

Focus sur Nicolas Alamome IAM Tribe Leader et BPL Cyber Sécurité

Nicolas Alamome est Business Partner Lead Cyber Sécurité et IAM Tribe Leader. Il nous explique lors cette interview son métier, et démystifie les questions autour de l'identité

Vendredi 30 avril, 2021 · 8 min. de lecture ·

🔒 2 🗨️ 0 ➦



Nicolas ALAMOME est Business Partner Lead Cyber Sécurité et Identity Access Management (IAM) Tribe Leader. Implanté en France, il est responsable de la mise en place et de la structuration d'un IAM Security à l'échelle du groupe Thales.

Comment es-tu devenu tribe leader ?

Je suis arrivé chez Thales, il y a 7 ans en tant qu'architecte sécurité, pour travailler sur des sujets de remise en conformité des systèmes d'information. Suite à quoi j'ai piloté l'équipe d'architectes travaillant sur ces sujets et nous avons créé une équipe d'expert dédié aux sujets de sécurité IAM (DSV – Directory Services).

Historiquement, cette équipe intervenait sur des sujets liés à l'active directory* et sa sécurisation. Nous avons diversifié nos offres pour intervenir globalement sur tous les sujets d'identité.

J'ai ensuite pris la responsabilité du département ISS (département des projets de sécurité France), en plus de mes responsabilités historiques.

Lorsque NexGen est arrivé, j'ai contribué à la création de la Value Tower Cyber Sécurité et j'ai eu la responsabilité de construire le modèle opérationnel cible de la Tribe IAM. Ainsi lorsque les candidatures ont été ouvertes, je me suis naturellement positionné sur le poste de Tribe leader IAM.

**L'active directory est un annuaire, une base de donnée qui centralise les accès (postes, serveurs, comptes utilisateurs, etc.) du parc informatique et permet de les gérer de manière centrale.*

Qu'est ce que la Tribe Identity Access Management ainsi que son ambition?

La Tribe IAM est une des deux composantes la Value Tower Cyber Sécurité. Elle contribue à élever le niveau de sécurité globale de nos infrastructures, améliorer l'expérience utilisateur, et faciliter les échanges et les interactions.

Elle se compose de trois piliers étroitement liés entre eux et transverses sur toutes entités:

- L'Identity Management (IdM)
- L'Access Mangement (AM)
- Le Privilege Access Management (PAM)

Son ambition globale est d'être facilitatrice en étant au service des autres Value Tower, des business et des utilisateurs, qu'il s'agisse de nos collaborateurs ou de nos partenaires externes.

Les objectifs sont les suivants :

- Définir une vision en se basant sur les visionning Workshop
- Créer une cohésion d'équipe et un sentiment d'appartenance
- Organiser les services de ses trois composantes qui hier étaient dispatchés dans plusieurs équipes
- Insuffler les principes agiles
- Etre proche de nos business
- Anticiper les besoins

Nous travaillons de pair avec les Global Chapters Lead et les Locals Chapters Lead afin de connaître les talents présents dans les autres pays. Cette richesse sera un atout indéniable dans la réussite de nos projets et l'atteinte de nos objectifs.

Aujourd'hui chaque pays, ou chaque région a sa propre identité ?

Aujourd'hui le master data EDIR est utilisé dans tous les pays de Thales, nous avons donc une identité maîtresse disponible partout.

L'utilisation et la déclinaison dans les systèmes de cette identité dans les différents pays peuvent cependant être différentes. Un des objectifs de la tribu est de pouvoir proposer des outils, des processus, afin de décliner cette identité de manière standardisée et normalisée dans les différents systèmes et applications.

Le challenge de l'IAM est de faire face à un monde qui bouge vite, qui se digitalise mais qui doit aussi assurer la pérennité des infrastructures historiques. Aujourd'hui on ne peut plus gérer de manière unitaire les identités et les accès, il faut créer et **gérer une identité unique et sécurisée** qui soit distribuée, qui soit performante pour simplifier les accès à tous les services, pour les utilisateurs, et peu importe qu'on soit en cloud ou On-Premise.

L'identité de demain est le nouveau firewall"

Quels sont les risques, s'il y a des failles sur ces aspects-là ?

La question est complexe et les risques sont multiples. Pour comprendre les enjeux je vous propose des parallèles de vulgarisation sur les 3 aspects de l'IAM.

IdM : Que se passerait-il si votre identité numérique était usurpée ? Si une personne mal intentionnée se faisait passer pour notre PDG ?

AM : Que se passerait-il si votre mot de passe était compromis et connu de tous ?

PAM : Que se passerait-il si les droits donnés à un collaborateur lui permettaient d'avoir accès à des informations ou des documents en dehors de son domaine de responsabilité ? Les feuilles de paye par exemple ?

Je me ferai un plaisir de pouvoir échanger avec qui le souhaite sur ces aspects J

Je vous invite aussi à visionner la vidéo de sensibilisation disponible sur [ThalesTube \(KeyWord DSV\)](#).

Quel seront les challenges à venir ?

