Une gestion agile, sécurisée et efficace des droits d'accès

Enjeux :

> Standardisation et automatisation de la création des comptes et des droits
> Gestion fluide et sécurisée des droits à l'arrivée, lors des mouvements et départ
> Traçabilité des droits attribués

Solution :

> cyberelements Identity

Bénéfices :

> Structuration des process d'attribution des droits d'accès
> Gestion agile des comptes et habilitations
> Renforcement du niveau de sécurité des accès

cyberelements Identity est une solution structurante qui nous permet de standardiser et automatiser la création des droits d'accès et de gérer de manière sécurisée le flux d'entrée et sortie des collaborateurs. C'est un pilier dans la sécurisation de nos process qui apporte également un réel confort à l'équipe informatique mais aussi aux utilisateurs.

Fabrice Le Bouquin
IT Manager chez GIMA

Les enjeux

GIMA (Groupement International de Mécanique Agricole) est l'un des acteurs mondiaux des systèmes de transmission pour tracteur agricole. GIMA est une joint-venture 50/50 entre deux entreprises du top cinq mondial de l'industrie du machinisme agricole : AGCO et CLAAS.

Ces équipes conçoivent et fabriquent une large gamme de produits de haute technicité (boîtes de vitesse et ponts arrière de 75 à 396 ch.) pour les fabricants de machines agricoles AGCO et CLAAS.
GIMA s'appuie sur l'expertise et le savoir-faire de plus de 700 collaborateurs pour produire 20 000 transmissions en moyenne par an.

La direction informatique du GIMA est composée de 15 personnes dont la mission est de garantir le fonctionnement et la sécurité des réseaux, du matériel informatique, de la téléphonie et des applications industrielles.
Véritable support pour les équipes de bureau et d'atelier, l'équipe informatique assure la fluidité et la robustesse du système d'information GIMA.

L'enjeu principal du département informatique du GIMA était d'uniformiser et d'automatiser la création des comptes et des droits d'accès aux différentes ressources du système d'information tout en accroissant la sécurité.

La solution

Afin de répondre à cet enjeu, Mme Frédérique Baroux, Chargée de projets et support, et Mr Fabrice Le Bouquin, Responsable du service informatique, ont recherché une solution de gestion des identités.

cyberelements Identity, solution d'IAM dont l'approche organisationnelle combine les modèles RBAC, ABAC et ORBAC, a été retenu par le GIMA. Il leur a permis de relever le défi en structurant les processus d'une part et en modélisant leurs standards.

Différents objectifs ont pu être atteints grâce à cyberelements Identity :
- Standardisation des caractéristiques d'un compte AD
- Respect du standard en place
- Limitation des accès directs à l'AD
- Gestion fluide et sécurisée du flux d'entrée/sortie des collaborateurs
- Gestion fluide et sécurisée des mouvements de collaborateurs pour éviter des cumuls de droits suite à des changements de service.
- Garantie de traçabilité des actions sur un compte tout au long de son cycle de vie : bon droit attribué à la bonne personne au bon moment.

Déployé depuis 2 ans au sein de GIMA, la solution cyberelements Identity est essentiellement utilisée pour gérer les comptes AD, les droits d'accès sur les serveurs de fichiers ainsi que les accès aux applications métiers. Son interfaçage avec l'outil GLPI permet de générer des tickets qui apportent beaucoup de rigueur dans toute cette gestion notamment par l'utilisation de workflows.

Structuration des process d'attribution des droits d'accès

Deux référentiels alimentent en amont cyberelements Identity. Le département informatique a donc travaillé en étroite collaboration avec le département Ressources Humaines pour remettre à plat les process de création de comptes et d'attribution des droits en rationalisant les profils, en corrigeant les incohérences et en supprimant les droits non standards afin d'aboutir à la standardisation du process de création des comptes.
Cette collaboration a permis de lister les droits les plus utilisés et de créer en conséquence une matrice de droits pour aboutir à des règles d'habilitation exploitables.

Aujourd'hui, le process de création de compte est complètement automatisé pour les droits standards. L'équipe informatique conserve une attribution manuelle pour des droits plus spécifiques mais travaille avec les différentes directions métiers pour continuer à affiner les standards et éviter autant que faire se peut tout droit spécifique.

