

© iStock

## Bienvenue au 26<sup>e</sup> Forum

Pourquoi une nouvelle revue pendant le salon d'Aditel ?  
Quels sont les objectifs ?

Il existe peu de témoignages sur les moments forts de nos précédents forums. D'autre part, nous n'avons jamais accordé beaucoup de place pour que vous puissiez vous exprimer, en dehors du questionnaire de fin de Forum.

Le but de ce journal est donc de donner la parole, aussi bien aux participants qu'aux exposants, pour évoquer des sujets

en cohérence avec le thème du forum, mais aussi pour exprimer un ressenti pris sur le vif. Dans un monde où l'image est le vecteur de communication prépondérant, nous avons souhaité immortaliser les moments forts avec des instantanés pris en temps réel. Aditel News, comme nous l'avons nommé, se veut aussi le reflet des enjeux qui viennent compléter les échanges du Forum.

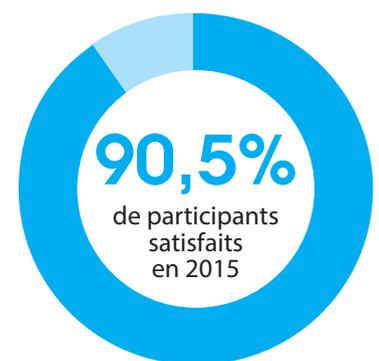
Vous y trouverez donc certains articles comme celui de Jean Tirole, prix Nobel d'économie 2004, sur les opportunités que peut apporter la révolution numérique ou l'analyse de François Marchessaux sur l'évolution du modèle sécuritaire. Enfin, nous espérons que vous prendrez plaisir à lire les interviews de participants, réalisés par Sandrine Legrand Diez rédacteur en chef du magazine "Sécurité Privée".

Steve Jobs disait « l'innovation, c'est une situation qu'on choisit parce qu'on a une passion brûlante pour quelque chose ». Si nous avons continué à innover cette année, c'est que nous avons la passion de rendre ce Forum le plus professionnel possible et qu'il devienne une manifestation incontournable. La réussite d'une nouvelle initiative est toujours incertaine ; on ne sait jamais à l'avance ce que chacun a envie et ce qui va le satisfaire. En espérant avoir répondu à vos attentes. Bon Forum.



## Chiffres clés

Taux de satisfaction du Forum Aditel

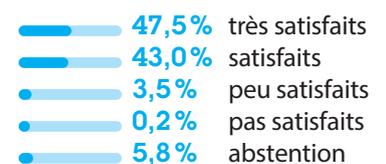


+12,4 %



de participants satisfaits par rapport à 2014

Détail à partir des enquêtes de fin de Forum



# 335 millions d'€

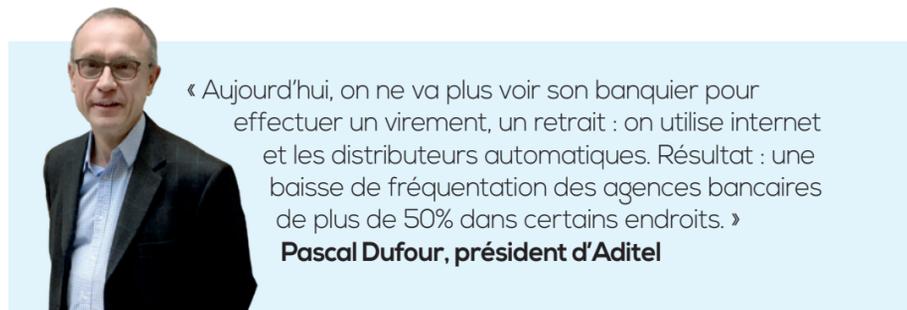
Après s'être fait la main sur les transactions en ligne des clients, les hackers se sont tournés vers une cible plus lucrative. Ce sont maintenant les marchés boursiers et les réseaux de paiements inter-bancaires qui sont visés par des attaques à répétition (affaires Carbanak, Swift, JP Morgan...). L'ampleur de la menace est telle que les acteurs de la banque et de l'assurance dépensent aujourd'hui sans compter pour s'en prémunir. Ainsi, le marché français de la cybersécurité dans la banque et l'assurance s'est établi à 335 millions d'euros en 2015 (+9,8%), d'après les estimations des experts de Xerfi. Et cette tendance devrait s'accroître en 2016 (+14%).

