# Médias, Santé, Industrie…
# à chacun sa stratégie IAM !

Comment les exigences sectorielles façonnent-elles les besoins en matière d'IAM ? Quels sont les enjeux spécifiques auxquels doivent faire face les RSSI ? Nos experts vous livrent leurs analyses.

Cybersecurity Solutions.
inetum.

# Sommaire

# Édito

En matière de cybersécurité, les RSSI ont une mission commune : protéger le système d'information et le patrimoine informationnel dont ils ont la charge.

À l'heure où l'information est partout et où les interconnexions n'ont jamais été aussi nombreuses, la tâche est complexe ! D'autant plus que la pression en matière de cyberattaque n'a jamais été aussi élevée qu'aujourd'hui.

Une stratégie claire de gestion des identités et des accès est un maillon essentiel d'une politique de cybersécurité adaptée aux enjeux du monde actuel.



Elle permet de garantir la sécurité des accès au système d'information, d'assurer la conformité à certaines réglementations, de réduire un grand nombre de risques opérationnels, d'améliorer la productivité et la qualité de service aux utilisateurs, mais aussi d'accompagner l'évolution et l'ouverture du SI vers le digital, la mobilité et le cloud, etc.

Toutefois, il est important de souligner que chaque organisation est unique et qu'il n'existe pas d'approche universelle de l'IAM, ni de solution standard. En effet, les modèles d'affaires, les risques associés, les pratiques métiers ou encore les réglementations diffèrent de façon significative en fonction du secteur économique dans lequel évolue l'entreprise.

**Alors, comment les exigences sectorielles façonnent-elles les besoins en matière d'IAM ?**

**Quels sont les enjeux spécifiques auxquels doivent faire face les RSSI ? Existe t'il des freins et obstacles particuliers dans certaines professions ?**

Pour répondre à toutes ces questions, nous avons réuni quatre experts du sujet. Ils vous livrent ici leur analyse des médias, de la santé, de l'industrie, mais également d'autres secteurs où les spécificités sont déterminantes. Au programme : **expertise, conseils et cas d'usages métiers**.

**Ce livre blanc a été pensé sous le prisme du partage et de la coopération.** Notre réseau de partenaires et notre communauté clients nous permettent de capitaliser sur l'expertise et les retours d'expérience de chacun pour construire les solutions de demain.

# 01

# Industrie : un secteur en pleine révolution !

**Gabriel Angot**
Consultant sécurité IT/OT chez Formind

Les révolutions industrielles ont des impacts forts sur l'économie et changent profondément la manière dont les humains produisent les choses. Depuis quelques années, le secteur industriel est entré dans sa 4ième révolution, également connue sous le nom d'industrie 4.0. Avec la puissance des nouvelles technologies, on se dirige aujourd'hui vers un modèle d' "usine connectée". Les objectifs sont clairs : accroissement de la productivité et de la performance, développement de l'innovation, réduction des coûts, amélioration du ROI des machines, etc.

Cependant, lorsque la technologie s'invite dans les systèmes industriels (OT), ce n'est pas sans risque ! En France, cela fait plusieurs années déjà que l'ANSSI alerte sur le sujet. L'intensification de la menace n'est pas qu'un ressenti mais bien une réalité ! Selon un rapport de Kaspersky, les attaques ciblant le secteur industriel atteignent un nouveau record au deuxième trimestre 2023 avec 26,8 % des ordinateurs de systèmes de contrôle industriel (ICS) touchés.

Le constat est sans appel : la cybermenace fait désormais partie du quotidien des industriels. Les interconnexions toujours plus nombreuses requises par l'industrie 4.0 sont autant de portes d'entrée pour des individus malintentionnés.

Sur le terrain, les contraintes de l'environnement industriel ne facilitent pas la mise en place d'une politique de cybersécurité optimale. Les frontières entre IT et OT se sont estompées. Cette convergence soulève des défis en termes de gestion et de sécurité. En effet, à mesure que la connectivité des systèmes OT s'est développée, tant avec l'informatique qu'avec le monde extérieur, ces systèmes ont été soumis à des cybermenaces qui n'avaient même pas été envisagées lors de leur conception.

***« En pratique, l'OT est un monde totalement différent de l'IT : les deux secteurs de l'entreprise ont des objectifs différents, une culture différente et des experts différents. Pourtant, aujourd'hui, ce sont bien les RSSI qui portent la responsabilité de maintenir la cybersécurité dans l'OT. »*** souligne Gabriel Angot, Consultant sécurité IT/OT chez Formind. ***« Pour réconcilier les 2 mondes, les experts ont mis à disposition un ensemble de référentiels et recommandations. Je pense notamment à la norme internationale IEC 62443, qui est une référence dans le secteur. La norme pose un cadre de cyberdéfense en profondeur des systèmes industriels et sert désormais de liant à ces deux environnements. »***



Au vu du contexte, il apparait clair que les RSSI voient leur stratégie de gestion des identités et des accès considérablement évoluer. Il s'agit maintenant de sécuriser des points d'accès toujours plus nombreux, voire d'être capable de traiter des identités machine. Le challenge est complexe et les nombreux systèmes hérités qu'il faut intégrer ne facilitent pas l'agilité. ***« Dans l'industrie, les mots d'ordre sont disponibilité et intégrité, notamment en raison de l'impact potentiel des arrêts sur la chaîne de production ! C'est pour cela que la confidentialité des données est longtemps passée au second plan. Il faut bien comprendre que les installations, mises à jour, maintenance des solutions doivent être réalisées sans interruption de service. La sécurité des systèmes ne doit absolument pas perturber le cœur de métier des industriels ! »*** explique Gabriel Angot. ***« Avec la médiatisation des attaques dans le secteur, il y a eu une vraie prise de conscience des enjeux cyber au niveau des industriels ; en revanche, sur le terrain il y a encore un travail important de sensibilisation et de transferts de compétence à faire côté OT. Ce sont des équipes qui ont traditionnellement plutôt concentré leurs efforts sur l'ingénierie et la maintenance des systèmes physiques plutôt que sur la sécurité informatique. »***

