ADITEL news

LE JOURNAL D'INFORMATION DE L'ASSOCIATION ADITEL | #14 | JUIN 2021

LES LECONS DE LA CRISE

Édito de Didier Moreau, président d'Aditel

En abordant 2021, nous nous doutions bien que cette année serait encore difficile. Mais imaginer que le forum 2021, notre trentième forum, serait encore incertain ne faisait pas partie des hypothèses. Pourtant, au moment d'écrire ces lignes, nous ne savons toujours pas dans quelles conditions il se déroulera. Déjà, devant l'évolution de la situation, nous avions décidé de tenir notre assemblée générale en juin, mais en distanciel.

REPENSER LA SÉCURITÉ

Malgré ces rebondissements, la vie d'Aditel continue plus que jamais, et nous avons des enseignements à tirer de cette crise. Dans nos métiers, elle nous a appris à réagir vite, à chercher de nouvelles solutions. C'est pourquoi il nous a paru intéressant de consacrer le dossier de cette newsletter aux réflexions qu'elle a pu susciter sur la sécurité de demain dans les agences, d'autant que les dernières innovations dans ce secteur « boostées » par l'intelligence artificielle ont parfois l'air miraculeuses.

CONTROVERSE

Le CNAPS ayant considéré que les services de maintenance d'automates sans accompagnement devaient être assimilés à une activité de transports de fonds, les sociétés exerçant cette activité ont sollicité l'autorisation du CNAPS, qui leur a été délivrée. Opposés à cette décision, les transporteurs de fonds demandent l'annulation de ces autorisations. Ils ne souhaitent pas voir un jour les constructeurs approvisionner les automates. Le pas à franchir n'est plus si grand maintenant qu'ils ont l'agrément. De leur côté, les constructeurs d'automates souhaitent conserver une part de marché que les transporteurs leur convoitent de plus en plus. La lutte s'annonce rude.

LÉGISLATION

La Commission européenne émet une proposition de règlement pour encadrer l'intelligence artificielle dont une des applications, la reconnaissance faciale, fait l'objet de nombreux débats et critiques. L'IA a profondément bouleversé le monde de la sécurité électronique, les usages des technologies et les solutions développées par les acteurs du marché. A tel point que les autorités européennes s'inquiètent de plus en plus des dévoiements possibles de cette révolution technologique.

INSTALLATEURS D'ALARMES ET SÉCURITÉ GLOBALE

A l'occasion de l'examen de sur la loi sur la sécurité globale, la question de l'ouverture du périmètre du Code de sécurité intérieure aux sociétés d'installation est à nouveau débattue.

En 2015, le projet d'ouvrir le périmètre du livre VI du Code de la sécurité intérieure aux sociétés d'installation fut abandonné en raison des difficultés rencontrées. Pourtant, le risque de sécurité est réel : un technicien malveillant ayant accès à la programmation des centrales d'alarme peut causer de lourds dégâts en prenant la main à distance. Les interconnexions entre les systèmes d'alarme et les réseaux informatiques de la banque créent de surcroît un risque d'intrusion.

Ce sujet controversé revient sur le devant de la scène à l'occasion de la discussion de la loi « pour une sécurité globale préservant les libertés » (PPL). Son article 19, qui demande la « *production par le gouvernement d'un rapport à remettre auprès du Parlement, dans un délai de 18 mois à compter de la promulgation de la loi, sur l'opportunité de l'ouverture du périmètre du CSI à certaines activités et notamment aux activités de conception, d'installation et de maintenance de systèmes de sécurité électronique (volet moralité + aptitude professionnelle)* », a été écarté par les sénateurs en première lecture, avant d'être réintroduit par la commission mixte paritaire*.
Le risque dans les banques est très sérieux, car il leur faut à la fois sécuriser la qualité des intervenants ayant accès à la programmation des centrales et maintenir une diversité d'intervenants pour tous les travaux de préparation, d'installation ou de maintenance des périphériques. La communauté bancaire doit continuer à suivre attentivement ce sujet.

