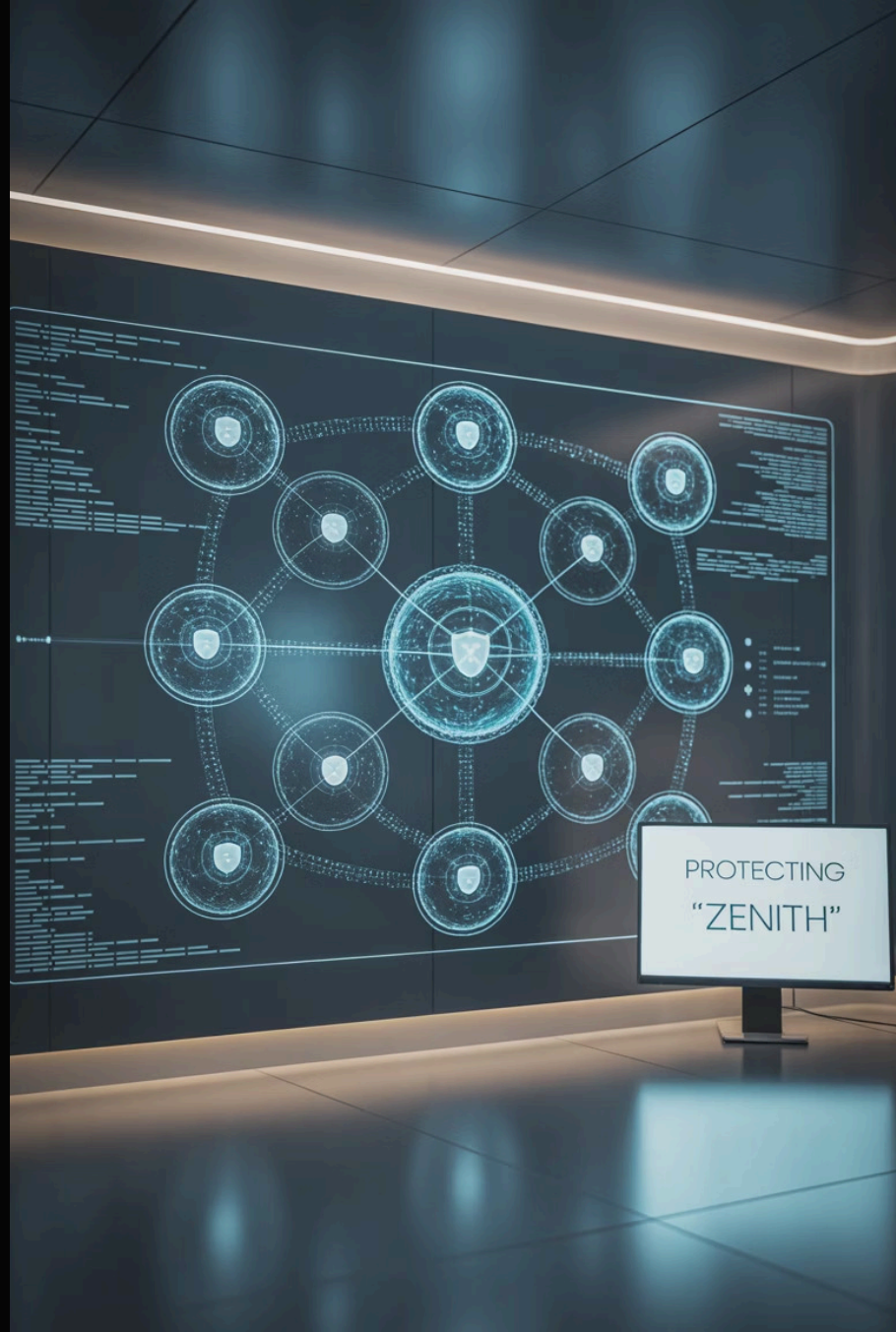
Les Diagrammes de Cas d'Utilisation en Cybersécurité

Une approche méthodologique essentielle pour l'analyse des risques et la spécification des besoins en sécurité informatique. Dans cette séquence pédagogique, nous découvrirons comment utiliser ces outils pour identifier et modéliser les interactions critiques entre utilisateurs et systèmes.