Source : Xerfi, communiqué relatif à l'étude « Le marché de la cybersécurité dans la banque et l'assurance - Stratégies des institutions financières, perspectives d'activité et axes de développement des spécialistes de la cybersécurité »



# +30%

Dans le cadre de la loi de programmation militaire les entreprises devront augmenter de 30% les coûts d'exploitation de leurs systèmes informatiques critiques.



« Aujourd'hui, on ne va plus voir son banquier pour effectuer un virement, un retrait : on utilise internet et les distributeurs automatiques. Résultat : une baisse de fréquentation des agences bancaires de plus de 50% dans certains endroits. »

**Pascal Dufour, président d'Aditel**

## Contre plongée

Comment les directeurs de la sécurité vivent-ils le virage numérique pris par les banques ? Regards croisés de Firouz Meguedad, directrice Sécurité et Continuité d'Activité Groupe, BPCE et de Laurent Allais, responsable du Département Sûreté Sécurité Prévention, LCL

### FIROUZ MEGUEDAD

La politique de sécurité doit, en premier lieu, inclure le traitement de menaces plus prégnantes, telles que les dérèglements climatiques, le terrorisme, la dépendance aux fournisseurs, notamment fiduciaires ; mais également être en prise directe avec le plan stratégique de nos entreprises : rechercher des solutions de sécurité innovantes, les adapter aux risques des métiers de nos entreprises qui évoluent vers le digital,

optimiser les coûts de sécurité en leur trouvant d'autres valeurs d'usage, prendre appui sur notre expertise pour piloter la mise en place et la gestion de la sécurité tout en gardant la gestion directe des incidents significatifs et des crises sécuritaires.

### LAURENT ALLAIS

Les conséquences sont plurielles. Le profil des membres de mon équipe est de plus en plus orienté vers l'informatique, car ils doivent comprendre le fonctionnement des systèmes qui leur sont proposés par les fournisseurs (souvent il est question de serveurs informatiques, de bases de données hébergées...), d'être force de proposition, d'échanger et mener des projets très techniques, avec le département informatique et télécoms ; ce qui n'est pas simple car il ne voit jamais d'un bon œil de « nouveaux » acteurs qui souhaitent connecter de nouveaux systèmes sur le SI.

Ce que je comprends bien, puisque ce sont de nouvelles failles potentielles qui sont créées. Nous devons rassurer le DSI, et le profil doit être très pointu pour pouvoir le faire. En terme de politique sécurité, cette évolution permet d'administrer en central plus facilement, plus rapidement les équipements et de libérer du temps commercial pour les équipes sur le terrain et aussi d'envisager de nouvelles applications pour nos systèmes.



### LAURENT ALLAIS

Responsable du département sûreté sécurité prévention, LCL



### FIROUZ MEGUEDAD

Directrice sécurité et continuité d'activité groupe, BPCE

## Les enjeux de l'évolution vers le tout numérique vu par Richard Olszewski

L'humanité produit tous les 6 mois plus de données numériques que sur toute la période de son histoire. Le tout numérique n'est donc pas un fait exclusif aux banques

On assiste à une accélération de l'histoire, des changements de paradigme économique comme avec l'impression 3D où l'on ne produira plus en Chine mais on imprimera soit à la maison soit dans une boutique de quartier. L'autre réalité, c'est qu'il y a des mini révolutions silencieuses régulièrement. Intéressez-vous à l'avènement des « blockchains » et anticipez leurs conséquences sur la façon de concevoir des systèmes de sécurité. Facilité, accessibilité, performance... les apports du « tout numérique » sont incontestables ; ce qui en fait un courant irréversible. Et

l'homme est ainsi fait : il évolue toujours dans le sens de l'optimisation (de son temps ou de son argent) !

