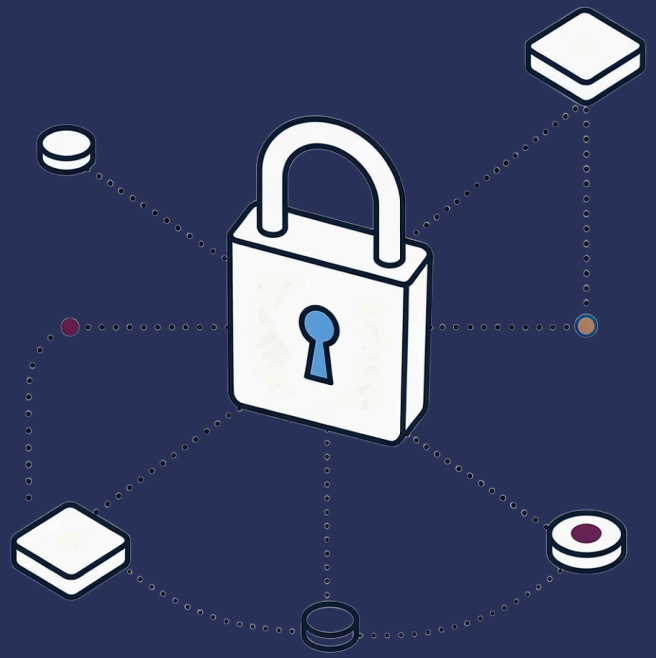
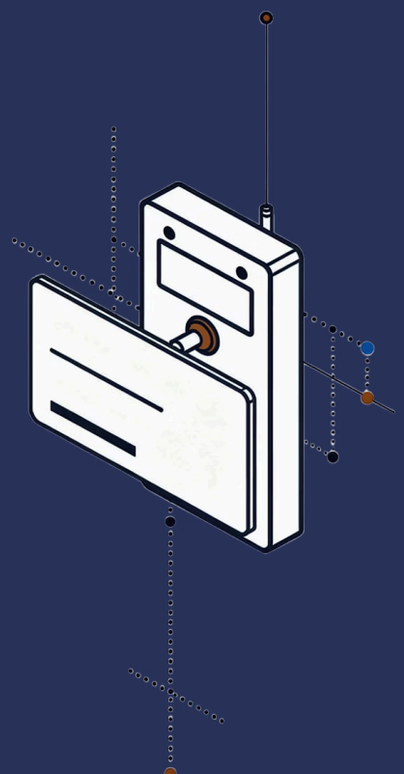


Identity and Access Management

Un pilier essentiel pour la cybersécurité, la gouvernance et la conformité TISAX



L'IAM va bien au-delà de la création de comptes

Un contrôle de sécurité majeur

Garantir que les bonnes personnes disposent des bons accès, au bon moment, et uniquement pour ce dont elles ont besoin.

Un enjeu stratégique

L'IAM protège les données sensibles, réduit la surface d'attaque et constitue une exigence fondamentale des référentiels de sécurité comme TISAX.

Une responsabilité partagée

IT, cybersécurité, management et métiers sont tous acteurs de la gouvernance des accès.

Objectifs principaux de l'IAM

Comptes nominatifs

Chaque utilisateur dispose d'un compte personnel et traçable.

Moindre privilège

Accès limités au strict nécessaire selon le rôle.

MFA

Authentification multi-facteurs obligatoire pour tous les accès sensibles.

Contrôle des admins

Comptes privilégiés strictement encadrés et surveillés.

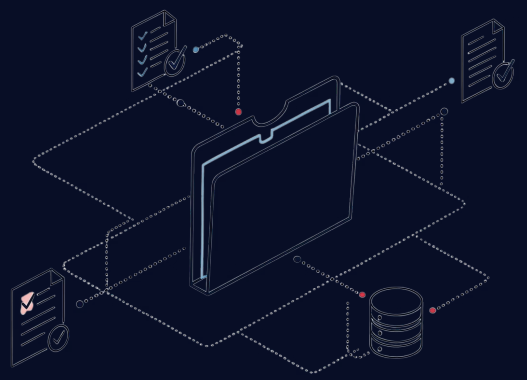
Traçabilité

Journalisation de toutes les actions d'accès.