Par **David DONISA, Enseignant en BTS SIO**



Contexte : Introduction à l'UML

UML (Langage de Modélisation Unifié) est une notation standardisée essentielle pour visualiser et documenter les systèmes logiciels. Il existe divers types de diagrammes pour modéliser différents aspects d'un système.

Structurels

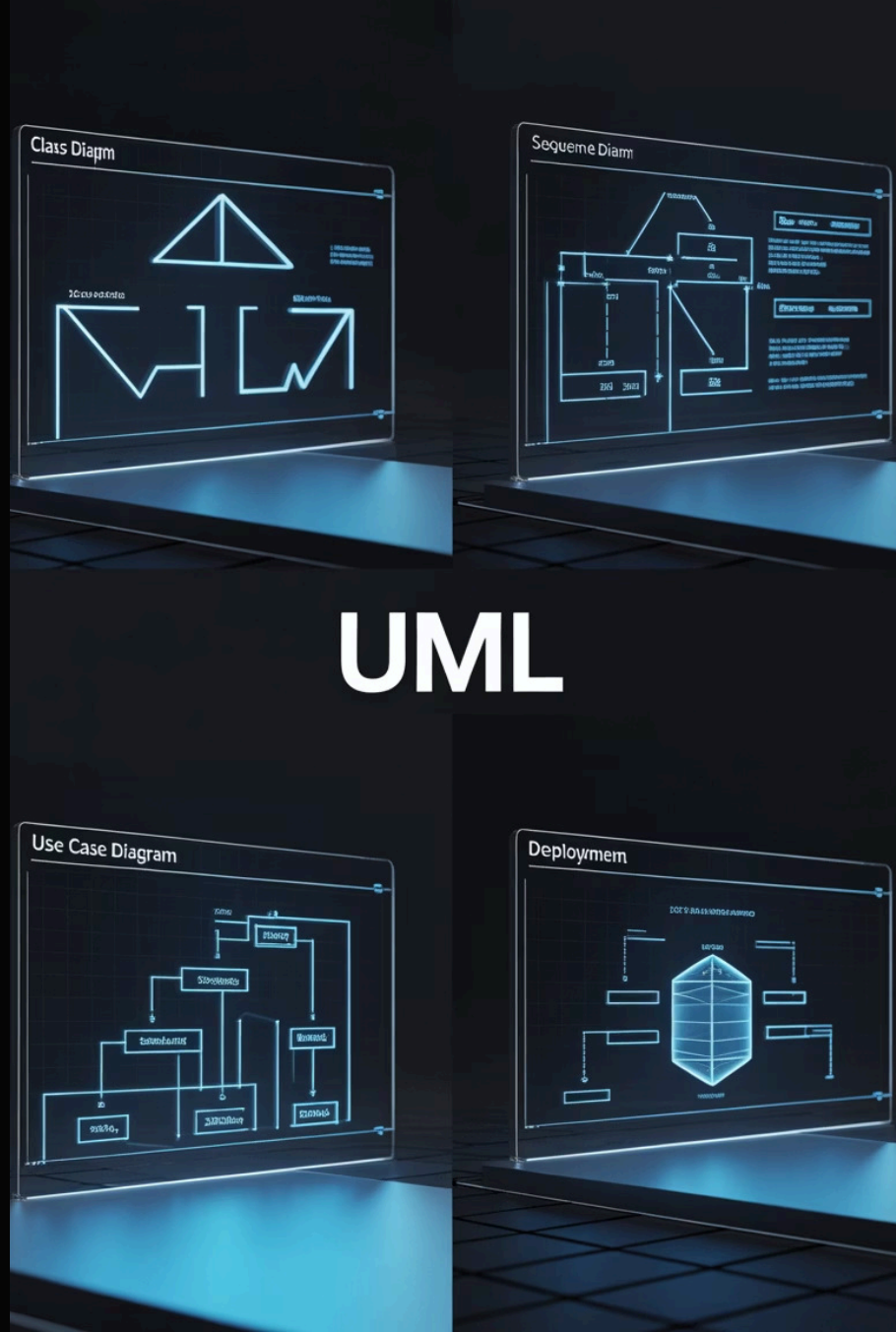
Décrivent l'architecture statique d'un système. Exemples : Classes, Composants, Déploiement.