Une chose est sûre, dans les environnements OT, les mots de passe abondent et continuent d'être une cause majeure de violation. ***« Les mots de passe sont bien souvent partagés en interne ou en externe, l'accès n'est pas limité à certains périphériques ou réseaux spécifiques, on trouve également beaucoup de comptes génériques ou encore de mots de passe par défaut sur les appareils de types IoT »*** explique Gabriel Angot. ***« Et là on est pile dans le terrain de jeu de l'IAM ! Il est tout à fait possible d'inclure les dispositifs OT dans la stratégie IAM de l'entreprise, même si ceux-ci ne supportent pas les protocoles standards d'authentification ! Il existe des solutions de eSSO ou de web SSO permettant de gérer tous types d'applications, et même le legacy ! Et contrairement aux idées reçues, elles ne sont pas contraignantes, bien au contraire elles permettront d'offrir aux utilisateurs un parcours d'accès fluide et adapté à leur contexte de travail. »***

Lorsqu'il s'agit d'infrastructures critiques, et c'est bien le cas dans l'industrie, un soin tout particulier doit être apporté aux habilitations. Il faut tendre vers des approches zero trust, en appliquant notamment le principe du moindre privilège. Ceci est d'autant plus important que le secteur industriel brasse une population d'utilisateurs variés et éphémères. De plus, pouvoir révoquer très rapidement les accès d'une identité en cas de compromission pour limiter les impacts est un must dans un secteur où la réactivité est au centre des priorités.

En adoptant une approche permettant de sécuriser les accès OT ainsi qu'une gouvernance des identités et des habilitations optimales, la surface d'attaque et les risques de sécurité réduisent considérablement.

L'industrie 4.0 change le paradigme de l'industrie, en renforçant l'agilité et la flexibilité des systèmes industriels. Elle a fait naître le besoin d'une cybersécurité industrielle robuste et capable de prendre en compte un environnement complexe. ***« Les industriels qui tirent aujourd'hui leur épingle du jeu sont ceux qui ont su poser les bases d'une gouvernance adaptée de la cybersécurité en misant sur la collaboration IT/OT, le partage de bonnes pratiques et la complémentarité des expertises. »*** conclut Gabriel Angot ***« Il y a fort à parier que les acteurs les plus avancés vont s'orienter vers des authentifications continues, contextuelles et dynamiques afin de protéger leurs systèmes critiques en temps réel »***.

# Zoom sur le terrain

## Sébastien, Technicien de maintenance dans un grand groupe industriel

*« Je souhaite accéder aux systèmes de contrôle industriel. »*

### Mes attentes

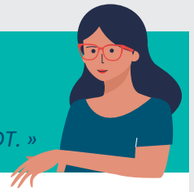
- Un accès simple et rapide aux systèmes de contrôle industriel
- Ne pas être ralenti par la sécurité

### La solution

- Mise en place d'une solution de gestion des identités et des habilitations avec un provisionning basé sur les rôles/profils métiers et prenant en compte la politique de sécurité préconisant le principe de moindre privilège
- Implémentation d'une solution de MFA en passwordless pour l'accès aux ressources critiques via le déploiement d'une authentification avec carte à puce
- Mise en place d'un système de récupération et d'envoi vers le SIEM des informations d'audit concernant les authentifications et les modifications des habilitations

### Les bénéfices

- Pour l'OT :
  - Renforcement de la sécurité des accès aux systèmes critiques
  - Gestion fine des droits d'accès selon les niveaux de compétence et les besoins opérationnels
  - Surveillance des accès et de la gestion des habilitations
  - Audit et conformité réglementaire facilités grâce à une meilleure traçabilité
- Pour Sébastien : un processus d'authentification fluide et adapté à son métier et ses habilitations



## Emma, Responsable sécurité opérationnelle dans un grand groupe industriel

*« Je souhaite sécuriser les APIs utilisées pour les échanges entre systèmes OT. »*

### Mes attentes

- Protéger les accès aux APIs utilisées pour les échanges entre systèmes OT
- Gérer et simplifier la gestion des habilitations d'accès à ces APIs

### La solution

- Mise en place d'une plateforme IAM permettant de gérer les habilitations et de proposer un fournisseur d'identité pour une protection par fédération des accès
- Mise en place de politiques de sécurité définissant clairement qui peut accéder à quoi et à quelles conditions avec des droits périssables

### Les bénéfices

- Pour l'OT : amélioration de la sécurité des accès aux APIs
- Pour Emma : simplification de l'intégration de nouveaux services



## Christophe, Responsable sécurité du système d'information dans un grand groupe industriel

*« Je souhaite sécuriser l'infrastructure IoT dans mon installation énergétique. »*

### Mes attentes

- Intégrer des technologies IoT au sein de l'infrastructure existante sans compromettre la sécurité
- Gérer les identités numériques des nouveaux appareils connectés et des utilisateurs
- Assurer l'authentification des ces acteurs et le contrôle de leurs accès
- Faciliter la maintenance prédictive et améliorer/ optimiser l'efficacité de l'installation

