à jour logicielles en service (ISSU) et en permettant des interconnexions mesh ou en ring dédiées. Le châssis virtuel constitue une solution économique pour simplifier la gestion du réseau tout en assurant une haute disponibilité.
4. **Envisager de mettre en œuvre le protocole de redondance des routeurs virtuels (VRRP).** VRRP améliore la résilience du réseau en fournissant un routeur virtuel de secours qui peut prendre le relais en toute transparence en cas de défaillance du routeur principal.
5. **Déployer une solution qui garantit que vous disposez de toutes les sauvegardes des configurations** des switch réseau et que vous serez en mesure de les restaurer dans le pire des cas, ou lorsque vous en aurez besoin.
6. Une mesure de sécurité complémentaire consiste à **avoir un code sécurisé et diversifié** qui randomise l'emplacement des différents segments de code sur vos switch, ce qui accroîtra considérablement la sécurité. Cela peut être associé à une vérification indépendante et à un processus de validation. Ces processus sont menés par un expert en cybersécurité tiers qui analyse et teste le système d'exploitation afin d'identifier et d'éliminer toutes les vulnérabilités potentielles, les portes dérobées, les programmes malveillants ou les exploits de système.

Justifier les investissements dans une infrastructure sécurisée

Investir pour garantir la résilience et la sécurité de votre réseau est toujours judicieux. Cependant, il peut être complexe et long de comprendre où il est préférable d'investir - donc la planification est essentielle. Avant de commencer, voici quelques points clés à prendre en compte pour garantir la sécurité et la résilience dont votre entreprise a besoin :

- **Revoyez et mettez à jour la conception de votre réseau** afin de vous assurer que les exigences de votre entreprise sont prises en compte dans le réseau. Il en est de même pour le niveau approprié de résilience pour les zones sensibles et critiques qui ont un impact sur les services publics essentiels. **Pour les zones critiques**, prévoyez d'ajouter des serveurs de sauvegarde et des connexions multiples lorsque cela est possible et applicable.
- **Tenez compte de l'importance croissante du temps de réponse en cas d'incident :** par exemple, nous utilisons des fonctionnalités d'intelligence artificielle (IA) et d'apprentissage automatique (ML) pour notre Alcatel-Lucent OmniVista Network Advisor afin d'identifier et de résoudre les problèmes plus rapidement. Cet outil permet de résoudre les problèmes avant qu'ils n'affectent les utilisateurs finaux, en identifiant et en traitant de manière proactive les problèmes de réseau ou de sécurité. Il facilite le dépannage et améliore la sécurité du réseau grâce à des audits de configuration et à l'administration d'alertes en temps réel pour tout changement soudain observé dans le comportement du réseau.
- Pensez à installer des **switch durcis pour les environnements difficiles**. La gamme de switch Ethernet durcis d'Alcatel-Lucent Enterprise est spécialement conçue pour exceller dans des environnements difficiles et soumis à des températures extrêmes. Ces switch sont fabriqués avec des composants résistants et protégés par des boîtiers solides, ce qui garantit leur durabilité et leur fiabilité. Ils sont dotés du même système d'exploitation que le reste des commutateurs ALE. Pour renforcer la sécurité et protéger les informations sensibles, certains modèles de switch sont équipés d'alertes d'intrusion et de relais d'alarme qui permettent de connecter des systèmes d'alarme externes. Certains modèles prennent même en charge MACsec pour sécuriser les communications de données entre les deux extrémités. Grâce à la capacité de châssis virtuel des switch durcis, vous pouvez améliorer la redondance, la résilience et l'évolutivité.

Rendre les infrastructures de communications résilientes

Les communications sont essentielles pour permettre aux services publics d'interagir avec les citoyens, les parties prenantes de de l'organisation et les autres services, ainsi que pour la diffusion d'informations importantes. Les systèmes de communication doivent être disponibles en temps de crise, lorsque les citoyens ont le plus besoin d'aide. La résilience et la sécurité évoluent, et des révisions périodiques vous aideront à maintenir la sécurité et la disponibilité de votre solution de communication Alcatel-Lucent Enterprise.