Comportementaux

Modélisent les aspects dynamiques et fonctionnels. Exemples : Cas d'utilisation, Activité, Machine d'état.

D'Interaction

Illustrent les flux de contrôle et de données. Exemples : Séquence, Communication.



Qu'est-ce qu'un Cas d'Utilisation ?

Définition

Un cas d'utilisation décrit une **interaction spécifique** entre un utilisateur (acteur) et un système pour atteindre un objectif précis. Il constitue la base de l'analyse des besoins fonctionnels.

En cybersécurité, chaque cas d'utilisation représente un **point d'entrée potentiel** dans le système, nécessitant une évaluation des risques associés.

Exemples concrets

- Authentification utilisateur
- Accès aux données sensibles
- Sauvegarde automatique
- Gestion des permissions

Les différents scénarios associés à ces cas d'utilisation seront détaillés dans les cartes suivantes.

Importance en Analyse des Risques

Chaque scénario révèle des **vulnérabilités potentielles** qu'il faut identifier et traiter :

→ Identification des Points d'Attaque

Les cas d'utilisation exposent les interfaces et fonctionnalités accessibles aux utilisateurs, donc potentiellement exploitables par des attaquants.

→ Évaluation des Scénarios d'Exception

Ces scénarios révèlent comment le système réagit aux erreurs et aux tentatives d'intrusion, permettant d'identifier les failles de sécurité.

→ Planification des Contre-Mesures

Une fois les risques identifiés, il devient possible de définir les mécanismes de protection appropriés pour chaque cas d'utilisation.

Rôle dans l'Analyse des Besoins Client

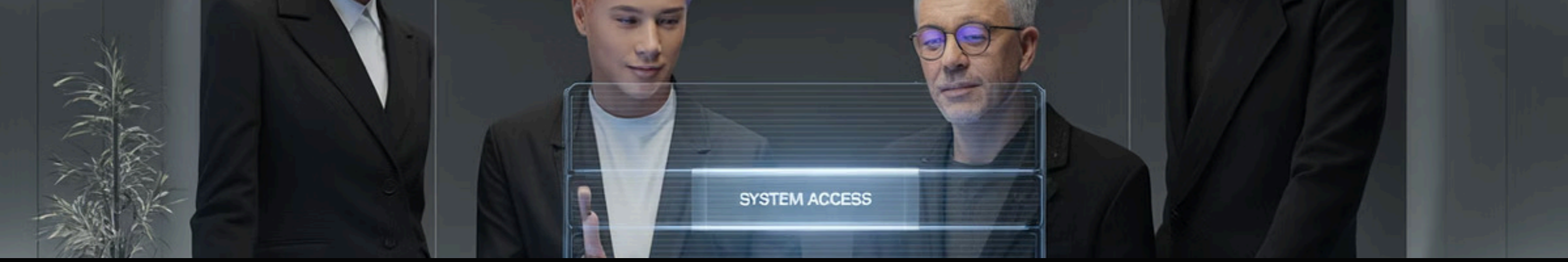
Les diagrammes de cas d'utilisation servent de **pont entre les besoins métier** du client et les spécifications techniques du système.

Communication

Ils permettent aux clients de visualiser concrètement les fonctionnalités et de valider que leurs besoins sont correctement compris.

Documentation

Ils constituent une base documentaire solide pour les phases de conception et de développement, garantissant la traçabilité des exigences.



Les Acteurs : Qui Utilise le Système ?

1

Acteurs Principaux

Utilisateurs qui **initient les cas d'utilisation** pour atteindre leurs objectifs métier.

Exemples : Employé, Client, Administrateur

2

Acteurs Secondaires

Systèmes ou services qui **participent aux cas d'utilisation** sans les initier.

