**SCENARIO**

GUY-LOUP MOREAU – SULLIVAN LEFEVRE

Problématique/Besoin :

Dans une entreprise IT, la gestion des systèmes informatiques et la sécurité sont essentielles. Il est crucial de garantir que chaque système est audité régulièrement, que les vulnérabilités découvertes sont rapidement identifiées et corrigées, et que les responsabilités des employés dans ces processus sont bien définies.

L'entreprise dispose de plusieurs départements, chacun responsable de la gestion de divers systèmes critiques (serveurs, bases de données, réseaux, etc.). Les audits de sécurité sont réalisés périodiquement pour évaluer l’état de ces systèmes, et les vulnérabilités détectées doivent être traçables et suivies jusqu'à leur résolution. Afin de structurer ces processus, une base de données est nécessaire pour centraliser les informations relatives aux employés, systèmes, audits, et vulnérabilités.

Description de la base de données et du schéma relationnel :

Le schéma relationnel de cette base de données comprend cinq tables principales :

Table EMPLOYEES :

id (PK) : Identifiant unique de l'employé.

last\_name : Nom de famille.

first\_name : Prénom.

position : Poste de l'employé (ex : administrateur système, ingénieur sécurité).

department\_id (FK) : Clé étrangère référant au département auquel l'employé est affecté.

Cette table stocke toutes les informations personnelles des employés. Chaque employé est une ressource essentielle pour gérer et exécuter les audits de sécurité dans l'entreprise.

Table SYSTEMS :

id (PK) : Identifiant unique du système.

name : Nom du système (ex : serveur, base de données).

type : Type de système (réseau, serveur, application).

department\_id (FK) : Clé étrangère vers le département responsable du système.

manager\_id (FK) : Clé étrangère vers l'employé responsable du système.

Cette table répertorie les systèmes informatiques de l'organisation. Ces systèmes sont des actifs critiques nécessitant un suivi et des audits réguliers pour garantir leur sécurité.

Table DEPARTMENT :

id (PK) : Identifiant unique du département.

manager\_id (FK) : Clé étrangère vers l'employé gérant le département.

type : Type de département (ex : IT, Ressources Humaines, Marketing).

status : Statut du département (actif/inactif).

location : Localisation du département.

Cette table décrit les différents départements de l'entreprise. Chaque département est responsable de certains systèmes et des employés qui les gèrent.

Table SECURITY\_AUDITS :

id (PK) : Identifiant unique de l'audit.

date : Date de l'audit.

status : Statut de l’audit (complet, en cours).

employee\_id (FK) : Clé étrangère vers l'employé qui a effectué l'audit.

system\_id (FK) : Clé étrangère vers le système audité.

Cette table enregistre tous les audits de sécurité réalisés. Chaque audit est documenté avec des informations comme la date, l’employé en charge, et le système audité.

Table VULNERABILITIES\_DETECTED :

id (PK) : Identifiant unique de la vulnérabilité.

audit\_id (FK) : Clé étrangère vers l’audit associé.

system\_id (FK) : Clé étrangère vers le système concerné.

severity : Gravité de la vulnérabilité (faible, moyenne, élevée).

status : Statut de la vulnérabilité (corrigée, en attente).

Cette table enregistre les vulnérabilités détectées lors des audits. Chaque vulnérabilité est associée à un audit spécifique et à un système, permettant de suivre les problèmes de sécurité et leur résolution.

Schéma relationnel et explication des relations entre les tables :

EMPLOYEES est lié à DEPARTMENT par department\_id : chaque employé appartient à un département spécifique. Cela permet de savoir quelles équipes sont responsables de la gestion des systèmes et des audits.

SYSTEMS est lié à DEPARTMENT par department\_id : chaque système est assigné à un département, indiquant quel département est responsable de sa gestion.

SYSTEMS est aussi lié à EMPLOYEES par manager\_id : chaque système a un employé qui en est responsable, facilitant la gestion des systèmes et des audits de sécurité.

SECURITY\_AUDITS est lié à EMPLOYEES par employee\_id : chaque audit est réalisé par un employé spécifique, assurant une traçabilité des audits effectués par qui et sur quel système.

SECURITY\_AUDITS est lié à SYSTEMS par system\_id : chaque audit est associé à un système spécifique. Cela garantit que chaque système critique fait l'objet de contrôles réguliers.

VULNERABILITIES\_DETECTED est lié à SECURITY\_AUDITS par audit\_id et à SYSTEMS par system\_id : chaque vulnérabilité détectée est associée à un audit spécifique et à un système particulier, permettant de suivre les vulnérabilités de manière détaillée et de gérer leur correction efficacement.