### La solution

- Mise en place d'une solution IAM et implémentation d'une solution de MFA pour tous les utilisateurs accédant à la plateforme de gestion IoT
- Authentification des appareils IoT avec une approche basée sur le principe de zero trust, pour s'assurer que seules les sources fiables peuvent communiquer au sein du réseau
- Mise en place d'une authentification adaptative : les droits d'accès sont adaptés en fonction du contexte, de la localisation de l'utilisateur, de l'heure de la connexion et de la ressource demandée

### Les bénéfices

Pour l'OT et Christophe :

- Renforcement de la sécurité de l'infrastructure IoT
- Sécurisation des accès des utilisateurs
- Analyse et optimisation de la distribution de l'énergie de l'entreprise grâce au contrôle des accès aux données des capteurs

## Parole de client

*Chez M TAG nous avons des utilisateurs très variés, allant des conseillers de vente aux conducteurs de tram ou techniciens de maintenance, et des cas d'usages bien spécifiques. Nous nous appuyons sur le binôme Formind – Ilex pour la partie AM. L'expertise et la réactivité des équipes, ainsi que l'agilité et la robustesse de la solution Ilex Access Management nous ont séduits.*

M TAG
*Le mouvement, c'est la vie*

**Mathias BILLION**
Administrateur Systèmes chez M TAG

# 02 Médias : un secteur sous le feu des projecteurs !

**Aymeric Durand**
Manager de la practice Access
chez I-TRACING

Le secteur des médias et du divertissement a considérablement évolué ces dernières années et s'est pleinement engagé dans l'ère du digital. En effet, sur un marché ultra concurrentiel, la différence entre le succès et l'échec réside dans la capacité à s'adapter, voire à anticiper, l'évolution des usages de ses audiences. Les acteurs cherchent à se positionner sur de nouvelles offres de services afin d'améliorer l'expérience client et de gagner des parts de marché.

Parallèlement, les entreprises connaissent un niveau de risque cyber inédit et le secteur des médias est loin d'être épargné. En effet, il compte parmi les secteurs les plus ciblés, de par la résonnance qu'il représente au niveau mondial et les enjeux géopolitiques actuels ne font qu'amplifier le phénomène. Pour exemple, le 6 février dernier des pirates informatiques soutenus par l'Iran ont réussi à interrompre les programmes d'une plateforme de diffusion en continu de télévision aux Émirats arabes unis afin de diffuser un faux journal généré par l'IA[1]. Un scénario presque digne d'un film et pourtant, c'est bien une réalité aujourd'hui.

Pour les RSSI du secteur média, le défi est de taille. Il faut maîtriser et sécuriser les périmètres critiques, réduire les risques et élever le niveau de résilience des infrastructures de l'organisation, sans pour autant entraver leur cœur de métier : diffuser l'information et proposer à son audience des services à haute valeur ajoutée. Et cela prend tout son sens à l'aube des JO 2024, une vitrine pour notre pays mais également une aubaine pour les attaquants qui perçoivent le fort retentissement médiatique autour de l'événement.

Mettre en place une stratégie claire de gestion des identités et des accès est un indispensable d'une politique de cybersécurité et les RSSI en ont aujourd'hui pleinement conscience. ***« Au vu du contexte, rares sont les entreprises qui ne sont pas au fait des bienfaits de l'IAM. En revanche, il existe de grandes disparités sur le terrain entre les organisations. »*** explique Aymeric Durand, Manager de la practice Access d'I-TRACING. ***« On remarque notamment qu'en terme d'infrastructure, les médias sont très en avance et innovants sur toute la partie flux vidéo, images, haute disponibilité et performance. Ça se comprend assez aisément puisque la priorité métier reste la production et la diffusion d'information. En ce qui concerne la cyber en revanche les SI sont moins matures. On y arrive progressivement mais ce n'est pas dans l'ADN premier des équipes »***.

[1] SOURCE : Émirats arabes unis : des hackers pro-Iran ont diffusé un faux journal généré par IA (france24.com)



La protection des accès a bénéficié d'un effet de levier lié à la prise de conscience générale des conséquences lourdes d'une intrusion malveillante dans le SI.

Ainsi, authentification, contrôle d'accès, MFA sont de plus en plus intégrés, qu'il s'agisse de protéger les accès des collaborateurs ou de proposer aux clients finaux des parcours d'inscription et d'authentification fluides et fiables. Les cas d'usages étant extrêmement vastes et les parcours très différents d'un type d'utilisateur à l'autre, il faut faire le choix d'une solution IAM agile et avancer de façon pragmatique.

En revanche, la gestion des accès doit impérativement s'accompagner d'un travail sur la gouvernance des identités et des habilitations. Et c'est là que réside toute la complexité pour les acteurs du secteur ! ***« Les utilisateurs au sein d'un média représentent une population extrêmement variée et volatile. On retrouve par exemple des pigistes, des intermittents, des prestataires. C'est une véritable ruche de l'information ! »*** poursuit Aymeric Durand. ***« La gestion d'une population hybride et "temporaire" n'est pas un exercice facile c'est vrai et les projets d'identités sont plus structurels que les projets d'accès. Ce qui explique que sur le terrain, il n'est pas rare de voir encore en régie des postes de travail partagés où chacun se connecte sur un compte générique pour travailler sur la production du JT par exemple… il faut absolument y mettre fin et que chacun puisse se connecter à une session nominative et c'est précisément le rôle de l'IAM. »***

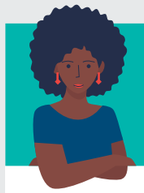
Une solution d'IAM vous permet de maîtriser et d'industrialiser le cycle de vie de vos utilisateurs. Le provisioning à l'entrée et la suppression des ressources logicielles au départ, sans oublier la gestion en temps réel des changements de fonctions/statuts, sont des fonctionnalités incontournables pour garantir sécurité et traçabilité sur tous les postes mis à disposition (station de travail individuelle, postes de régie partagés, smartphone…).