Exemples : Base de données, Service d'authentification

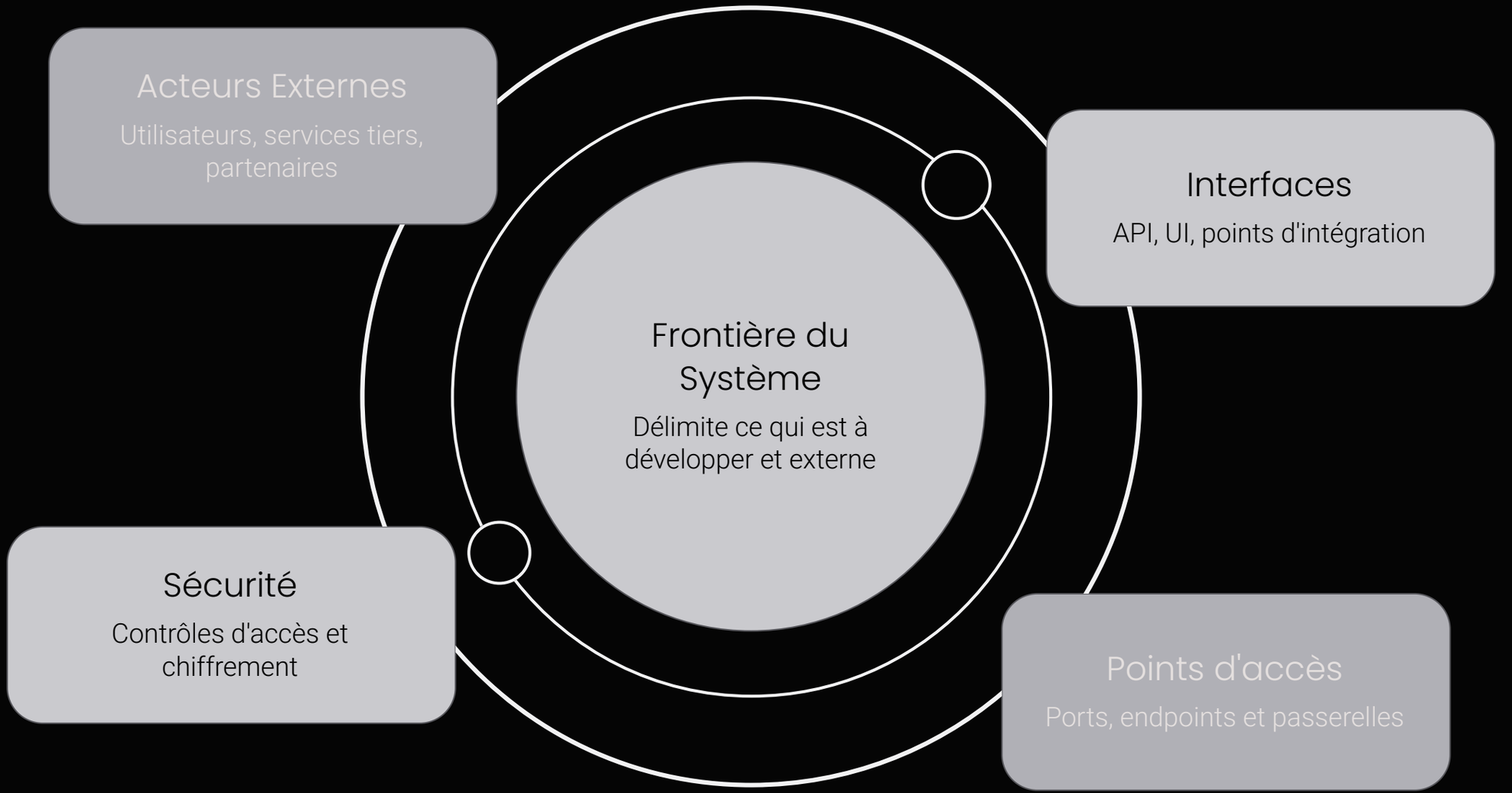
3

Regroupement d'Acteurs

Possibilité de **classifier les acteurs** ayant des rôles similaires pour simplifier la modélisation.

Exemple : "Utilisateurs internes" regroupant employés et managers

Systèmes et Frontières



Le **système** représente l'ensemble des fonctionnalités à développer. Sa frontière délimite ce qui est *à l'intérieur* (à développer) et ce qui est *à l'extérieur* (acteurs et systèmes existants).

En cybersécurité, cette délimitation est cruciale pour identifier les **périmètres de sécurité** et les points de contrôle nécessaires.

Relations entre Cas d'Utilisation

1

Lien d'Inclusion (<>)

"Nécessite obligatoirement de"

Un cas d'utilisation en inclut systématiquement un autre pour se réaliser.