Le premier challenge vient du fait que l'IAM est une brique de sécurité, et aujourd'hui encore, la sécurité est vue aux yeux de beaucoup comme quelque chose de compliqué, qui empêche le projet d'avancer vite et qui a un coût. Mon premier challenge est de faire changer cette vision. Je souhaite définir **l'identité comme un service**, je veux que les utilisateurs puissent consommer et utiliser leur identité et leur accès, de manière transparente.

Et pour ce faire, il faut que nous soyons intégrés **dès le début des réflexions dans les projets** pour pouvoir anticiper ou à défaut orienter de la meilleure façon l'implémentation et le design des solutions.

Le sponsorship est un facteur important dans les sujets d'IAM. Toutes les fonctions ont un rôle à jouer. Les RH, la finance, l'ingénierie, le hosting, les applications, le workplace, la collaboration. Bref vous l'aurez compris l'IAM est transverse.

Le deuxième challenge va être de **réussir la fusion et définir les synergies entre les 3 domaines que nous avons évoqué précédemment.**

Donner un sens commun et avoir une définition commune de ce qu'on souhaite faire et comment on veut le faire. Derrière les identités numériques, il y a des humains, (des machines aussi, mais restons sur les humains), il va falloir réussir à embarquer ces personnes-là et les faire aller dans le même sens pour travailler le plus efficacement possible.

En quoi Next Gen peut vous aider ?

J'aimerais que la **sécurité et l'identité soit inscrite dans l'ADN** de chacun des **projets** que les service owner et product owner ainsi que les tribe leaders ont. Ce sont eux qui vont pouvoir porter les bons messages et qui vont pouvoir guider les membres de la squad et les accompagner.

Personnellement, je passe d'une posture franco-française, à une **posture worldwide**, et en deux mois, avec des synergies qu'a réussi à amener Next Gen IS/IT, le changement d'état d'esprit chez les gens est assez impressionnant. Des personnes de plusieurs pays sont curieuses et demandeuses de tous ces schémas d'architecture liés à la sécurité et de l'identité, et veulent implémenter ces modèles-là. Nous avons aussi beaucoup à apprendre tous ensemble.

Un deuxième **avantage** important se joue **au niveau des compétences**, nous allons pouvoir aller discuter avec nos pairs dans les autres pays pour comprendre leur choix d'implémentation de certaines solutions techniques, de certains designs et on va pouvoir les challenger et eux aussi vont pouvoir nous challenger.

Quelles sont les prochaines étapes ?

On a initié une synchronisation du « who is who » au sein de la VT, effectivement Next Gen transforme beaucoup de choses, j'ai besoin de créer ce sentiment d'appartenance au sein de ma tribu et aussi au sein de la VT. Avec Samuel Bird qui est le tribe lead sur la partie Cyber défense nous organisons régulièrement des échanges entre nos Product/Service Owners.

La prochaine étape qui arrive dans quelques jours est l'organisation de la première VTEC (Value Tower Executive Committee).

Un mot aux personnes qui sont dans ta tribe, et pour les personnes qui souhaitent te rejoindre ?

Ce que je veux leur dire, c'est qu'aujourd'hui nous travaillons tous dans l'intérêt commun de Thales, **on ne travaille pas pour une équipe mais pour Thales**.

Mon message: Venez travailler avec nous et venez écrire cette histoire, cette vision, et venez construire chaque marche pour pouvoir avancer sur ce chemin. Il y a plein de choses à construire, y a plein de choses à faire, l'identité c'est le futur firewall. Les challenges et les opportunités seront nombreux pour pouvoir se dépasser intellectuellement parlant !

Overview des squad de la tribe Identity Access Management

Squad AD Convergence : En cours de training dont le Product Owner est **Edith FEVRIER**. Cette squad se retrouve dans le domaine Identity Management. Cette squad a pour objectif de faire converger infrastructures informatiques des entités d'une GBU en un seul domaine.

Squad SAAM : SAAM est un bastion d'administration dont le PO est **Raphael KNEIP**. Cette squad se retrouve dans le domaine Privilège access Management.

Squad LUCI : LUCI est une solution d'authentification et d'administration des identités pour les utilisateurs et les ordinateurs (postes et serveurs). Le PO est Olivier ISNARD. Cette squad se retrouve dans le domaine Privilège Access Management.

Squad MFA+ : Multi Factor Authentication : **Jean Christophe de MAISONNEUVE** est le Product Owner. Cette squad se retrouve dans le domaine Access Management.

Cette squad permet de sécuriser l'authentification en appliquant une solution adaptative, flexible et globale qui permet d'adapter les méthodes d'authentification aux enjeux de sécurité tout en optimisant l'expérience utilisateur. Un premier succès de cette squad a été le déploiement de la solution sur **~18 000** utilisateurs DIS pour accéder à leur messagerie office 365.

Squad Service Trusted Core : Le service Owner est **Olivier LAUSSINE**. Cette squad se retrouve dans le domaine Privilège access Management.

C'est la solution de PAM de tout le système d'information France. Elle permet aux 800 administrateurs qui l'utilisent de travailler quotidiennement de manière sécurisée Cette solution a été co-construite entre Microsoft / Thales et l'ANSSI.

[Plus d'informations ici](#)

👁 205 vues