Revues régulières

Validation périodique des droits et gestion des exceptions.

IAM et conformité TISAX



1 Préparation aux audits

L'IAM fournit les preuves documentées exigées lors des évaluations TISAX : journaux, revues et validations horodatées.

2 Documentation ISMS

Les politiques d'accès, les rôles et les exceptions doivent être formalisés dans le système de management de la sécurité.

3 Exigences de contrôle d'accès

TISAX impose la gestion des droits, la séparation des rôles et la traçabilité des accès aux informations sensibles.

Les principaux risques IAM à maîtriser

Comptes orphelins

Comptes actifs d'anciens collaborateurs ou prestataires non désactivés.

Droits excessifs

Accumulation de privilèges au fil du temps sans revue.

Comptes génériques

Comptes partagés sans traçabilité individuelle.

Authentification faible

Absence de MFA sur des accès critiques.

Comptes de service non maîtrisés

Identifiants techniques sans propriétaire ni revue.

Accès externes non revus

Partenaires ou invités avec des droits persistants.

MFA et accès conditionnel

MFA obligatoire

Second facteur d'authentification sur tous les accès sensibles : VPN, cloud et postes d'administration.

Emplacements de confiance

Définition des réseaux et appareils autorisés pour un accès sécurisé.

Accès basé sur le risque

Renforcement de l'authentification selon le contexte – localisation, appareil, comportement.

Suivi des exceptions

Toute dérogation au MFA doit être documentée, approuvée et limitée dans le temps.

Gestion des accès privilégiés (PAM)

Séparation des comptes

Les administrateurs disposent d'un compte dédié distinct de leur compte standard – jamais de navigation web ou de messagerie avec un compte admin.

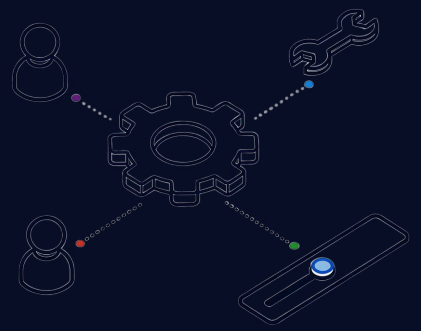
Surveillance renforcée

Toutes les actions privilégiées sont journalisées et auditables.

Moindre privilège

Droits d'administration accordés uniquement pour la durée et le périmètre nécessaires.

Comptes de service et exceptions techniques



Inventaire obligatoire

Chaque compte de service, compte break-glass ou contournement MFA doit être répertorié avec un propriétaire identifié.