Exemple : "Accéder au système" inclut obligatoirement "S'authentifier"

2

Lien d'Extension (<>)

"Nécessite éventuellement de (facultatif)"

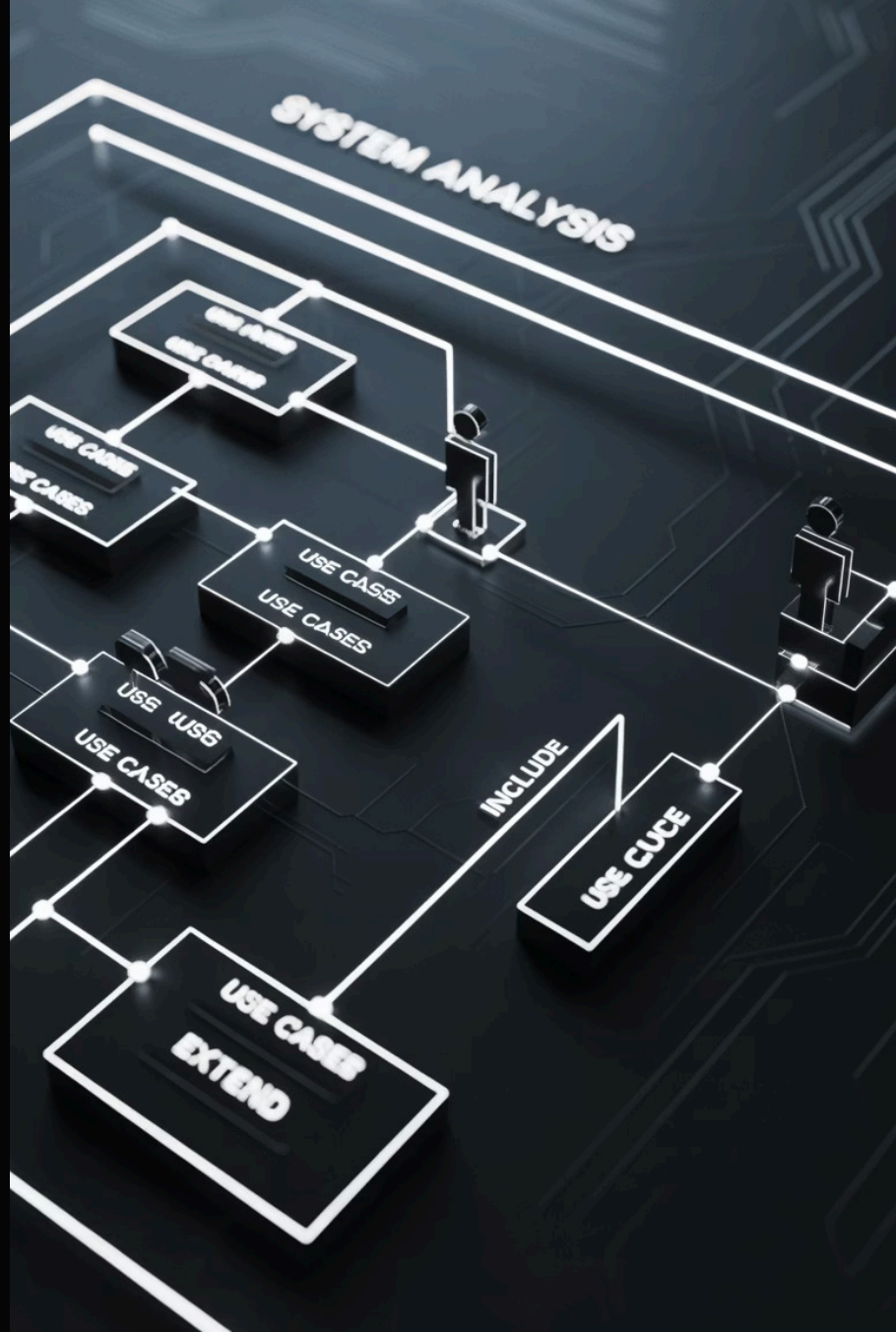
Un cas d'utilisation peut optionnellement en déclencher un autre selon certaines conditions.

Exemple : "Se connecter" peut étendre vers "Réinitialiser mot de passe" si oublié

Exemples Concrets de Diagrammes de Cas d'Utilisation

Pour illustrer la théorie, examinons quelques exemples pratiques de diagrammes de cas d'utilisation. Ces visualisations sont essentielles en cybersécurité pour identifier clairement les interactions utilisateurs/système et anticiper les vulnérabilités potentielles.