Soulignons que la cybersécurité est toujours une affaire d'équilibre et de compromis. Avec une population d'utilisateurs éphémères et pas toujours formés aux procédures internes, il est important de rehausser la sécurité sans renier sur l'expérience utilisateur afin de gagner leur adhésion. Pour cela, il faut se tourner vers des solutions IAM modulaires, agissant comme un véritable "hub d'authentification" et permettant d'offrir de multiples moyens de se connecter au système d'information tout en respectant la politique de sécurité mise en place.

***« Le secteur des médias a bien changé ces dernières années et est pleinement engagé dans le numérique. Plutôt que d'opposer cybersécurité et enjeux commerciaux ou productivité, il faut créer des ponts afin que l'un serve l'autre. J'encourage les RSSI à être force de proposition sur les parcours d'authentification, car ils sont le trait d'union entre sécurité et expérience utilisateurs. »*** conclut Aymeric Durand. ***« Les acteurs les plus avancés en la matière se dirigent vers du passwordless, et tout semble présager que les entreprises qui amorcent ce virage avec pragmatisme et méthode feront émerger des leviers de croissance considérables. »***

Selon un rapport du Gartner® ***« D'ici à 2025, plus de 50 % des méthodes d'authentification du personnel et plus de 20 % des méthodes d'authentification des clients se feront sans mot de passe, contre moins de 10 % aujourd'hui ».*** Le passwordless n'est donc pas un mythe mais bien l'avenir.

# Zoom sur le terrain



## Marie, Journaliste pour une chaîne de télévision nationale

*« Je souhaite accéder à mes applications sur un poste de travail en régie pour travailler rapidement sur ma chronique prévue au JT. »*

### Mes attentes

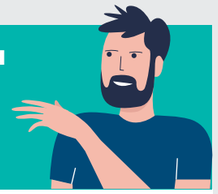
- Un accès simple et rapide à mes applications
- Retrouver ma session de travail même sur un poste partagé
- Ne pas être ralentie par la sécurité

### La solution

- Mise en place d'une solution d'authentification forte, contrôle d'accès et SSO
- Je m'authentifie grâce à mon badge d'accès aux locaux
- Je passe mon badge sur le lecteur et je retrouve mon espace de travail
- Je n'ai plus de mot de passe à taper

### Les bénéfices

- Pour l'IT : Sécurité et traçabilité des accès
- Pour Marie : un processus d'authentification adapté à son contexte d'usage, fluide et sans risque



## Jules, Abonné aux services de VOD d'un grand groupe média

*« Je souhaite accéder à mon espace abonné facilement pour bénéficier de mes services où que je sois et sans crainte de fraude pour mes données personnelles. »*

### Mes attentes

- Un accès simple et rapide à mon espace abonné
- Pouvoir me connecter depuis mon smartphone, ma tablette ou ma box internet et avoir la même fluidité peu importe le device
- Accéder à mes différents services et aux services partenaires sans avoir à saisir de multiples mots de passe
- Être rassuré sur la sécurité de mes données

### La solution

Mise en place d'une solution de CIAM avec gestion de l'identité client, authentification multifacteur, contrôle d'accès et SSO

### Les bénéfices

- Pour l'IT :
  - Augmentation du niveau de sécurité des services en ligne
  - Harmonisation des parcours d'identification, d'authentification et d'inscription en ligne de l'ensemble des sites et applications de mon organisation
  - Intégration des parcours d'inscription sur tous les portails fédérés SSO des partenaires
- Pour Jules : un parcours d'authentification sécurisé, fluide et sans couture, ainsi qu'un ensemble de services tels que l'authentification sociale ou un self-Service de gestion des données personnelles (données d'identité, d'authentification et de fédération, gestion des consentements...) sur l'ensemble de mes périphériques



## Delphine, Responsable IT dans une société leader de mesures d'audience

*« Je souhaite donner un accès à nos médias partenaires à leur espace contenant les services auxquels ils ont souscrit. »*

### Mes attentes

- Gérer le cycle de vie des comptes utilisateurs clients
- Sécuriser les accès clients aux applications auxquelles ils ont le droit
- Capitaliser sur l'infrastructure IAM en place pour la gestion des accès collaborateurs

### La solution

- Mise en place d'une solution d'authentification forte, contrôle d'accès et SSO
- Implémentation d'une solution de gestion du cycle de vie des utilisateurs du SI et de leurs droits

### Les bénéfices

- Un socle IAM unique pour l'ensemble des besoins de l'organisation
- Gestion fine des droits d'accès selon les contrats clients
- Sécurisation des parcours et processus d'authentification

# Parole de client

*L'approche organisationnelle et fonctionnelle des deux sociétés I-TRACING et Ilex a été déterminante pour Médiamétrie. Les 2 experts ont combiné de réels atouts pour mener à bien notre projet d'IAM et ont su conjuguer leurs compétences dans les phases de conception comme de réalisation.*

**Fabrice GRUNCHEC**
Chef de projet IT chez Médiamétrie

# 03

# Santé : un secteur sous tension !

**Guillaume Maquaire**
Manager équipe IAM au Mipih

S'il y a bien un secteur où l'on ne peut ignorer les enjeux de cybersécurité, c'est bien celui de la santé, qui fait malheureusement la Une des journaux de plus en plus souvent ! Le CHU de Rouen en 2019, le CH de Dax en 2021, le CH Sud Francilien en 2022, le CHU de Rennes en 2023 … tous ont subit la tourmente d'une cyberattaque. Et la cybermenace ne diminue pas, bien au contraire ! Les établissements sanitaires et médico-sociaux sont une cible de choix pour les attaquants : les données traitées sont sensibles et de grande valeur, les systèmes sont complexes et vulnérables, les contraintes budgétaires sont fortes… Un cocktail explosif pour des infrastructures critiques !