Les solutions de communication ALE sont sécurisées dès leur conception. Cela signifie que nous prenons en compte la sécurité à chaque étape dès la conception, du développement et de la livraison du produit. Tout le matériel et les systèmes d'exploitation sont renforcés, et la protection contre les attaques par déni de service (DoS) est intégrée. Nous nous conformons aux certifications et accréditations reconnues pour les normes mondiales en matière de sécurité et de confidentialité (ISO 27001, ISO 27017 et ISO 27018). En outre, nous respectons les normes de sécurité et de confidentialité propres aux secteurs d'activité, telles que la certification HDS (Hébergeurs de Données de Santé) pour l'hébergement des données médicales en France. Ou la Certification Services Premier Niveau de l'ANSSI. Nous respectons aussi les normes régionales de sécurité et de confidentialité, telles que le règlement général sur la protection des données (RGPD) au sein de l'Union européenne.

6 bonnes pratiques pour sécuriser vos solutions de communication

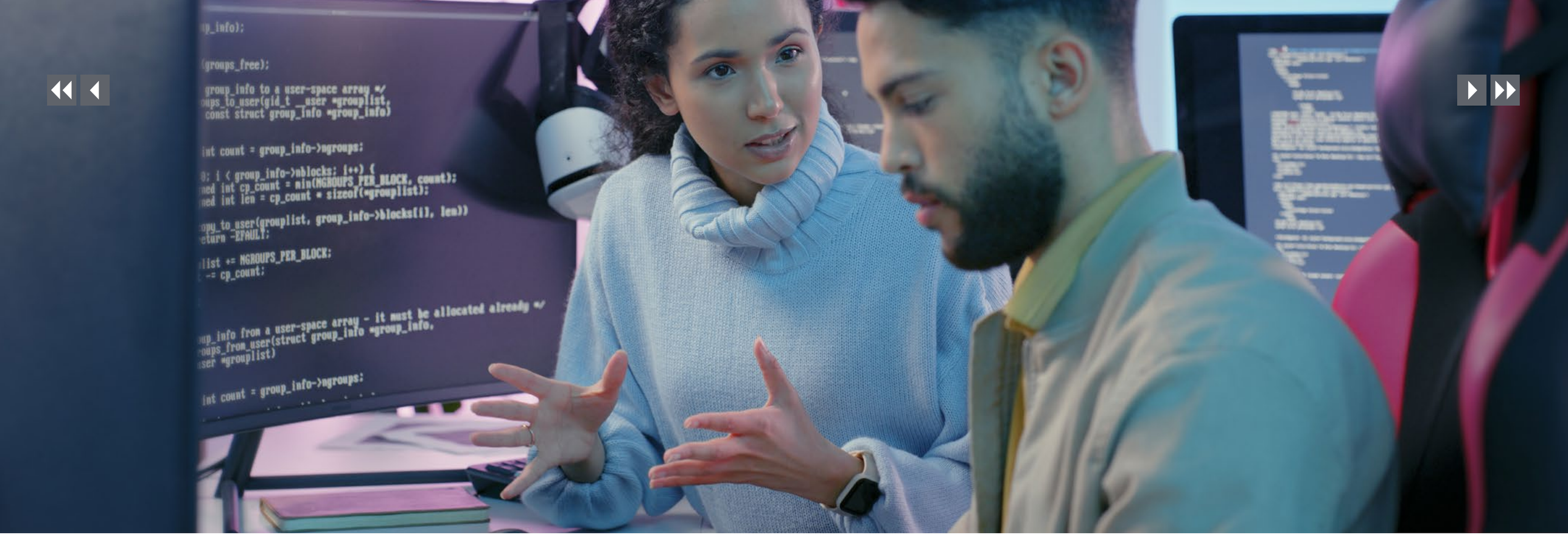
Voici 6 bonnes pratiques pour vous aider à optimiser la résilience et la sécurité de vos solutions de communication ALE.