*La CMP est composée de 14 membres titulaires et de 14 membres suppléants, dont 4 rapporteurs (les députés A. Thourot et J.-M. Fauvergue et les sénateurs M.-Ph. Daubresse et L. Hervé) se sont accordés sur une rédaction du texte le 29 mars.

LES FAILLES DES SYSTÈMES DE GESTION DES BÂTIMENTS

Presque tous les grands ensembles immobiliers, dont les sièges de banques, sont aujourd'hui équipés d'un système de gestion technique de bâtiment (GTB), qui administre les fonctions vitales nécessaires au bon fonctionnement de l'immeuble (climatisation, température, éclairage). Il peut aussi assurer la protection incendie et d'autres équipements mécaniques ou électriques importants, comme les ascenseurs et le contrôle d'accès. De plus en plus en plus souvent connectés au réseau des entreprises et à Internet, ces systèmes apportent des bénéfices considérables aux exploitants, surtout sur le plan énergétique, mais ils sont exposés au risque de cyberattaques. Les hackers peuvent sans difficulté exploiter les failles de sécurité, si elles existent, pour modifier, par exemple, la température des pièces, au risque de mettre en péril des équipements et bloquer le fonctionnement de certaines activités. C'est le cas des data-centers qui ont besoin d'être maintenus dans un environnement entre 17 et 27 °C. Les conséquences d'un piratage informatique peuvent être nombreuses : pannes, destruction de l'installation, incendie, mise en danger de la vie des personnes présentes, etc. De la même façon, la sécurité physique des bâtiments peut être atteinte. Ces dangers, encore largement sous-estimés, ont fait l'objet, en juillet 2019, d'un avertissement du ministère américain de la sécurité intérieure.

UN CONCEPT SÉDUISANT D'ANALYSE VIDÉO

ESI, spécialisé dans la réception d'images vidéo multi-protocoles sur un frontal de dernière génération installé chez le télésurveilleur, a développé un nouveau module logiciel. Ce système, AV1, possède 3 grandes fonctionnalités qui répondent parfaitement aux préoccupations de la banque :

- La reconnaissance d'objets et de comportements permettant la qualification de clips vidéo reçus et la discrimination de fausses alarmes.
- La vérification et le pointage des caméras, ainsi que la détection d'objets déposés ou enlevés, au travers de rondes vidéo cycliques.
- La reconnaissance d'objets et de comportements avec génération d'alarmes durant des rondiers vidéo automatiques réalisés en tâche de fond ou de façon aléatoire.

La reconnaissance comportementale intègre la notion de gestes, d'actions, de barrières franchies, de comptage, mais aussi la reconnaissance faciale. La recherche *a posteriori* d'individus sur différentes caméras enregistrées est en cours de finalisation. En toute logique ce système permettrait d'utiliser les caméras de l'agence pour faire de la détection de mouvement à la place des détecteurs traditionnels. Il serait également possible de faire des rondes vidéo à l'ouverture pour lister les personnes filmées et s'assurer qu'elles font partie de l'agence avant d'envoyer une alarme agression au télésurveilleur. Le but : dépolluer les stations de télésurveillance à l'ouverture.

INNOVATION

Advantech et Actility lancent un nouveau capteur de vibrations intelligent intégré à la plateforme IoT ThingPark Enterprise. Le capteur surveille les températures de surface et calcule leurs valeurs de vibration et leurs caractéristiques pour les applications de maintenance prédictive. Ne faut-il pas voir dans cette innovation le détecteur sismique, placé sur les chambres fortes, de demain ?

IL L'A DIT

Le président de la banque centrale américaine craint plus une cyberattaque à grande échelle qu'une crise financière mondiale. Les risques d'une crise ressemblant à celle dite des subprimes « sont très, très faibles », a déclaré Jerome Powell au cours de l'émission 60 Minutes sur la chaîne CBS News.

SANS CONTACT

La Covid a donné l'idée à un fabricant berlinois (Bird Home Automation) de développer un interphone vidéo IP sans contact (DoorBird modèle D2101WV). L'appareil détecte les gestes à une distance de 10 centimètres et envoie un signal de sonnette à un carillon IP ou à un moniteur intérieur. Il est censé protéger contre la Covid les personnes qui l'utilisent. Jusqu'où ira-t-on dans ce domaine ?