Conscient de la situation, le gouvernement s'est emparé du sujet et en a fait une priorité nationale. Rappelons en effet que le numérique irrigue aujourd'hui l'ensemble des activités des établissements publics et qu'un dysfonctionnement peut entraîner des conséquences dramatiques. Les programmes et subventions se multiplient pour œuvrer collectivement au renforcement de la sécurité informatique des établissements de santé et mieux les préparer aux situations de crise. Dernier en date, le programme CaRE, annoncé par le Ministère de la Santé et de la Prévention en décembre dernier. Une première tranche de financement de plus de 230 M€ est allouée en 2024 pour un montant global qui pourrait atteindre jusqu'à 750 M€ en 2027.

***« Les RSSI dans le secteur de la santé sont sous pression, ils sont sous le feu des projecteurs et doivent relever de nombreux défis ! »*** explique Guillaume Maquaire, Manager équipe IAM au Mipih. ***« Soulignons tout de même que les SI de santé sont extrêmement complexes et interconnectés et que les données à protéger sont dispersées. Sans compter qu'il subsiste encore des technos vieillissantes, pas toujours simples à maintenir et sécuriser. Au vu des événements récents, les équipes IT ont fortement gagné en maturité sur le sujet cyber et les risques associés c'est certain, mais elles manquent de moyens pour rattraper le retard accumulé. »***

Dans ce contexte, la mise en place d'une stratégie de gestion des identités et des accès par les établissements et entreprises du domaine de la santé est déterminante. Les réglementations et recommandations des organismes tels que l'ANS ou l'ANSSI poussent d'ailleurs dans ce sens. ***« Sur le terrain, même si les RSSI sont parfaitement conscients de la nécessité d'avoir une maîtrise globale de l'IAM, il existe de vraies disparités. »*** poursuit Guillaume Maquaire. ***« Le secteur étant composé d'une multitude d'acteurs de toutes tailles, on comprend aisément qu'un CHU et une clinique de ville n'évoluent pas forcément à la même vitesse.***

***Le point positif c'est que rares sont les établissements qui partent de zéro en matière d'IAM et qu'il existe souvent a minima des solutions éparses pour répondre à des besoins précis. »***

Une des priorités des professionnels de santé est de garantir la confidentialité des données patients. La sécurisation des applications a donc toujours été un enjeu majeur pour les RSSI. S'assurer que seuls les professionnels habilités ont accès aux bonnes informations, et ce indépendamment de leurs points d'accès, prend tout son sens lorsqu'il s'agit de données médicales. En revanche, les types de personnels et les cas d'usages sont multiples et bien spécifiques dans le domaine de la santé.

***« Les mouvements de personnels au sein d'un hôpital sont extrêmement importants. Maîtriser la gestion du cycle de vie des utilisateurs en s'appuyant sur un annuaire d'établissement de santé (AES) est donc indispensable pour réduire le risque opérationnel de failles de sécurité. La théorie est indiscutable… En revanche, dans la pratique, l'IAM n'est malheureusement pas une solution "magique" qui règle tous les problèmes en un clic ! Ce type de projet nécessite l'implication de nombreux acteurs transverses (RH, logistiques, IT, soins, …) afin de mener une réflexion en amont sur les processus métiers de l'établissement. »*** précise Guillaume Maquaire. ***« Et c'est bien là que ça se complique ! Faute de moyens humains et financiers, la gestion des identités et des habilitations n'est pas toujours industrialisée et il n'est pas rare de constater dans de nombreux établissements des comptes génériques partagés ou encore des problèmes de droits non coupés par exemple ! »***

Au-delà des moyens, force est de constater que ces projets sont encore trop souvent perçus comme des projets "techniques" en interne. Malgré une prise de conscience générale du risque cyber, au quotidien l'ADN reste avant tout de soigner. La sécurité passe souvent au second plan et est ressentie comme une contrainte.

***« Sur le volet accès, le SSO et le MFA sont assez rapidement adoptés car cela permet d'amener de la souplesse et de l'ergonomie tout au long du parcours de l'agent. Ne plus avoir à saisir de multiples logins/mots de passe et pouvoir naviguer simplement entre ses différents services applicatifs depuis n'importe quel terminal est un gain de temps précieux ! »*** analyse Guillaume Maquaire. ***« Pour ce qui est du volet gouvernance des identités, la clé est de lotir et d'avancer de façon pragmatique en gardant pour objectif l'automatisation. Cette finalité sera la priorité des équipes métiers qui pourront se décharger de nombreuses tâches à faible valeur ajoutée. Par la même occasion, l'automatisation d'un certain nombre de traitements liés au cycle de vie des utilisateurs permettra de réduire les actions manuelles et facilitera le reporting pour les audits. »***