1. Veiller à disposer de **la dernière version du logiciel ou des correctifs appropriés** afin de bénéficier des dernières améliorations en matière de sécurité pour une meilleure protection.
2. Envisager une solution qui intègre l**a surveillance d'alarmes** et effectuer les mises à jour régulières avec les bons seuils. Vérifier si les notifications relatives aux défaillances du système de communication ou aux alertes de qualité sont envoyées aux personnes concernées.
3. Examiner et appliquer une **politique de mot de passe durci**, de préférence en utilisant l'authentification externe avec un serveur RADIUS. Mettre en place des rappels pour les utilisateurs afin de prévenir la fraude téléphonique, qui reste une menace dans de nombreux pays.
4. **Sensibiliser les employés à la sécurité** et s'assurer qu'ils sont conscients des risques et des mesures de prévention
5. S'assurer de **disposer d'une sauvegarde automatisée du système à distance** pour éviter la perte des données de configuration
6. Envisager **un VLAN spécifique pour la voix.** En séparant la voix du reste du trafic, on réduit le risque de contamination qui pourrait perturber les opérations et éventuellement les services gouvernementaux.

Comment renforcer les sécurité de votre infrastructure de communications

Avant d'investir dans une solution de communication, voici quelques points clés à considérer pour renforcer la résilience et la sécurité de votre organisation :

- **Une architecture redondante et résiliente.** Votre architecture doit être entièrement redondante et résiliente. La duplication des serveurs d'appels dans les zones critiques, la mise en œuvre d'une redondance des sites distants et la duplication des serveurs d'applications critiques peuvent fournir une protection supplémentaire.
- Créer un workflow à l'aide de Rainbow et/ou Visual Notification Assistant (VNA) d'Alcatel-Lucent Enterprise avec des déclencheurs automatiques (déclencheur humain, IoT ou système) pour avertir les principales personnes des problèmes du système afin qu'elles agissent rapidement et accélèrent le processus de récupération.
- Déployer un puissant **système de cryptage**. Le cryptage repose sur des normes industrielles élaborées de manière native dans la solution, sans aucun impact sur la qualité et les performances vocales.



- Essayer Rainbow™ par Alcatel-Lucent Enterprise, l'outil de collaboration idéal pour compléter les solutions de communication ALE. Rainbow offre un ensemble complet de fonctionnalités, notamment la voix, la vidéo et la messagerie instantanée, permettant des communications transparentes et une collaboration efficace. Avec Rainbow, vous pouvez échanger des images, des vidéos et des flux de vidéosurveillance, ce qui améliore la connaissance du contexte et permet de prendre de meilleures décisions. Rainbow fournit également des communications hybrides avec une connectivité sécurisée entre les sites et le cloud. Il garantit des communications résilientes, vous permettant de rester en contact avec vos collègues et vos clients en utilisant Rainbow, offrant une connectivité ininterrompue même dans des situations difficiles. Les communications hybrides présentent également l'avantage de permettre aux opérations cloud et ceux sur site d'être exécutées à partir de sites différents, ce qui garantit une résilience optimale et permet de maintenir des communications ouvertes.
- Pour les services ayant des exigences de sécurité plus strictes, Rainbow Edge offre **une alternative sur site avec une instance cloud privée.** L'instance peut être hébergée dans n'importe quel centre de données, offrant un contrôle total sur les serveurs, le stockage et les réseaux. Cela permet aux services de personnaliser et de configurer l'infrastructure en fonction de leurs besoins. Des politiques de sécurité personnalisées peuvent être mises en œuvre et les ressources peuvent être gérées de manière autonome. Ce niveau de contrôle offre une visibilité et une autorité totales sur l'infrastructure, ce qui permet aux agences de prendre des décisions éclairées et d'optimiser les performances en fonction de leurs objectifs.
- Définir une stratégie de communication sécurisée pour le personnel distribué ou sur le terrain.ALE offre de multiples options de communication et de collaboration pour les employés distribués, mobiles et travaillant à domicile, notamment :
  - Rainbow
  - IP Desktop softphone
  - ALE SoftPhone
  - Deskphone avec VPN intégré et peut être déployé en masse avec une sécurité intégrée (VPN)