Passons maintenant à un exemple plus complexe, un système de planification des ressources d'entreprise (ERP), pour approfondir notre compréhension.



Exemple Détaillé : Se connecter au système

Le cas d'utilisation **"Se connecter au système"** est fondamental et illustre parfaitement la richesse des scénarios possibles ainsi que leur importance pour la sécurité.

Scénario Nominal : Connexion Réussie

L'utilisateur saisit son nom d'utilisateur et son mot de passe corrects. Le système vérifie les informations d'identification, accorde l'accès et redirige l'utilisateur vers son tableau de bord principal. C'est le parcours fluide et attendu.

Scénarios Alternatifs : Options Flexibles

- **Authentification à Deux Facteurs (2FA) :** Après avoir entré le mot de passe, l'utilisateur doit fournir un code de vérification supplémentaire envoyé par SMS ou via une application d'authentification.
- **Connexion Unique (SSO) :** L'utilisateur choisit de se connecter via un fournisseur d'identité tiers (ex: Google, Microsoft) sans saisir de nouvelles informations d'identification pour le système actuel.

Scénarios d'Exception : Gestion des Risques

- **Mot de passe incorrect :** L'utilisateur entre un mot de passe erroné. Le système affiche un message d'erreur et invite à réessayer. Après un nombre défini de tentatives infructueuses, le compte est temporairement verrouillé.
- **Compte bloqué :** Le système détecte une activité suspecte ou plusieurs échecs de connexion, bloquant l'accès et notifiant l'utilisateur/administrateur.
- **Tentative d'intrusion :** Une adresse IP suspecte ou un comportement anormal déclenche un blocage immédiat et une alerte aux équipes de sécurité.