La tendance de fond du secteur santé est au décloisonnement, à la mutualisation et au partage. L'objectif final est de gagner en efficacité et ainsi d'offrir aux patients une meilleure qualité de soins. Les groupements hospitaliers de territoires (GHT) en sont le parfait exemple. Si aujourd'hui l'intérêt de la mutualisation n'est plus à démontrer, le défi reste de taille. Il s'agit notamment de faire converger des SIH non seulement complexes, mais également très disparates dans leur degré de maturité. Chaque établissement dispose de ses processus, de son parc applicatif, et de ses solutions de sécurité. La gestion des identités et des accès joue un rôle essentiel dans la mise en place d'un espace de communication médical sécurisé. Les solutions doivent être suffisamment agiles pour prendre en compte ces organisations complexes et permettre aux établissements de santé d'ouvrir leur SI en toute sécurité à un écosystème étendu (patients, hôpitaux, médecins de ville, mutuelles, etc.). S'appuyer sur un socle de sécurité de référence qui garantira à la fois le respect de la politique de sécurité et l'interopérabilité avec le monde numérique externe est la clé.

# Zoom sur le terrain

## Virginie, Aide-soignante au Centre Hospitalier

*« Je souhaite accéder facilement et rapidement au dossier médical de mes patients où que je sois dans l'établissement (bloc, chambre, poste kiosque, ...). »*

### Mes attentes

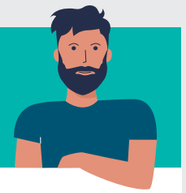
- Un accès simple, rapide et sécurisé au DPI
- Pouvoir me connecter depuis n'importe quels appareils (terminaux aux lits des patients, postes en libre accès dans l'établissement, tablettes...)
- Ma priorité est le soin, parfois l'urgence est vitale, il faut que ça aille vite
- Je dispose d'une carte CPS

### La solution

- Mise en place d'une solution d'authentification forte, contrôle d'accès et SSO
- Je m'authentifie grâce à ma carte CPS à l'ensemble de mes applications, dont le DPI
- Ma carte CPS me permet de me connecter de facon sécurisée sur les postes embarqués sur les chariots médicaux, sur les terminaux aux lits des patients, sur les postes kiosques de l'établissement...
- En cas d'oubli de ma carte CPS, je peux utiliser le mode secours pour me connecter à l'aide d'un mot de passe

### Les bénéfices

- Pour l'IT :
  - Renforcement de la sécurité
  - Respect de la confidentialité des données
  - Audit et conformité réglementaire facilités grâce à une meilleure traçabilité
- Pour Virginie : un processus d'authentification adapté à son métier et ses contraintes



## Pierre, RH au Centre Hospitalier

*« Je souhaite gérer l'arrivée d'un agent hospitalier au sein de l'établissement de façon simple, fluide et immédiate. »*

### Mes attentes

- Permettre à l'agent de prendre son poste le jour J et de bénéficier de toutes les ressources dont il a besoin pour travailler (équipement, badge cantine, accès informatique, ...)
- Ne pas avoir à saisir les informations concernant l'agent dans une multitude d'outils informatique.
- Être en mesure de gérer le personnel (arrivée, départ, mutation, ...) facilement et en temps réel

### La solution

Mise en place d'une solution de gestion du cycle de vie des utilisateurs du SI et de leurs droits au sein de l'établissement

### Les bénéfices

- Pour l'IT :
  - Industrialisation et sécurisation de la gestion des identités et des habilitations
  - Centralisation des identités dans un annuaire de santé
  - Audit et conformité réglementaire facilités grâce à une meilleure traçabilité
- Pour Pierre :
  - Modernisation de l'environnement de travail (fini les processus utilisant des formulaires « papier »)
  - Saisie des données dans un seul outil
  - Gain de temps et productivité dans l'on boarding



# Parole de client

*Les solutions ILEX installées au sein de notre établissement ont permis de sécuriser et fiabiliser l'accès à notre système d'information ainsi que la gestion des habilitations en lien avec l'affectation des agents ; permettant ainsi de répondre aux consignes de limitation de l'accès des utilisateurs aux seules données strictement nécessaires à l'accomplissement de leurs missions. L'accompagnement proposé par le Mipih a permis la mise en place de ces outils en adéquation avec les besoins des utilisateurs et a contribué à faire évoluer la gestion des ressources, les rendant ainsi plus efficientes au fil du temps.*

**Centre Hospitalier Isarien**
Établissement Public de Santé Mentale de l'Oise

**Sabine PARIGOT**
Direction des Systèmes d'Information
au sein du Centre Hospitalier Isarien

# 04

# On aurait aimé vous parler de...

**Guillaume Guerrin**
Directeur Avant-Vente
chez Inetum - Cybersecurity

L'éclairage sectoriel de nos partenaires nous laisse entendre qu'en matière de cybersécurité, et plus particulièrement d'IAM, il est indispensable de comprendre les spécificités métiers et contextuelles d'une organisation pour proposer une réponse adéquate. Il n'existe pas d'approche universelle de l'IAM puisque chaque secteur et chaque organisation est unique. Si nous avons évoqué en détail avec nos partenaires les secteurs de la santé, de l'industrie et des médias, prenons le temps de jeter un coup d'œil du côté des secteurs de la Défense, des collectivités territoriales, des banques ou encore du retail.