La sécurité demain

Face aux mutations rapides qui touchent la société dans son ensemble, les acteurs de la sécurité sont confrontés à de nouveaux défis qui exigent de se réinventer et d'imaginer de nouvelles réponses. Un nouveau monde se prépare, dans lequel les technologies, et en particulier l'intelligence artificielle, joueront à n'en pas douter les premiers rôles.

Le nouveau paradigme de la sécurité

En quelques années, sous l'effet d'une succession d'événements qui ont marqué l'actualité, il semble que nous soyons entrés dans un nouvel âge de la sécurité. Cette évolution impose une réflexion sur de nouvelles stratégies.

Culturellement, la direction de la sécurité-sûreté concentrait le maximum de ses efforts dans la protection des valeurs entreposées dans les agences et dans la sécurité du personnel. Régulièrement, en fonction des circonstances, les différents acteurs revoyaient certaines lignes de leur stratégie pour faire face à de nouvelles situations… jusqu'au jour où survint l'attentat contre le journal satirique Charlie Hebdo. Dans les mois qui ont suivi ce tragique événement, nous sommes entrés dans une période de transformation a amenés à changer de paradigme dans la façon de penser la sécurité. D'autant plus que de nouveaux événements se sont produits – attentat du Bataclan presque un an après, montée de l'islamisme dans les entreprises… – auxquels est venue s'ajouter la crise sanitaire début 2020. Le plus inquiétant concernant la Covid-19 est la détérioration du climat social, perceptible à un certain nombre de signaux alarmants, comme la montée de la violence et les comportements incivils. Parallèlement, les attaques à main armée et les agressions physiques de GAB ont régressé, tandis que la cybercriminalité connaît une hausse exponentielle, notamment dans le domaine des retraits GAB.

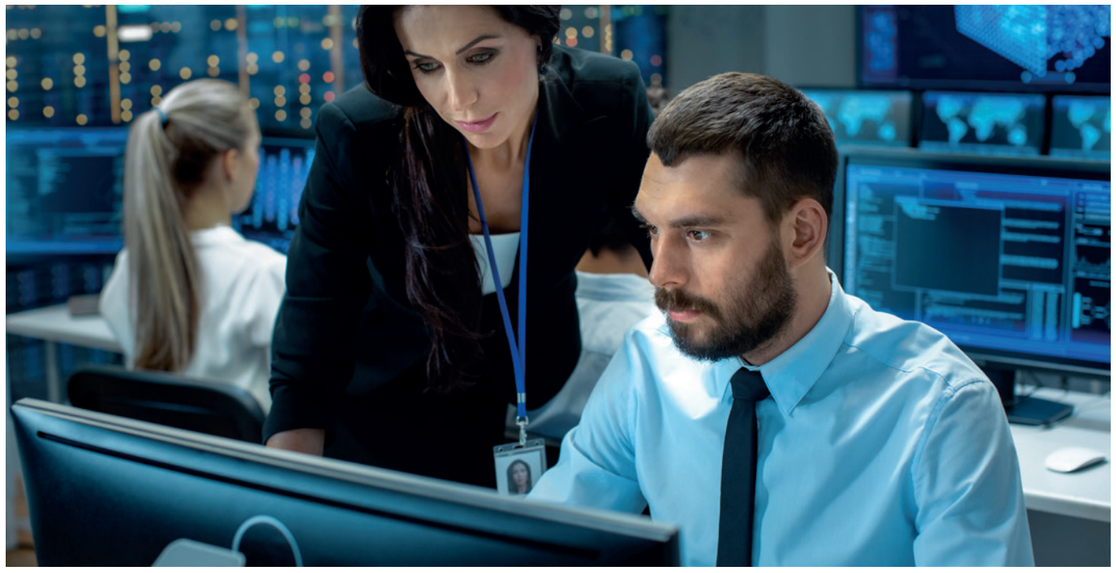
> Ces constats doivent conduire à réviser les pratiques anciennes

RÉPONSES TECHNOLOGIQUES

Comme souvent lorsque tant d'événements inattendus se succèdent, les industriels font preuve d'une impressionnante capacité d'adaptation. De nombreuses solutions innovantes voient le jour, faisant souvent appel à l'intelligence artificielle. Elles permettent de renforcer la sécurité, mais aussi, par exemple, de raffermir les gestes barrières dans le cadre des mesures imposées par la Covid-19, comme le contrôle automatique de la distanciation physique.