Protéger les personnes et les équipements

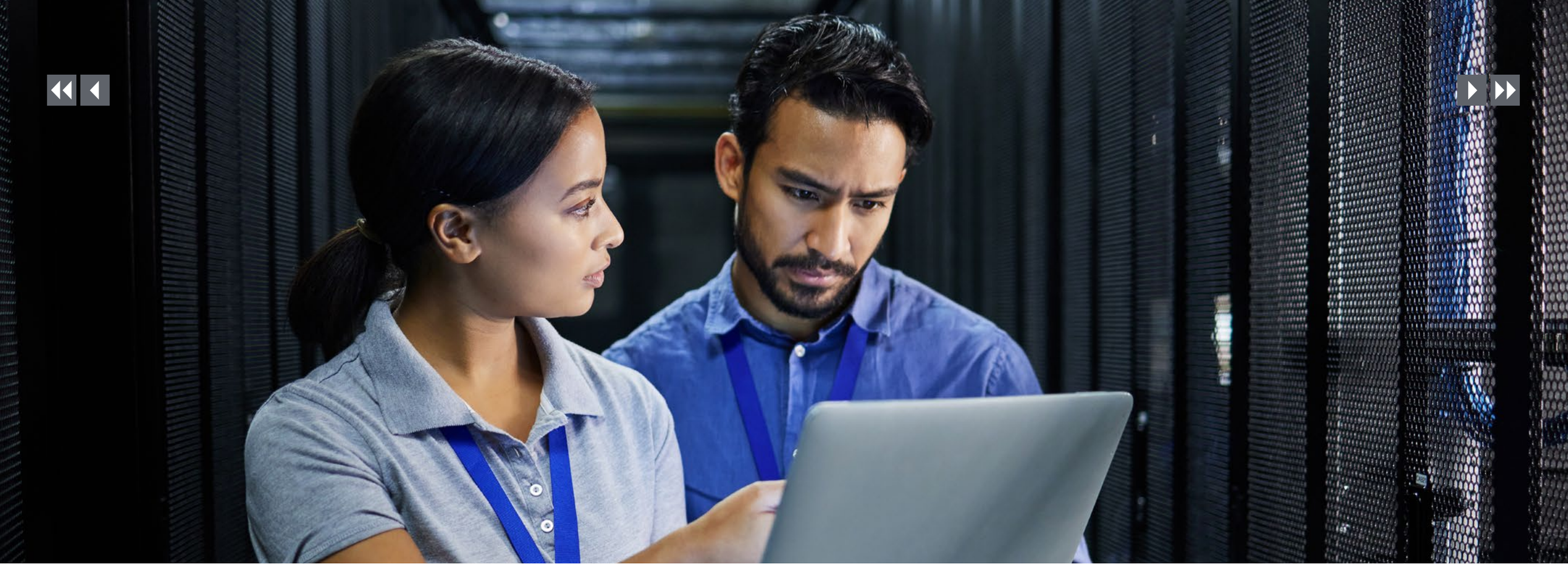
ALE offre des systèmes de communications et de notification flexibles, sécurisés et hautement accessibles en temps réel. Ces solutions s'intègrent aux opérations des centres de contrôle de la sécurité publique ou des villes intelligentes en améliorant la gestion des appels, la contextualisation des données IoT et la collaboration entre premiers intervenants et parties prenantes, pour une meilleure prise de décision et coordination.

La capacité d'interconnecter les terminaux IoT au sein des bâtiments, des sites et des villes, combinée à l'analyse et à l'IA, transforme fondamentalement le paysage des communications. Grâce à l'intégration de capteurs, de la vidéosurveillance, du flux de travail Rainbow et de l'IA, il est possible de passer d'une approche réactive à une approche proactive, ce qui améliore l'efficacité des processus en termes de temps et de coûts. Cette intégration facilite une compréhension globale du contexte, soutient les processus de prise de décision et réduit par conséquent les délais d'intervention en cas d'urgence. En outre, des fonctionnalités telles que **le suivi des équipements et le contrôle des serrures et des lumières intelligentes**, rationalisent les opérations. Par ailleurs, l**a possibilité d'enregistrer les communications et les actions** simplifie l'analyse post-événement, ce qui améliore les processus de sécurité et permet de limiter les responsabilités potentielles. Pour réaliser ces avancées, il est essentiel de disposer d'un environnement connecté avec un accès Wi-Fi omniprésent et une intégration sans effort de l'IoT.