### QUID DE L'ÉVOLUTION LÉGISLATIVE ?

Il est avéré que les pouvoirs législatif et réglementaire auront toujours un temps de retard sur les évolutions d'usages et technologiques. Une des solutions pour cadrer cette déferlante numérique est, selon moi, de passer par l'éthique et la formation. Face à la dématérialisation des finances mondiales, je vous invite à méditer cette réflexion d'Alexandre Zinoviev : « Il me semble que

dans le système de séparation des pouvoirs, il faudrait ajouter à ses trois composantes traditionnelles, le législatif, l'exécutif et le judiciaire, une quatrième : le pouvoir monétaire ».



### RICHARD OLSZEWSKI

Secrétaire général du Haut-Comité Français pour la Défense Civile

## 3 questions

à Patrice Cheramy, DG du Crédit Agricole Atlantique-Vendée et président de Nexecur

**Aditel News : Quels sont les impacts et les enjeux de la digitalisation pour le secteur bancaire ?**

**Patrice Cheramy :** On assiste à une évolution capitale à travers tous les outils digitaux qui existent aujourd'hui du comportement des clients. Pour la banque, la digitalisation est par conséquent devenue un enjeu de développement et d'accompagnement de nos clients. Ce qui justifie les programmes d'investissement importants engagés par les banques et le Crédit Agricole en particulier. Ce sont des investissements

d'avenir sans lesquels nous ne pourrions pas mener la révolution (bien plus qu'une évolution !) qui s'impose à nous.

**L'évolution du numérique vous paraît-elle inéluctable ?**

Absolument. L'évolution des services aux particuliers (autosurveillance, IOS10 et connectique de la maison) connaît une ampleur sans précédent. La télésurveillance est dans ce mouvement et dans un mouvement de digitalisation qu'il va falloir accélérer pour devenir, demain, des acteurs qui comptent.

**Aujourd'hui encore SI des télé-surveilleurs et SI bancaires restent étanches. Comment franchir cet obstacle ?**

C'est en effet une difficulté majeure. Je suis convaincu que dans le domaine informatique, nous aurons entre la télésurveillance et la banque à davantage rapprocher nos systèmes d'information, à les rendre plus communicants. Nous devons faire en sorte que la télésurveillance ne soit pas un métier à part mais, au contraire, - et c'est tout l'enjeu de la digitalisation - un métier totalement intégré au métier de la banque.

## Ils nous ont dit



### DAVID MURAT

Société Générale  
« Le fonctionnement traditionnel des banques en silos est-il toujours possible ? »



### JEAN-LAURENT SANTONI

Clever Courtage  
« J'aborderais plutôt les enjeux dans le sens suivant, celui de la digitalisation dans un monde qui se sécurise. »



### PHILIPPE BOGAERT

directeur commercial, Telem  
« Nous sommes à l'aube d'une nouvelle ère : SI et systèmes de sécurité doivent désormais être étroitement liés. »



### FABIAN RODES

Fasis consulting  
« La transformation digitale nécessite d'appréhender le risque numérique. »

## 38

Le nombre de vols à main armée passe de 32 à 38 faits en 2015. Une chute vertigineuse par rapport aux 2185 vols à main armée de 1986...