La réflexion sur ces constats doit conduire inexorablement les directeurs de la sécurité à réviser les pratiques anciennes. C'est le moment de repenser la sécurité.

Une révolution culturelle à mener



La digitalisation et l'hyperconnexion modifient la donne sécuritaire dans les entreprises et imposent de plus en plus une vision coordonnée et transversale des différents services.

Dans les entreprises et les banques, l'informatique a toujours été pilotée indépendamment des autres directions. Une des raisons est que l'informatique, arrivée bien après les différentes fonctions qui structurent une entreprise, est restée longtemps un domaine à part, ayant peu de relations avec les autres. Les choses changent avec la digitalisation, notamment en matière de risques. Les risques informatiques ont aujourd'hui des répercussions sur les risques physiques, et inversement. La convergence et la transversalité des risques nécessitent donc de penser un nouveau modèle de gouvernance avec une prise en compte au plus haut niveau de l'entreprise.

Les risques informatiques ont aujourd'hui des répercussions sur les risques physiques, et inversement.

CONSTRUIRE UNE STRATÉGIE GLOBALE

Il est fondamental que les différents domaines se rapprochent pour mieux se comprendre et construire ensemble une stratégie globale de la sécurité. Sans cela, les attaquants ne manqueront pas d'utiliser toutes sortes de failles physiques ou logiques pour arriver à leurs fins. Les menaces de cyberattaques prennent une dimension inédite dans notre société hyper connectée. Elles concernent aussi bien les mouvements financiers que l'intégrité des équipements de sécurité installés dans les agences. Se pose donc la question cruciale du rapprochement de tous les domaines de l'entreprise, qui ne peut plus fonctionner en silos. Il s'agit d'un changement culturel majeur qui concerne aussi bien les services de sécurité-sûreté – lorsqu'ils référencent un nouveau matériel – que le service informatique, par exemple lorsqu'il change un équipement réseau ou fait un patch pour résoudre une faille sécuritaire entraînant parfois le blocage de certains services d'une centrale d'alarme. Coordonner s'impose donc comme un enjeu stratégique.

GOUVERNANCE

Pour atteindre les objectifs fixés, la gouvernance doit impérativement fonctionner dans deux directions :
- *Top Down, pour définir et communiquer ce qu'il y a à faire*
- *Bottom Up, pour confirmer ce qui a été fait.*

Une évolution durable de la gestion des accès

Avec l'épidémie de Covid-19, le contrôle sécuritaire des accès aux sites des entreprises se double de précautions sanitaires. Les nouvelles pratiques seront probablement maintenues après la crise.

La gestion des droits d'accès dans les banques est généralement très claire. Selon les autorisations, un salarié ou un visiteur peut accéder, ou non, à certaines zones. Les portes de chaque site, bâtiment ou salle ne s'ouvrent ainsi qu'à ceux qui disposent des droits d'accès, le tout étant géré au sein d'un système de contrôle sur la base d'une politique définie par la direction.
Mais la pandémie est venue compliquer cette mécanique bien huilée. Elle impose des contraintes comme la distanciation entre les personnes, et oblige les entreprises à mettre tout en œuvre pour protéger les salariés contre le risque de contamination. Il ne s'agit plus simplement de contrôler qu'une personne a le droit de pénétrer dans un lieu parce qu'elle est accréditée, il faut en plus s'assurer que les conditions sanitaires sont remplies.

Dans un monde qui s'aseptise, les collaborateurs se montreront à l'avenir plus exigeants.