Pour les plateformes de communication en temps réel sensibles au facteur temps, sécurisées et extrêmement disponibles, une infrastructure performante est vitale pour garantir des opérations sans faille. Votre infrastructure doit inclure des logiciels adaptés, des protocoles réseau hautement disponibles, ainsi que la flexibilité requise pour intégrer, en toute transparence, **des commutateurs réseau performants, capables de résister à des conditions difficiles,** telles qu'une circulation d'air limitée, des chocs et des températures extrêmes. Le choix d'un équipement résistant garantit la longévité dans des lieux difficiles où un équipement non résistant présenterait une durabilité moindre.

Dans le domaine des systèmes de sécurité physique, les enjeux sont importants. Chaque minute et chaque élément de la séquence vidéo peuvent être déterminants pour les autorités dans le cadre de l'identification d'un acte répréhensible, de la localisation de la source d'un incident ou de la compréhension de la cause d'une catastrophe. Une infrastructure de vidéosurveillance performante est essentielle. L'infrastructure réseau doit non seulement fournir une bande passante suffisante et une alimentation électrique par câble Ethernet (PoE) pour les caméras de surveillance, mais aussi s'intégrer de manière transparente aux systèmes de gestion de la vidéosurveillance. Cette intégration garantit un réseau de surveillance efficace et fiable avec un fonctionnement fluide et un dépannage facile. L'équipe opérationnelle doit être capable de résoudre rapidement tout problème vidéo, en particulier dans des environnements où chaque image vidéo est capitale. Les possibilités d'intégration de la solution OmniSwitch® d'Alcatel-Lucent Enterprise par le biais de plugins avec les principaux systèmes de gestion vidéo, vous permettent d'atteindre cet objectif majeur.

En outre, dans certaines situations, il est nécessaire de procéder au **suivi des équipements ou de localiser des personnes ou des équipements** au sein de votre organisation. Une solution de suivi des équipements efficace dépend de sa capacité à localiser facilement et avec précision les personnes et les équipements. Un tel système améliore également la sécurité et la sûreté en permettant l'envoi rapide d'une assistance lorsque la localisation des personnes est avérée. Grâce à la solution de suivi des équipements OmniAccess® d'Alcatel-Lucent Enterprise, le personnel et les équipements peuvent être localisés rapidement et affichés sur un plan d'étage. Le suivi des équipements fournit également des informations sur les schémas d'utilisation. Savoir si les équipements sont surutilisés ou sous-utilisés peut fournir des informations précieuses.



Souveraineté et sécurité des données

Alcatel-Lucent Enterprise dépasse les autres fournisseurs de technologie, en mettant en œuvre les meilleures pratiques requises pour une cybersécurité de bout en bout. Chez ALE, nous :

- veillons à ce que nos produits obtiennent les principales certifications industrielles, telles que HDS, CSPN, HIPAA
- ALE International se conforme à la directive de l'Union européenne relative à la sécurité des réseaux et de l'information (NIS 2)
- suivons les meilleures pratiques et recommandations du National Institute of Science and Technology (NIST) lors de l'évaluation des risques liés aux nouvelles fonctionnalités et lors de la mise en œuvre de fonctions de cybersécurité, telles que le cryptage natif, dans nos solutions
- possédons la certification Critères Communs EAL2+
- respectons des normes ISO 27001 appliquées à toutes nos solutions basées sur le cloud
- prenons en charge le modèle ZTNA, correspondant à la segmentation granulaire du réseau et à des politiques de sécurité très spécifiques afin de réduire le risque d'activités non autorisées
- procédons à des tests hautement spécialisés et spécifiques en matière de sécurité, tels que des tests de pénétration, sur nos produits.

En tant qu'experts reconnus en matière de cybersécurité, nous contribuons aux propositions de directives de l'Union européenne sur la cybersécurité. Nous mettons également à profit notre expertise en matière de cybersécurité pour aider nos clients à choisir et à mettre en œuvre la bonne combinaison de solutions de communications unifiées et de collaboration sécurisées pour répondre à leurs besoins. Nous formons également leurs employés aux meilleures pratiques en matière de cybersécurité.

Alcatel·Lucent
Enterprise