Les projets IAM sont essentiellement drivés par 3 enjeux : la sécurité, la conformité et l'expérience utilisateur. Selon les secteurs d'activités, ces enjeux sont plus ou moins prioritaires pour les RSSI de l'organisation. ***« Prenons l'exemple de la Défense. Il s'agit ici d'un secteur d'importance vitale où les infrastructures sont critiques et les réglementations strictes. Les projets d'IAM sont abordés sous le prisme de la sécurité et de la conformité. »*** explique Guillaume Guerrin, Directeur Avant-vente chez Ilex Inetum. ***« Il s'agit avant tout de protéger les accès aux actifs sensibles afin de limiter le risque de failles, de violations de données ou d'attaques, qui peuvent entraîner des conséquences dramatiques. Au vu du rôle capital des organismes de la Défense, l'IAM permet également aux RSSI de répondre au cadre réglementaire rigoureux auquel ils sont soumis.***

***Alors oui, l'expérience utilisateur reste importante pour que la sécurité soit bien acceptée, mais ce n'est pas l'enjeu prioritaire lorsqu'on parle de la Défense. »***

Au-delà de la Défense, la menace fait partie intégrante du quotidien des RSSI du secteur public au sens large, qu'il s'agisse des administrations centrales ou des collectivités territoriales. La sécurité des infrastructures nationales et la protection des données citoyens sont des enjeux gouvernementaux. En parallèle, les administrations et collectivités ont entamé leur transformation numérique afin de répondre aux exigences des citoyens, fortement influencés par leur quotidien de consommateurs numériques. ***« Aujourd'hui, on assiste à une multiplication des services publics numériques à destination des citoyens. »*** analyse Guillaume Guerrin ***« Cette croissance n'est évidemment pas sans risque et c'est bien là toute la complexité : il faut réussir à ouvrir son système d'information tout en renforçant la sécurité et en proposant un espace numérique moderne à l'ensemble des citoyens ! C'est là qu'entre en jeu l'IAM, qui permet aux RSSI de répondre à la fois aux besoins des agents et aux attentes des citoyens, tout en respectant les obligations réglementaires et normes sectorielles. »***

L'ouverture vers l'extérieur et le développement important de services numériques est également une tendance forte du secteur bancaire ces dernières années.



***« La directive DSP2 a d'ailleurs accéléré les choses et poussé le secteur à s'ouvrir encore plus et à s'engager dans l'ère de l'Open Banking. On voit arriver de nouveaux entrants qui proposent des services innovants et réinventent le business model.*** » selon Guillaume Guerrin ***« Aujourd'hui, l'expérience client est un véritable levier de croissance sur un secteur où la concurrence est de plus en plus rude. »***

Rappelons que le secteur financier est particulièrement exposé à la cybercriminalité. De nombreuses études soulignent une augmentation significative des tentatives de fraudes bancaires ou d'usurpations d'identités ces dernières années. C'est notamment la raison pour laquelle le cadre réglementaire a significativement évolué et est particulièrement exigeant. Les obligations en matière de contrôle interne sont strictes et les audits sont nombreux.

Ouvrir davantage le système d'information tout en garantissant le niveau de sécurité le plus élevé possible face aux risques d'attaques exige de mettre en œuvre une architecture de protection vertueuse selon une approche "Security by design".

***« Le socle technologique de cette architecture doit impérativement s'appuyer sur une solution intégrée de gestion des identités et des accès, à laquelle seront raccordés tous les services et autres applications. »*** explique Guillaume Guerrin ***« L'IAM est le seul moyen de remettre l'utilisateur au cœur du système d'information de manière maîtrisée, de contrôler son identité et ses habilitations et de valider ses accès. »***

À noter qu'il est important d'opter pour une solution qui permet d'intégrer les derniers standards d'authentification pour ne pas s'enfermer dans des impasses technologiques. Cela permettra aux RSSI de tendre vers de nouvelles méthodes d'authentification, et notamment le passwordless qui se dessine comme l'une des tendances fortes des années à venir.

***« Le passwordless n'est pas un simple buzz word, c'est une avancée majeure dans le domaine de la sécurité des accès. »*** selon Guillaume Guerrin ***« Nous avons aujourd'hui de nombreux clients qui ont des cinématiques d'authentification sans mot de passe. Je pense notamment à certains acteurs du retail qui offrent à leurs conseillers de vente un parcours sans couture à leurs sessions de travail en magasin. Aucun mot de passe, un accès fluide à sa session de travail dans l'ensemble des postes partagés du magasins et le tout en s'authentifiant rapidement via un badge ! »***

Les outils digitaux et innovations technologiques ont profondément transformé le retail, et notamment le rapport que les entreprises entretiennent avec le consommateur. Le consommateur est avide de nouveaux services, de nouvelles expériences, d'innovations… Toute la stratégie de vente des entreprises s'en trouve bouleversée et il est impossible de faire l'impasse sur ce nouveau business modèle. La DSI doit être en mesure d'accompagner les enjeux stratégiques de l'entreprise. Il faut proposer des solutions répondant à la fois aux attentes des consommateurs et des métiers, sans pour autant rogner sur la sécurité et les menaces croissantes et omniprésentes. Les entreprises qui réussissent le mieux dans le domaine sont celles qui ont parfaitement appréhendé un parcours du consommateur de plus en plus hybride.