Gestion agile des comptes et habilitations

Avec l'automatisation de l'attribution des droits d'accès, le service informatique reçoit beaucoup moins de demandes d'accès à traiter manuellement, notamment lors des mouvements de collaborateurs (les arrivées et changements de service), ce qui représente un gain de temps indéniable pour les équipes qui n'ont plus à gérer les allers-retours via tickets ou téléphone. Elles peuvent se consacrer à d'autres projets.
Les fonctionnalités avancées de workflow permettent de mettre en place des notifications confirmant à l'arrivée d'un collaborateur que son compte a bien été provisionné et d'envoyer à son manager ses identifiants.

« Au moment du départ du collaborateur, un workflow notifie le dé-provisionnement du compte et indique alors à l'informatique les opérations à effectuer par l'intermédiaire d'un ticket. »
En s'appuyant sur le modèle ORBAC de cyberelements Identity, GIMA bénéficie à présent d'une gestion agile et fiable des mouvements de personnel (arrivées, départs, changements de poste, etc.) qui permet une attribution automatique des droits dès que le changement de service est effectif. En effet, certains droits peuvent être directement gérés au niveau de l'organisation, ce qui offre rapidité et efficience.

Renforcement du niveau de sécurité des accès

L'interfaçage de cyberements Identity avec le référentiel RH garantit la fiabilité des données au moment de la création des comptes et de l'attribution des droits. Une resynchronisation des référentiels est même possible à tout moment.
cyberements Identity propose des fonctionnalités de traçage et de contrôle qui permettent à GIMA de démontrer, lors des audits du système d'information, que les circuits de départs sont sécurisés, en apportant toutes les évidences attendues par les auditeurs.
Grâce au mécanisme de workflow, lors d'un départ de collaborateur, un ticket GLPI va être créé et celui-ci restera ouvert tant que les droits ne seront pas dé-provisionnés. Ceci permet d'éviter les comptes dormants, le cumul des droits, et élève nettement le niveau de sécurité avec la suppression des droits dès que le collaborateur a quitté la société.

« Aujourd'hui l'équipe s'est vraiment appropriée la solution. cyberements Identity, avec ses fonctionnalités d'automatisation, de synchronisation, de traçabilité et de workflow, est devenu un des piliers de la sécurisation de nos processus, un outil indispensable et incontournable pour l'équipe informatique » conclut Monsieur Le Bouquin.

À propos de cyberlements Identity

cyberelements Identity est un produit de Gestion et de Gouvernance des Identités (IGA, Identity Governance and Administration). Il offre un référentiel des identités d'employés (méta-annuaire) et permet de gérer leurs habilitations, en garantissant une parfaite cohérence entre votre système d'information RH et votre système d'information de production. Grâce au produit, vous pouvez automatiser vos workflows de demande d'accès, vos processus d'arrivée, de mobilité ou de départ de personnel, et provisionner automatiquement les comptes et les droits dans les applications et systèmes cibles (notamment l'annuaire Active Directory ou équivalent). Le produit permet aussi de garantir la cohérence des habilitations (SoD, segregation of duties) et de réaliser des campagnes de certification de droits, pour les auditeurs de vos contrôles internes ou externes.
Le produit tire sa puissance d'expression des règles d'habilitations en combinant les modèles RBAC, ABAC et OrBAC, permettant une gestion agile des droits et habilitations dans des contextes multi-identités/multi-établissements, et une véritable réactivité dans un contexte de crises permanentes. Il apporte des fonctionnalités de synchronisation des données pour garantir que chaque utilisateur dispose du bon accès au bon moment.

À propos de Systancia

Systancia est un éditeur de logiciels de cybersécurité indépendant et souverain, animé par le concept de Zero Trust.
Notre mission est de fournir aux organisations les éléments cyber nécessaires pour booster leur performance grâce à la confiance numérique. Pour ce faire, nous réunissons nos propres technologies dans une plateforme unique, combinant rapidité et facilité d'utilisation pour favoriser la productivité des utilisateurs et la performance des organisations.
La plateforme Zero Trust de Systancia permet de donner aux collaborateurs ou aux prestataires, quel que soit leur contexte (au bureau, en télétravail, chez un prestataire, opérateur industriel …) un accès transparent, immédiat, sécurisé et tracé (métier ou privilégié, local ou distant, …) à toutes les ressources dont ils ont besoin pour travailler (applications cloud, applications dans le datacenter de l'organisation, postes de travail, données, infrastructures informatique ou industrielles, services).