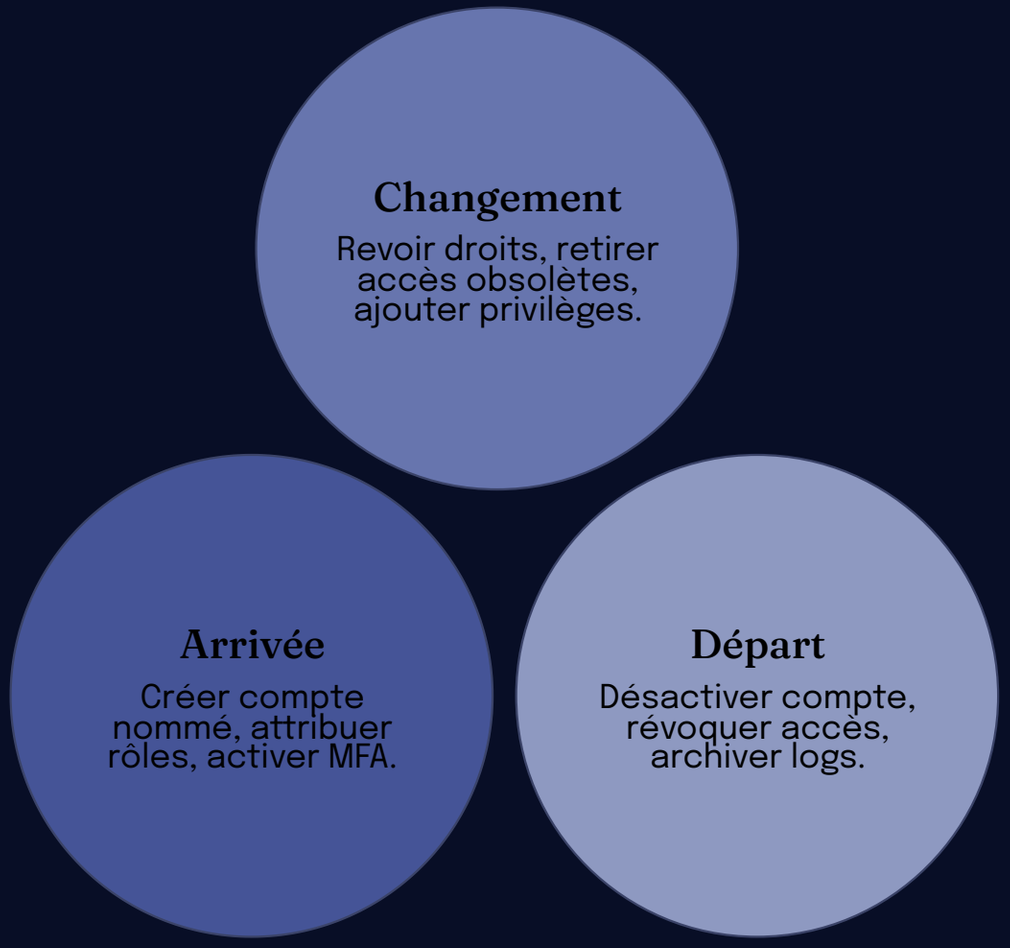
Justification et approbation

Toute exception technique doit être formellement justifiée et validée par le responsable sécurité.

Revue régulière

Ces comptes font l'objet d'une revue périodique pour vérifier leur pertinence et leur sécurisation.

Cycle de vie des accès



Une gestion rigoureuse du cycle de vie des accès garantit qu'aucun droit ne subsiste sans justification, de l'arrivée d'un collaborateur jusqu'à son départ.

Journalisation et preuves d'audit

Conservation des journaux

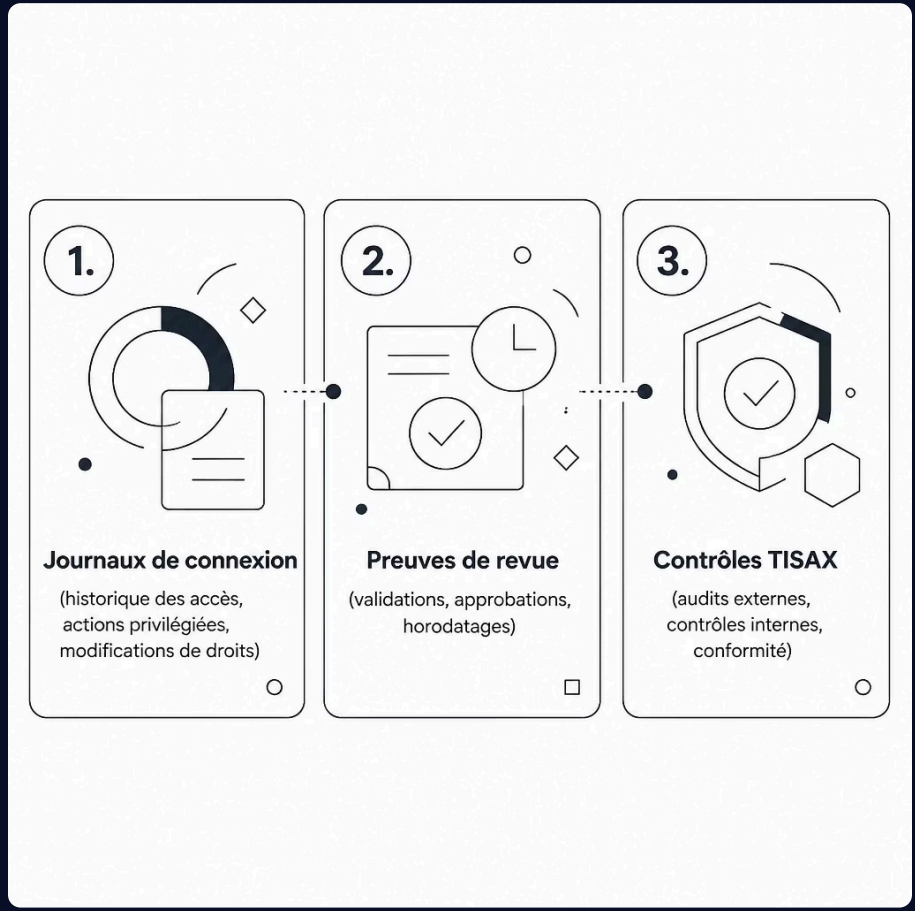
Historique des connexions, des actions privilégiées et des modifications de droits conservé selon la politique de rétention définie.