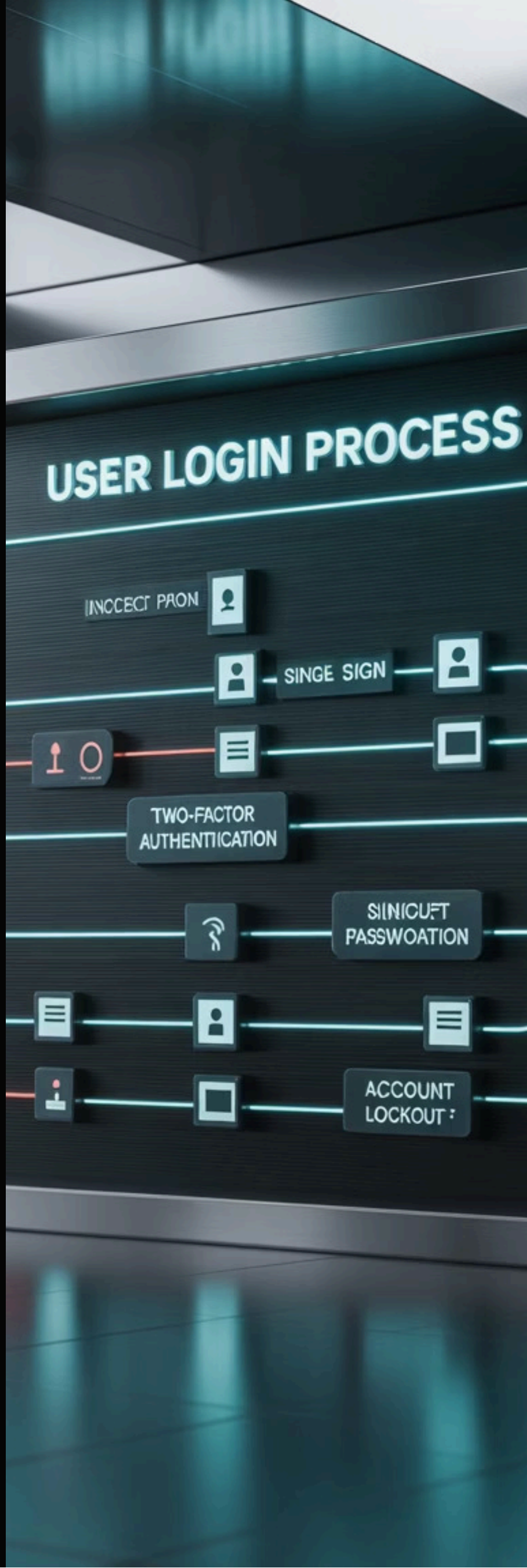
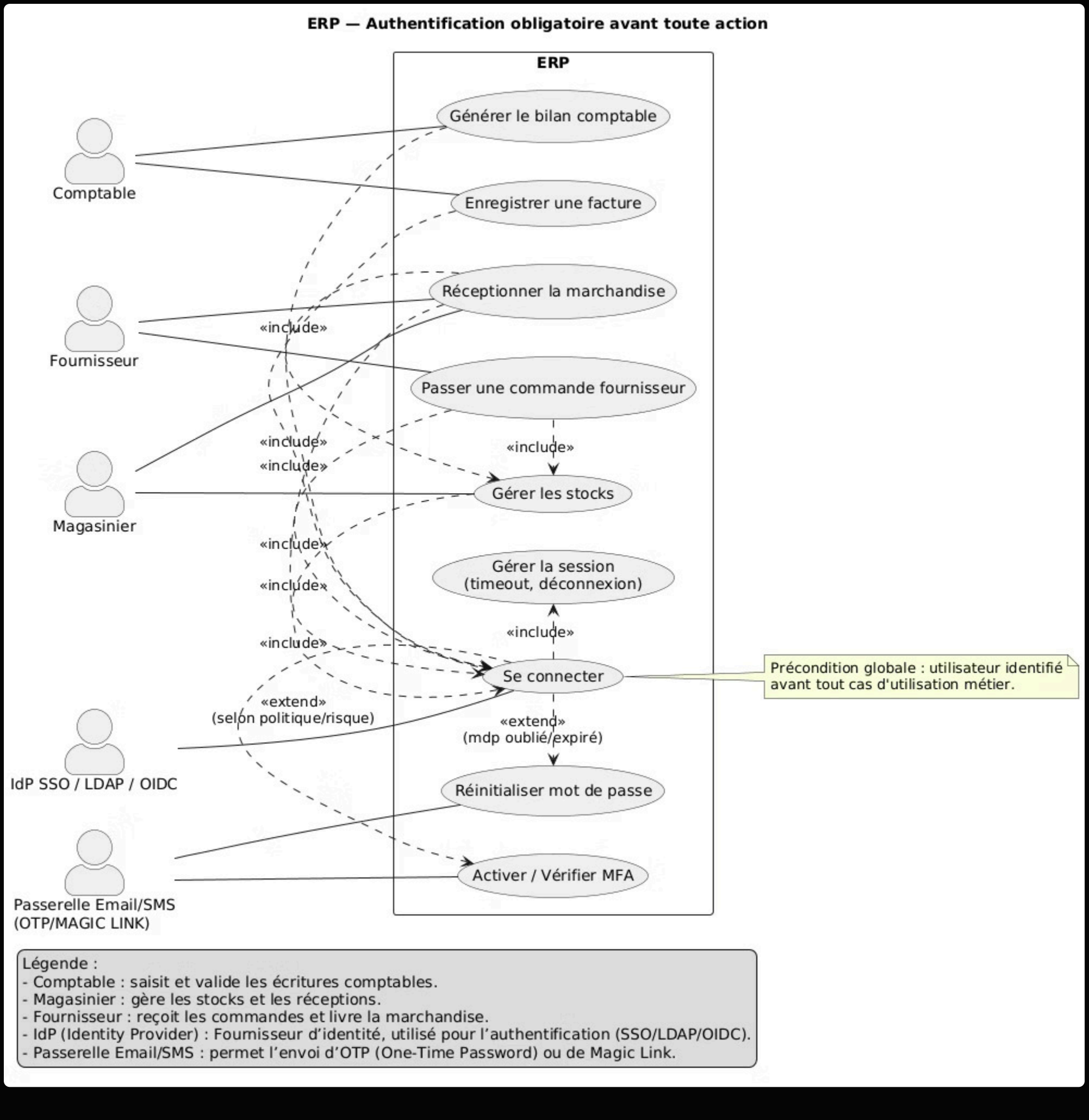


Diagramme de Cas d'Utilisation : Système ERP



Analyse du Système ERP

Ce diagramme illustre un système ERP (Enterprise Resource Planning) en action, mettant en lumière la complexité des interactions et la nécessité d'une modélisation précise pour anticiper les besoins fonctionnels et les enjeux de sécurité.