VERS LE SANS-CONTACT GÉNÉRALISÉ

On pourrait penser qu'il ne s'agit là que de contraintes temporaires. Certaines le sont, mais celles qui concernent l'hygiène des surfaces pourraient bien perdurer : dans un monde qui s'aseptise, les collaborateurs se montreront à l'avenir plus exigeants. Ils demanderont des solutions plus efficaces pour éviter toute transmission d'infection bactérienne. Le remplacement du badge par un smartphone s'imposera progressivement mais de manière inévitable pour parvenir au contrôle sans contact. D'autres problèmes liés au contrôle d'accès se poseront, en particulier dans le cadre du télétravail en mode nomade (lire le précédent numéro d'*AditelNews*). Il implique en effet de gérer des demandes d'accès temporaires à des agences ou à des locaux se trouvant dans les bâtiments centraux. La situation dans ce cas est un peu plus complexe car elle demande des moyens humains supplémentaires pour répondre à la demande ou le déploiement d'organisations compliquées.

L'IA et les solutions de nouvelle génération

Les solutions intégrant des briques d'intelligence artificielle ont déjà commencé à modifier l'approche de la sécurité dans les banques. Une évolution technologique à laquelle il va falloir s'adapter.

Sous l'effet de la digitalisation, les nouvelles technologies se sont largement développées ces dernières années dans le domaine de la sécurité bancaire. Une nouvelle réalité technologique est en train de faire évoluer nos habitudes en induisant de nouveaux usages. En parallèle, l'évolution de l'environnement sociétal, marqué par la menace terroriste, la multiplication d'actions violentes commises par des groupes extrémistes et désormais le contexte épidémique, oblige à repenser la sécurité des agences. A cela s'ajoutent les effets que peut avoir la transformation digitale sur les attentes du personnel. Un salarié qui peut faire une transaction bancaire à partir de son portable n'acceptera pas, demain, de devoir utiliser un badge pour accéder à son lieu de travail.

La fonction de sécurité-sûreté demandera à l'avenir un niveau d'expertise différent.

MULTIPLES APPLICATIONS

Déjà, les solutions traditionnelles commencent à évoluer. On le constate avec les nouvelles générations de détecteurs, dont l'IA renforce les capacités pour limiter les fausses alarmes, surtout dans de grands espaces ouverts. De plus en plus, les caméras les concurrencent avec succès grâce à une résolution plus grande, des prix qui baissent et l'intégration de processeurs qui embarquent des applications faisant notamment appel à l'intelligence artificielle, avec de multiples applications possibles : détection de présence, reconnaissance de visages, détection de température, suivi de personnes, enregistrement de photos ou vidéo…

Un des enseignements à retenir de ces évolutions est que la fonction de sécurité-sûreté dans l'entreprise demandera à l'avenir un niveau d'expertise différent pour choisir les solutions adaptées en fonction de multiples objectifs, actuels ou nouveaux.

Cybersécurité, un maillon à renforcer

Les failles informatiques offrent un point d'entrée aux malfaiteurs là où on ne les attend pas, menaçant à la fois les établissements, leurs salariés et leurs clients.

Perçue comme l'apanage des experts techniques, la cybersécurité est souvent délaissée par les responsables sécurité, qui se trouvent démunis face au risque informatique. Pourtant, de nombreuses attaques ne sont pas le fait de hackers opérant cachés, souvent depuis des pays hors de contrôle. Dans les banques, généralement bien protégées de ce point de vue, c'est au pied des automates que se réalisent les plus grandes escroqueries. Il est donc de la responsabilité de la sécurité d'imaginer les meilleurs moyens pour assurer la protection des clients mais aussi l'intégrité des équipements. Les nouvelles technologies peuvent apporter demain des solutions (lire dans ce numéro « L'IA et la sécurité nouvelle génération »).

Les nouveaux risques demandent une plus grande collaboration entre la DSI, la direction des opérations et la sécurité.