## Les nouveaux rôles de la fonction SI

Le fait que tous les acteurs, tous les collaborateurs de l'entreprise utilisent dans leur quotidien le monde numérique, le web, des smartphones avec des ergonomies mises à disposition dans le grand public, pose une exigence renouvelée sur le SI au sein de l'entreprise. En effet les collaborateurs, lorsqu'ils franchissent les portes de l'entreprise, s'attendent à avoir un SI aussi flexible que ce qu'ils peuvent trouver à domicile. Cela veut dire que la fonction SI doit livrer aux utilisateurs des systèmes qui soient aussi simples, fonctionnels et pratiques que ce qu'ils peuvent trouver eux-mêmes sur le net. Auparavant, les DSI vivaient dans un monde clos au périmètre très délimité, et n'intervenaient que rarement dans le domaine de la sécurité des biens et des personnes ; les responsables sécurité s'auto-suffisaient aussi bien pour définir la stratégie à mettre en place que pour faire les choix techniques. Or, le numérique nécessite des compétences différentes, nouvelles. Il est donc nécessaire que les DSI passent d'un rôle de gardien du temple à celui de facilitateur de solutions pour aider les responsables sécurité dans leurs choix.

(Source : Etude du SIGREF avril 2014)

## Quelles sont les grandes révolutions à venir dans la télésurveillance ?

Par Marc Pourcellié, président de Sotel

L'arrivée de l'IP est le début d'une révolution car, avec les problèmes de sécurité informatique que cela représente, les compétences chez les responsables sécurité et les télésurveilleurs doivent être équivalentes à celles que l'on trouve dans tous les centres de production informatique qui sont généralement placés sous la responsabilité d'un Directeur du Système d'Information (DSI). Cette évolution signe la fin des architectures et des organisations actuelles présentes dans presque toutes les stations de télésurveillance. Les nouvelles architectures doivent être calquées sur ce que l'on trouve par exemple dans les banques.

Des Data Center parfaitement sécurisés autant sur le plan physique qu'informatique associant moyens et compétences informatiques pour gérer les machines et élaborer la stratégie numérique. Le traitement des alarmes et l'exploitation se faisant à partir de postes opérateurs répartis sur plusieurs centres d'exploitation distants. Cela nécessite des regroupements de moyens qui sont inéluctables ; car dans l'état actuel des choses, un télésurveilleur ne peut supporter tout le poids d'une DSI, capable de répondre aux objectifs ci-dessus. L'autre solution serait la mise en place d'opérateurs œuvrant pour plusieurs télésurveilleurs. Le té-



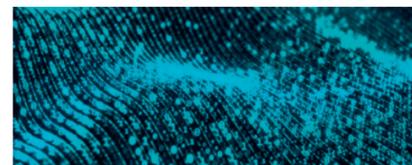
MARC POURCELLIÉ  
Président de Sotel

lésurveilleur se démarquant de ses concurrents par la qualité de ses prestations ou sa capacité à offrir des services. La révolution digitale et tous les objets connectés devraient voir le développement de nouveaux services permettant à chaque télésurveilleur de se caractériser.

## La cybersécurité

Un poste croissant dans les dépenses IT des banques

Les institutions financières investissent massivement pour se prémunir des attaques informatiques. JP Morgan compte par exemple dédier plus de 500 M€ à la cybersécurité en 2016. Quant au patron de Bank of America, il a déclaré en novembre 2015 lors d'une conférence que le budget cybersécurité de son entreprise était « illimité ». Ce choix est également adopté par les établissements français. Alors que Société Générale consacrait 2% de ses dépenses IT aux cybermenaces, cette part doit grimper à 5% sur la période 2016-2020.



## À lire

Économie du bien commun de Jean Tirole

Avec ce premier livre visant un large public, Jean Tirole nous fait partager une certaine vision de la révolution numérique en marche. Demain, elle bouleversera les secteurs de l'assurance, de la santé de l'énergie, de l'éducation.... Au-delà de l'extraordinaire progrès technique que la numérisation induit, synonyme de gain de temps et de pouvoir d'achat, l'économie numérique comporte des dangers qu'il nous faut bien mesurer. C'est pourquoi nous devons anticiper les nombreux défis de ce bouleversement. Et Jean Tirole se met ici à notre portée pour partager sa discipline et ses travaux.