Il démontre comment les cas d'utilisation sont interdépendants et comment les relations <> et <> structurent le comportement du système.

Acteurs Clés

Nous identifions le **Comptable** pour les opérations financières, le **Fournisseur** pour la gestion des approvisionnements, et le **Magasinier** pour la gestion des stocks. Chaque acteur a des objectifs métier distincts et des accès spécifiques.

Cas d'Utilisation Principaux

Le cœur du système est représenté par des fonctionnalités comme "Gérer les Commandes", "Gérer le Stock", "Traiter les Factures" et "Générer les Rapports". Ces cas couvrent les processus métier essentiels d'une entreprise.

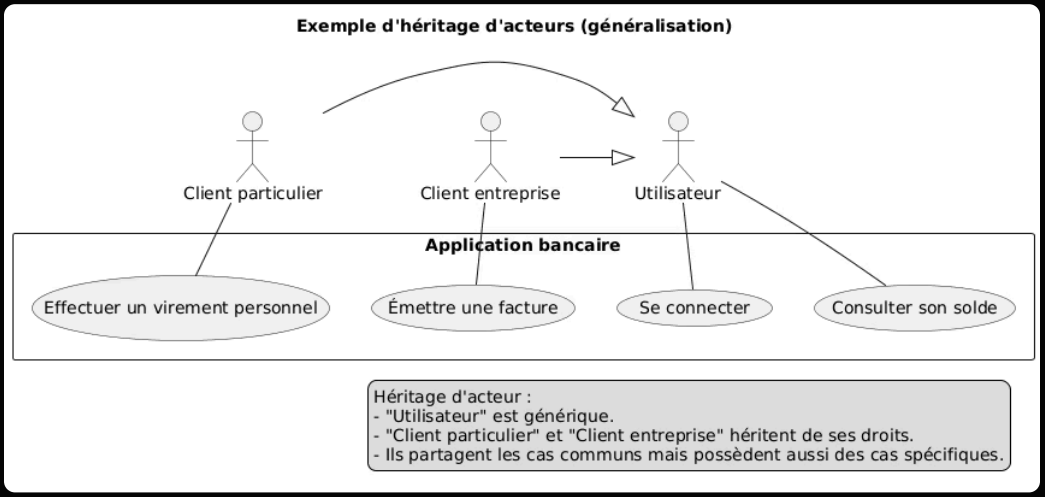
Relations Essentielles

Le lien **<<include>>** sur "S'authentifier" est crucial : chaque interaction sensible comme "Gérer les Commandes" nécessite une authentification préalable. La relation **<<extend>>** permet des scénarios optionnels comme "Notifier Retard" dans la gestion des commandes.

Sécurité par Conception

L'exigence d'authentification pour presque toutes les actions met en évidence l'importance de la sécurité. Cela garantit que seuls les utilisateurs autorisés peuvent effectuer des opérations et souligne la prévention des accès non autorisés et des manipulations frauduleuses.

Héritage et Généralisation



Héritage d'Acteurs

Un acteur **spécialisé hérite** des capacités d'un acteur plus général.

Exemple : "Administrateur système" hérite de "Utilisateur" avec des privilèges supplémentaires

Généralisation de Cas

Plusieurs cas d'utilisation spécifiques peuvent partager un **comportement commun** généralisé.

Exemple : "Sauvegarder fichier" et "Sauvegarder base" généralisent "Effectuer sauvegarde"

Cette approche facilite la **réutilisation** et la maintenance du code.

Synthèse et Applications Pratiques

Les diagrammes de cas d'utilisation constituent un **outil fondamental** pour l'analyse de sécurité des systèmes informatiques. Ils permettent de :

Identifier exhaustivement les interactions

Cartographier tous les points d'accès au système et les acteurs impliqués

Anticiper les scénarios de risque

Prévoir les cas d'exception et les tentatives d'intrusion potentielles

Concevoir une architecture sécurisée

Définir les mécanismes de protection adaptés à chaque cas d'utilisation

Prochaine étape : Nous appliquerons ces concepts à travers des exercices pratiques de modélisation sur des systèmes réels.