Supervision des accès critiques et gouvernance de la sécurité IT

Contexte & enjeux

Dans un environnement multi-sites intégrant des systèmes IT et IoT, le RSSI doit protéger les données, réduire les risques et maintenir une gouvernance de sécurité claire, sans freiner les usages métier ni multiplier les outils.

Attentes clés :

- **Supervision en temps réel** des accès critiques et des droits sensibles.
- **Réduction des risques** liés aux droits excessifs, aux comptes dormants et aux comptes techniques.
- **Conformité démontrable** (SoD, audits internes et externes, ISO, RGPD) avec une piste d'audit claire.
- **Contrôle centralisé des accès** collaborateurs, prestataires et comptes techniques.
- **Intégration fluide** aux systèmes existants, sans refonte complète.
- **Sécurisation** des transformations et des nouveaux usages dans un cadre maîtrisé.
- **Meilleure visibilité** pour piloter les risques, les écarts et les actions correctives.

Promesse RSSI : Superviser en temps réel les accès critiques, renforcer la sécurité des identités et garantir une traçabilité exploitable pour la conformité, les audits et la gouvernance.

Ce que ROK apporte

- **Organigramme dynamique = source de vérité :** l'organisation réelle (rôles, sites, responsabilités) alimente automatiquement les droits, les workflows et les contrôles, en lien direct avec le SIRH et l'annuaire électronique.

- **IGA piloté par le métier :** chaque mouvement IN / MOVE / OUT met à jour les accès des collaborateurs et prestataires, avec journal d'audit exploitable et contrôles automatisés des droits d'accès.

- **Contrôles SoD & risques intégrés :** détection des conflits de rôles ou d'utilisateurs, avec alertes, validations et traitements automatisés.

- **IT et IoT :** gestion centralisée des accès pour les collaborateurs, prestataires et comptes techniques (robots, services, intégrations), avec durée d'accès maîtrisée, expiration automatique et traçabilité complète.

- **Transformation sécurisée :** applications, workflows et automatisations modélisés en no-code assisté par IA générative, dans un cadre gouverné et traçable.

- **Interopérabilité complète :** intégrations avec SIRH, annuaires, ITSM, ERP, plateformes IAM / IGA existantes et MCP, sans complexifier l'existant.

Résultats observés chez nos clients

Novares
(industrie, 23 pays multi-filiales)

- Organisation et IAM unifiés.
- Référentiel unique à jour en continu.
- Validations plus rapides et meilleure visibilité sur les droits d'accès.

Elis
(ERP, déploiement international)

- Automatisation et sécurisation des accès.
- Standardisation multi-sites, droits délivrés 5× plus vite.
- Coûts d'administration ÷10.

Transdev
(référentiel fournisseurs / P2P)

- Standardisation et sécurisation des données.
- Plus de 1 000 demandes/mois traitées automatiquement via OCR et workflows.
- Conformité renforcée.

Concrètement chez vous : Les mêmes mécanismes peuvent être activés pour les accès collaborateurs et prestataires, le contrôle automatisé des droits, la traçabilité des actions, la réduction des comptes à risque et la production de rapports consolidés.

Modules clés ROK

A. Organigramme dynamique & rôles

- **Modélise l'organisation et l'écosystème** (sites, BU, sous-traitants), gère rôles et responsabilités, et alimente automatiquement les droits d'accès.
- **Who's Who visuel**, filtres multi-critères, historique des postes.

B. IGA & supervision des accès critiques

- **Automatise** la création, l'affectation et le retrait d'utilisateurs et de droits (rôles métiers et droits applicatifs - RBAC / ABAC) à partir du SIRH ou de l'annuaire électronique.
- **Orchestre l'ensemble du cycle des accès :** demande → approbation → provisioning → contrôle des droits → retrait, avec notifications et contrôles SoD.
- **S'intègre nativement à l'ITSM** déjà en place, pour provisionner les accès sans reconfigurer l'écosystème.

C. Contrôles continus & préparation des audits

- **Contrôles configurables** (périmètre, fréquence, seuils), alertes en cas de droits excessifs, comptes dormants ou écarts.
- **Journal d'audit** lisible et rapports consolidés en quelques clics (SoD, ISO, finance, RGPD).
- **Visibilité** claire pour les audits, la sécurité et les équipes de gouvernance.

D. Intégrations & architecture

- **Connecteurs natifs** SIRH (Workday, SuccessFactors, Oracle...), Active Directory (Entra ID), ITSM, ERP et plateformes IAM / IGA préexistantes.
- **MCP :** activation rapide de milliers d'intégrations sans développement spécifique.
- **IA exogène au choix :** accélère la modélisation des workflows et applications tout en garantissant la confidentialité.
- **Applications et robots créés sans code**, publiés rapidement et maintenus par les équipes métiers.

Bénéfices attendus

- **Protection renforcée des données :** accès mieux maîtrisés, droits excessifs réduits, comptes à risque mieux suivis.
- **Gestion des risques simplifiée :** visibilité en temps réel sur les accès critiques, les écarts et les actions correctives.
- **Conformité facilitée :** audits internes et externes mieux préparés, preuves disponibles à tout moment.
- **Transformation sécurisée :** innovation et automatisation possibles dans un cadre gouverné.
- **Réduction de la complexité :** moins d'outils fragmentés, moins de traitements manuels, moins d'angles morts.
- **Support aux métiers :** sécurité renforcée sans ralentir les usages ni les projets.

Proposition de démonstration (30 min)

Périmètre conseillé : un site ou une entité + une application sensible + un scénario réel de gestion des accès (arrivée d'un collaborateur, accès d'un prestataire ou retrait d'accès).

Étapes :

1 – Organisation & accès	2 – Contrôle des droits	3 – Traçabilité & conformité	4 – Intégration & projection
• Visualisation de l'organigramme dynamique. • Rôles et responsabilités associés aux accès. • Identification des accès sensibles.	• Gestion des accès lors d'une arrivée ou d'une mobilité. • Contrôles SoD, et détection des écarts. • Mise à jour automatique des droits.	• Journal d'audit • Exemples de rapports consolidés • Visibilité sur les contrôles et les actions correctives.	• Connexion aux systèmes existants (SIRH, annuaire, ITSM). • Démonstration d'un scénario concret de gestion ou de retrait d'accès.

À l'issue de la démonstration : une vision claire des mécanismes activables chez vous, des gains potentiels et des premiers cas d'usage à prioriser.

Et si nous organisions un échange de 15 minutes ?