Date de parution: 11/05/2016  
Code ISBN : 978-2-13-072996-9



## Le modèle de la sécurité doit évoluer pour répondre aux nouveaux enjeux

La question n'est plus de savoir si les banques sont vulnérables mais d'identifier les vulnérabilités prioritaires et de mobiliser les moyens de prévention, de détection et de réaction adaptés à la menace. Par François Marchessaux, directeur associé, Columbus Consulting

Un nouveau modèle opérationnel émerge sur le secteur. Il s'appuie sur la création d'une ligne de défense qui complète la protection périmétrique historique des réseaux bancaires. Véritable base arrière du dispositif sécuritaire, cette seconde ligne de défense joue un rôle clé de veille, de prévention et de surveillance. Ce modèle assure également l'intégration de la sécurité au cœur des processus de « sourcing » et de conception logiciel. Il offre les capacités d'anticipation et de reporting nécessaires pour répondre aux dernières évolutions réglementaires. Au-delà de ce changement organisationnel, la mise en place d'un nouveau modèle opérationnel constitue un changement culturel impactant pour les acteurs des

services financiers et change leurs priorités. Ainsi, le partage d'information, historiquement proscrit, est aujourd'hui encouragé car indispensable à l'anticipation de la menace et à la hiérarchisation des vulnérabilités. Les actions de prévention et de transfert du risque tiers, autrefois secondaires, sont devenues prioritaires.

La sensibilisation des clients, la formation des partenaires et la négociation des clauses contractuelles relatives aux prestations dématérialisées sont essentielles à la sécurité des banques et assurances. La maîtrise en profondeur des systèmes d'exploitation et des infrastructures réseaux, usuellement dans le champ des éditeurs spécialisés devient stratégique pour la prévention,



FRANÇOIS MARCHESSAUX  
Directeur associé,  
Columbus Consulting

la protection et la détection du risque. La Cybersécurité n'est plus seulement l'apanage des spécialistes en administration de réseau et système mais une activité transversale et ouverte sur le monde extérieur, nécessitant la coordination de nombreux métiers et partenaires. L'acquisition et l'intégration de technologies de pointes et le développement de services de sécurité externalisés de type Security Operating Center nécessite l'intégration de compétences nouvelles. Dans les services financiers, la filière sécurité doit par conséquent se doter de spécialistes techniques, de hackers et d'experts métiers ainsi que d'acteurs capables de conduire des projets, de mener des études, d'administrer des centres spécialisés, de développer et d'entretenir des relations avec les autorités internationales. Elle doit aussi intégrer des métiers nouveaux (data-scientists, data-analysts) pour lesquels il n'existe pas de filière de formation/d'expérience mature.

## Ils participent



JEAN-MICHEL LE COITE  
services sécurité réseaux, CMIC

« La digitalisation a d'ores et déjà entraîné une amélioration de la sécurité en matière d'identification. »



ISABELLE ROHO  
responsable sécurité de l'information Société Générale

« Les clients sont devenus autonomes grâce aux services en ligne. De fait, les enjeux sécuritaires se sont déplacés vers le numérique. »



JEAN-MARIE CAPELLI  
directeur de Nexecur Sécurité bancaire

« La sécurité bancaire est aux prémices de sa révolution digitale. »



PATRICE BAYARD  
général de Gendarmerie

« Le braquage aussi se digitalise. Et l'activité des malfaiteurs s'est elle-aussi reportée sur Internet. »