LE RENFORT DE L'INTERNET DES OBJETS

En matière de cybercriminalité, la mise en place du télétravail crée un risque nouveau. Il demande une réelle collaboration entre la DSI, qui ouvre les portes des applications à utiliser, la direction des opérations qui les choisit et le responsable sécurité qui intègre la sécurité du travailleur. Le risque essentiel – la séquestration avec extorsion – s'accroît en période de confinement. En effet, il est plus difficile de s'assurer qu'un employé n'est pas sous contrainte lorsqu'il travaille 5 jours sur 5 de chez lui que lorsqu'il vient plus régulièrement au bureau. De nouvelles solutions doivent être trouvées, l'IoT en est une, qui s'intègre totalement dans la façon de penser la sécurité de demain pour le salarié.

EN CHIFFRE

4,13 *En moyenne, une carte fraudée est utilisée pour 4,13 paiements en ligne. Selon la gendarmerie, le montant moyen des fraudes s'élève à 615€.*

Les impacts d'un climat social dégradé

Dans une société déjà en tension, les risques de troubles civils s'accroissent avec les impacts économiques et sociaux de la crise sanitaire.

La forte augmentation, l'ampleur et la durée des émeutes, manifestations violentes et actes de vandalisme ces dernières années fait des troubles civils un risque important pour les banques. A cela s'ajoutent les conséquences économiques et sociales de l'épidémie de Covid-19. Avec la fin des aides d'Etat, celles-ci seront ressenties plus durement, ce qui risque d'aggraver la situation d'une partie de la population (étudiants, intermittents du spectacle, saisonniers, banlieues…), et du même coup de dégrader le climat social, à la fois parce que de nombreuses personnes sont inquiètes pour leur situation et que ces catégories sont plus promptes à manifester leur colère. Plusieurs études récentes, dont une publiée par le cabinet Verisk Maplecroft, confirment l'augmentation des risques liés aux troubles civils.

ADAPTER LES PCA

Dans ce contexte, on mesure l'intérêt d'ajouter aux plans de continuité d'activité un volet spécifique sur ces risques émergents. Cela permettrait de définir, de tester et de mettre en place des procédures pour assurer la poursuite d'activité dans un climat social hyper tendu sur une zone géographique. Alors que les entreprises mesurent déjà la difficulté de faire face à des actes d'incivilités modérés, il paraît indispensable de se préparer à passer à un niveau plus élevé. Et même de regarder plus loin. Car au-delà des difficultés sociales, ce risque est associé à l'amplification des contraintes et restrictions générées par la crise sanitaire. Demain, l'urgence climatique pourrait être le prochain élément qui, plus durablement que la crise sanitaire, engendrera des contraintes individuelles pouvant alimenter des tensions sociales.

Il paraît indispensable d'anticiper les contestations générées par l'adoption de nouvelles mesures de contrainte.

EN CHIFFRE

X2 *Les troubles civils dans le monde ont doublé en 10 ans selon une étude de l'Institut pour l'économie et la paix. L'organisme de recherche anticipe une intensification des conflits provoquée par les répercussions de la crise sanitaire.*

Sécurité-fiction : une journée idéale à la banque

La révolution technologique de la sécurité n'a pas encore eu lieu, mais *AditelNews* a une petite idée de ce qu'elle pourrait donner. Voyage (presque) imaginaire dans un futur proche.

Au commencement de la télésurveillance, la protection des agences bancaires reposait sur une centrale d'alarme reliée à des détecteurs. Lorsqu'une présence ou des coups sur une paroi étaient détectés, la centrale envoyait un signal par le réseau téléphonique commuté à une baie de réception située chez le télésurveilleur. Les choses ont un peu changé avec la transmission numérique. Puis on a ajouté quelques caméras, mais rien qui évoque une quelconque disruption. Pourtant, le catalogue des solutions de sécurité s'est étoffé : haute résolution, algorithmes d'analyse d'images…