***« Pour ce qui est du parcours on-line, de nombreuses enseignes proposent par exemple des authentifications sociales via des mécanismes de fédération d'identité. Le principe est simple : un consommateur authentifié sur un réseau social peut accéder directement aux sites de ces enseignes et à leurs contenus, sans avoir à créer un nouveau compte utilisateur. Ce parcours d'acquisition étant fluidifié, le risque de perdre le consommateur, rebuté par une énième inscription en ligne, est considérablement limité. »*** explique Guillaume Guerrin. ***« En magasin, permettre aux conseillers de vente afin d'accompagner les clients tout au long de leurs parcours d'achat est une cinématique rendu possible grâce à l'IAM également. »***

# De **beaux succès métiers...**


### Visionnez le webinar Leroy Merlin

Postes partagés : 12 ans que **Leroy Merlin** a fait le choix du sans contact pour une expérience utilisateur inégalée


### Visionnez le webinar du CD95

Retour sur l'évolution de la stratégie de gestion des identités et des accès du **Conseil Départemental du Val d'Oise (CD 95)**


### Visionnez le webinar Airbus Cybersecurity

Retour d'expérience **Airbus Cybersecurity** : la gestion des identités et des accès au cœur du SOC


### Consultez la success story Natixis

**Natixis** sécurise ses accès et améliore l'expérience utilisateur grâce à la solution Ilex Access Management



# ... basés sur **Ilex IAM Platform**

- Une **couverture de l'IAM à 360°** grâce à une offre unique pour adresser l'ensemble de vos besoins **IAM & CIAM**
- Des solutions co-construites avec nos **communautés d'utilisateurs** afin de répondre aux **évolutions métiers**
- Un socle **pérenne et évolutif** pour une stratégie IAM optimale
- Une gamme de **solutions éprouvées**, **rapides à déployer**, couvrant les besoins des plus standards aux plus spécifiques

## **Une plateforme unique** pour vos clients, vos partenaires et vos collaborateurs

Ilex. Access Management Solution inetum.

Ilex. Identity Management Solution inetum.


Ilex. Customer IAM Solution inetum.

Des solutions disponibles en modes SaaS, On-premise et hybride

# Nos partenaires

formind

Formind est un leader français indépendant expert en cybersécurité. Notre mission est simple et belle : protéger nos clients.

Qualifié PASSI, en cours de qualification PRIS par l'ANSSI et certifié ISO 27001, nous aidons nos clients à être plus résilients et à se protéger des risques numériques à travers nos trois métiers : CONSEIL - INTÉGRATION - SOC&CERT.

Formind adresse les expertises suivantes :

- Gouvernance Cyber : Stratégie, gestion des risques, pilotage et contrôle
- Continuité, crise et résilience
- Conformité légale, réglementaire et normative
- Expertise technique, architecture, Cloud, IAM, OT
- Intégration de solutions
- Audits techniques, sûreté, redteam
- Services managés (CERT, SOC, vulnérabilités) et gestion d'incident (FIR)
- Formation

Formind propose également une offre dédiée au tissu économique des ETI et PME-PMI, venant répondre à leurs problématiques spécifiques de cybersécurité.

**formind.fr**

i-TRACING CYBERSECURITY

**I-TRACING, Human Intelligence for Cybersecurity**

I-TRACING est un pure-player français des services de cybersécurité qui accompagne de plus de 400 entreprises leaders à travers le monde, dont 35 acteurs du CAC 40.

De l'anticipation proactive des menaces à la mobilisation ultra-réactive de ses équipes en cas d'attaque, I-TRACING propose une gamme complète de services de cybersécurité allant du conseil à l'intégration, aux services managés, SOC et CERT Follow The Sun 24/7.

En tant que partenaire de confiance, I-TRACING donne aux organisations les moyens de se développer à la hauteur de leurs ambitions digitales et peut compter sur l'engagement de ses 600 experts en France, en Suisse, en Grande-Bretagne, à Hong Kong, au Canada, en Chine et au-delà.

I-TRACING réalise un CA plus de 115 millions d'euros en 2023 et est détenu par ses fondateurs et managers ainsi que par les fonds d'investissement Eurazeo et Sagard NewGen.

**i-tracing.com**

mipih

Le Mipih, éditeur public investi sur le marché de la e-santé, s'engage à redonner du temps aux acteurs de soins en leur fournissant des solutions numériques performantes, sécurisées, éthiques et souveraines ; en cohérence avec les politiques publiques de santé. Le groupement compte 4 agences, à Toulouse, Amiens, Bordeaux, Reims et un bureau à PariSanté Campus.

**mipih.fr**

## À propos d'Inetum, division Software

La division Software du groupe Inetum est n°1 des éditeurs multi-métiers avec 27 centres de R&D et plus de 50 logiciels dans le domaine des Ressources Humaines, de l'Assurance, de la Finance, du Secteur Public, de la gestion de documents et de la cybersécurité. L'innovation est le principal moteur de développement des solutions d'Inetum grâce à l'industrialisation des composants de ses FabLab (mobilité, chatbot, RPA, Flex Office…), à ses expertises métier et aux évolutions technologiques (Move-to-Cloud). d'organisation sectorielle et de solutions de qualité industrielle. Présent dans plus de 27 pays, le Groupe compte près de 27 000 collaborateurs et a réalisé en 2021 un chiffre d'affaires de 2,2 milliards d'euros.

## À propos d'Ilex IAM Platform

Dans le domaine de la cybersécurité, Inetum accompagne ses clients dans leur stratégie IAM grâce à la plateforme Ilex Identity & Access Management. Cette offre complète se décline en 3 gammes de solutions (Ilex Access Management, Ilex Identity Management et Ilex Customer IAM) afin de proposer un socle solide capable de concilier sécurité et expérience utilisateur. Forte de plus de 300 clients et 14 millions d'utilisateurs à travers le monde, l'offre allie innovation, flexibilité et performance. Disponible en modes SaaS, On-premise et hybride, elle s'adapte parfaitement aux besoins complexes des organisations et aux évolutions du marché.



Cybersecurity Solutions.

inetum