## De nouveaux usages pour la vidéosurveillance

Par Sébastien Mauqué, directeur général de Partenaire Sécurité

La première évolution qui répond aux nouveaux besoins du marketing directement produits par la digitalisation et aux contraintes pécuniaires se traduit dans les offres destinées aux nouveaux usages de la vidéosurveillance tournés vers l'analyse vidéo. Les fonctionnalités comme le comptage, l'analyse de flux dans l'image et, plus globalement, l'analyse comportementale sont les futurs outils de demain pour la différenciation commerciale des concepts d'agencement et de définition des modalités tactiques au plan commercial des interactions clients/conseiller au sein des réseaux bancaires. Ces mêmes outils seront de plus en plus performants en termes d'analyse et de recoupement de données pour répondre au changement de paradigme en matière de sûreté et produire des outils d'identification, d'analyse et d'alerte liés aux incivilités par exemple. Qui du client ou de l'employé génère l'incivilité ? Les nouveaux usages technologiques devraient nous permettre de clarifier ce point.

# 65%

des DSI craignent que leur entreprise ne soit victime d'une grave fuite de données dans l'année.

## La nécessité d'intégrer le contrôle d'accès dans les SI de la banque

Par Roland de la Chapelle, associé et directeur du développement de Locken

Le pilotage du contrôle d'accès au travers des plateformes de supervision internes des banques s'inscrit dans la stratégie de convergence des solutions électroniques de sécurité au sein des Systèmes d'Information.

Pour piloter cette activité de supervision d'agences, de nombreuses banques font appel à des plateformes de télésurveillance. Avec son offre logicielle Locken Smart Access, Locken permet de faire collaborer les logiciels de différents partenaires dans le Système d'Information de la banque. La gestion des accès s'intègre ainsi en toute sécurité dans le système du client et permet de superviser l'activité de toutes les solutions

électroniques coexistantes au sein de la banque.

### Le renforcement de la sécurité logicielle au sein du contrôle d'accès

Les banques et plus particulièrement leurs DSI portent une attention particulière à la capacité des prestataires à produire des logiciels en accord avec leurs exigences éle-

vées en matière de sécurité. L'authentification des acteurs - utilisateurs, administrateurs ... - qui animent ces solutions sécuritaires est au cœur de ces problématiques. De par la convergence des systèmes, les solutions de contrôle d'accès se doivent d'être en harmonie avec la sécurité intrinsèque des réseaux bancaires qui les hébergent.



## La sécurité bancaire en évolution

La convergence des systèmes électroniques de sécurité dans les SI de la banque par Azad Khamooshi, business development manager, Retail Segment, Axis Communications

L'évolution technologique est en constante accélération dans les institutions financières, la convergence et l'intégration de plus en plus poussées des systèmes électroniques de sécurité au travers de l'hyper-vision, l'arrivée du cloud computing, le gardiennage virtuel constituent les prémisses de ce

bouleversement. Les agences bancaires se modernisent par l'utilisation des nouvelles technologies, l'objectif étant d'optimiser les coûts et développer de nouvelles sources de satisfaction client. Les solutions de vidéo sur IP Axis Communications permettent d'ajouter des fonctionnalités à votre rythme, que ce soit des encodeurs, des

caméras, de la visiophonie, ou encore des fonctions proactives de sécurité et de vidéo intelligente. Vous pouvez aussi intégrer des solutions Axis à d'autres systèmes IP, tels que des systèmes d'alarme incendie ou de contrôle d'accès. La vidéo sur IP apporte aux solutions de sécurité les avantages de l'imagerie numérique.

## La convergence implique de partager, de mutualiser et de décloisonner

Par Stéphane Bidault, président de TEB

La convergence est déjà une réalité, source d'une plus grande efficacité des systèmes électroniques de sécurité et des systèmes d'informations plus largement. L'émergence du numérique a profondément et durablement modifié les produits mais aussi les usages ; il permet de s'affranchir des barrières entre les solutions. Malheureusement, le numérique seul n'est pas la réponse unique à la convergence. Pour y parvenir, trois facteurs doivent être combinés : les infrastructures, l'usage et la gestion. Les infrastructures sont déterminantes car il en découle la capacité du système à gérer et à faire interagir une masse plus ou moins importante d'informations. Les usages, eux, doivent conduire à repenser la segmentation des

métiers qui aujourd'hui a souvent tendance à trop fonctionner en silos. La convergence implique de partager les outils, de mutualiser les actions et donc de décloisonner.