Preuves de revue

Validation des revues d'accès, approbations et décisions documentées et horodatées pour chaque cycle de contrôle.

Utilité pour les audits

Ces éléments constituent les preuves exigées lors des audits TISAX et des contrôles internes de sécurité.



Bonnes pratiques IAM

Comptes nominatifs exclusivement

Utiliser uniquement des comptes personnels et traçables, sans partage.

Moindre privilège systématique

Appliquer le principe du moindre privilège à chaque attribution de droits.

MFA sur tous les accès sensibles

Imposer le MFA sans exception sur VPN, cloud et systèmes critiques.

Revues régulières des droits

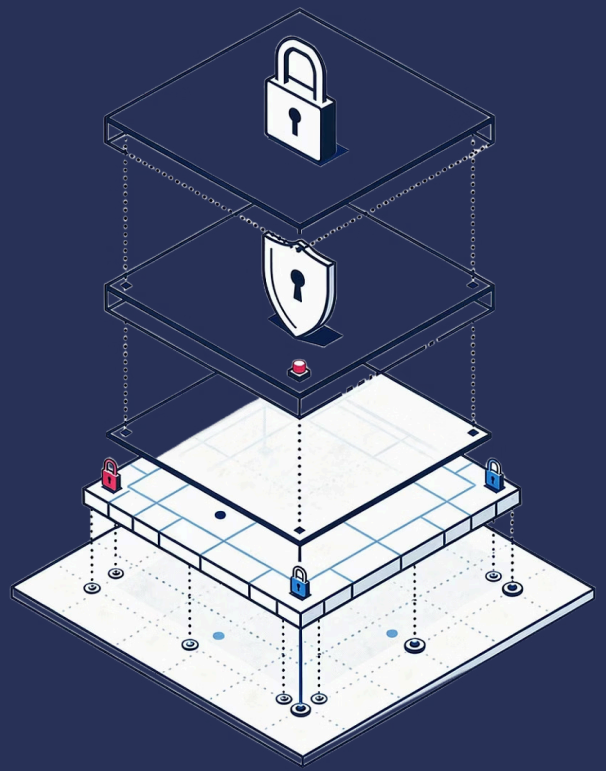
Valider périodiquement les accès et supprimer les droits obsolètes.

Désactivation immédiate

Désactiver immédiatement les comptes inactifs ou en départ.

Documentation des exceptions

Documenter et approuver formellement toutes les dérogations et surveiller les actions privilégiées.



L'IAM : fondation d'un SI sécurisé et auditable

Une base incontournable

Sans une gestion rigoureuse des identités et des accès, aucune stratégie de cybersécurité ne peut être pleinement efficace.

Sécurité, maîtrise, conformité

L'IAM protège les actifs critiques, garantit la traçabilité et démontre la maturité sécurité de l'organisation face aux audits TISAX.

Un engagement collectif

La réussite de l'IAM repose sur l'implication de tous – IT, management, métiers et cybersécurité.