VISION D'AVENIR

Rêvons un peu et imaginons le scénario idéal de la sécurité bancaire de demain. « *J'entre dans mon agence en déverrouillant la porte avec mon smartphone. La caméra de l'entrée, munie d'un module d'intelligence embarqué, me reconnaît. Elle s'assure que personne ne franchit la porte en même temps que moi. Si je suis le premier, je fais un tour de ronde. Si une ou deux autres caméras bien positionnées détectent une deuxième présence, une alarme est envoyée au télésurveilleur directement par le réseau de l'agence. L'agence ouvre, la caméra de l'entrée scrute toutes les personnes qui entrent. Sont-elles agitées ? Ont-elles sur le visage des marques d'agressivité ? Si oui, une pop-up est envoyée sur tous les postes de travail de l'agence. Une personne vient faire une opération bancaire qui demande une authentification, elle se présente devant la caméra qui la reconnaît sans avoir à présenter ses papiers d'identité. Le soir, les agents signalent avec leur smartphone qu'ils quittent leur service. Le dernier met en service la sécurité du site. Sur son smartphone, on lui signale une éventuelle présence, il valide ou pas la mise en service. Par ailleurs, tous les équipements sont connectés sur le réseau de l'agence, tous les détecteurs de présence sont remplacés par des caméras qui envoient une image en même temps que l'alarme pour faciliter le travail du télésurveilleur. Ces flux ne sont dirigés vers le télésurveilleur que si l'agence est sous sécurité sinon ils sont stockés.* »

La caméra scrute toutes les personnes qui entrent : sont-elles agitées, présentent-elles des signes d'agressivité ?

Ce n'est là qu'un avant-goût, mais pour le coup, cette fois, la disruption est en marche…

LE FORUM, TEMPS FORT DE L'ANNÉE D'ADITEL

Lors de chaque forum, Aditel s'attache à explorer en profondeur un sujet d'actualité au plus près des préoccupations des responsables sécurité. Généralement, le forum se déroule en deux temps : une première partie le jeudi après-midi, durant laquelle un intervenant expose sa vision, la plus large possible, sur le thème. Aditel privilégie pour cet échange des personnalités qui ont une connaissance du sujet sous toutes ses dimensions : scientifiques, experts, membres de la police ou de la gendarmerie... Le vendredi prend plutôt la forme d'un débat avec une table ronde dont le but est de dégager des solutions concrètes pour la profession (voir serveur web aditel-asso.fr). Le forum est aussi un moment d'échange auquel participent entre 30 et 40 exposants choisis pour leur capacité à apporter des solutions sécuritaire pour la banque.

QUELQUES THÈMES DES 30 DERNIERS FORUMS D'ADITEL

- 29e > L'intelligence artificielle : les clés pour comprendre et ses applications
- 28e > Les phénomènes radicaux
- 27e > Quelles perspectives pour le fiduciaire
- 25e > Les enjeux de l'évolution vers le tout-numérique
- 24e > Vidéo, état de l'art et perspectives
- 23e > Les nouveaux défis de la télésurveillance bancaire
- 22e > Les nouveaux outils au service de la sécurité
- 21e > Gestion de crise
- 20e > Evolution de la pérennité
- 19e > La violence au quotidien, comment faire face

Table ronde du 29e Forum qui a eu lieu en 2019 à Mandelieu

FORUM 2021

Le 30e forum se déroulera les 23 et 24 septembre au Palais des congrès de Vichy. Au programme de cette édition : **« Les métiers de la sécurité bancaire face à l'évolution de la menace »**

RÉSEAUX SOCIAUX

Aditel, c'est aussi une communauté présente sur les réseaux sociaux. Vous pouvez suivre l'actualité de l'association sur notre compte LinkedIn : **https://www.linkedin.com/company/aditel-association/**

AditelNews est édité par l'association Aditel : BP 31012 - 54521 Laxou Cedex • Directeur de la publication : Aditel • Comité de rédaction : Didier Moreau, Claude Pace • Rédaction : BC Publications • Direction artistique & mise en pages : Alexandra Pourcellié, Arekusu • Illustrations : Fiamma Luzzati • Photos : Istock • Contact : secretariat.aditel@orange.fr - Tél.: 0 820 90 11 44 • Impression : Reprint, 31 rue André Vasseur - 31200 Toulouse