Enfin, la gestion de la convergence est également clef, puisqu'elle amène à s'interroger sur la façon dont celle-ci sera mise en place ; à savoir, par qui et comment. Qui gère et pilote cette convergence ? Quels en sont les objectifs ? Les réponses à ces questions sont spécifiques à chaque entité et dépendent de leur organisation et de leurs priorités. Infrastructures, usages et gestion doivent être considérés simultanément pour aboutir à la convergence, ce qui oblige à faire des compromis.

## Le « Big Data » comme réponse

Par Viviane Bretagne, directeur commercial Gunnebo France

La sécurité bancaire est en pleine mutation. La convergence de la sûreté et de la sécurité informatique est en marche. Dans cette dynamique, notre approche aujourd'hui repose sur le premier concept sécurité orienté « Big Data ». En s'appuyant sur les standards réseaux, les bases de données et les systèmes d'exploitation, notre architecture s'intègre pleinement dans la stratégie informatique de la banque.

Au sein d'un environnement multi-sites et multi-systèmes, le responsable sûreté doit gérer des populations mobiles ; la solution SecurManager développée par Gunnebo lui offre de nouveaux outils d'analyse et de décision pour exploiter l'intelligence de ses données. Ce concept Big Data ouvre des perspectives nouvelles et enthousiasmantes, pour bâtir ensemble un avenir plus sûr.

## La DSI doit être partie prenante des choix sécuritaires

Par est Claude-Philippe Neri, PDG d'ESI Group

Avec la montée en puissance des réseaux numériques, des problématiques de sécurité de ces réseaux, de la puissance accrue des systèmes et leur mise en Data Center plutôt qu'un hébergement local, la convergence des systèmes d'information prend une dimension tout à fait particulière. Il devient en effet nécessaire surtout lorsque certaines prestations de sécurité (installation, télésurveillance, maintenance) sont externalisées, mais pas que, de faire en sorte que la DSI soit partie prenante des choix faits par les services en charge de la sécurité. Ce faisant, la dynamique ainsi naturellement créée devrait aboutir à l'émergence dans le milieu de la sécurité bancaire de nouvelles solutions non encore explorées ou exploitées.

## Ils exposent



**FRANÇOIS BUREAU**  
Cossilys 21

« Cette nouvelle organisation s'adapte aux attentes des exposants. »



**LIONEL SANVOISIN**  
Abloy

« Cette année, nous pouvons prendre plus de temps pour échanger avec les clients. »



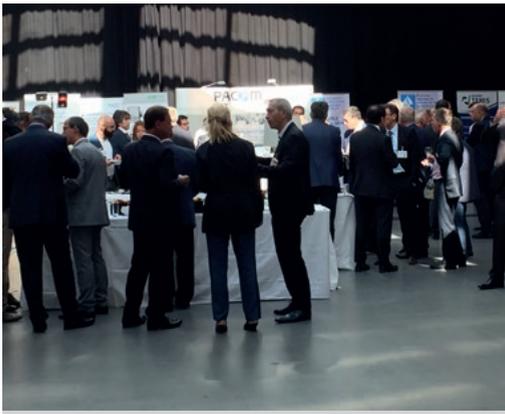
**CHRISTOPHE PERNET**  
Oberthur Cash Protection

« Le cadre est idyllique et très adapté à ce type de salon. »



**YVES CLOUSIER**  
Synchronic

« Cette nouvelle organisation est une amélioration dans la continuité. »



**SAVE**  
— the —  
**DATE**

Rendez-vous  
**Les 5 et 6 octobre 2017**  
à Montpellier  
Pour le 27<sup>e</sup> Forum Aditel