Sullivan Lefèvre – Guy-Loup Moreau

Le schéma relationnel de la base de données visualiser les relations entre les différentes tables et leurs colonnes. Ce document permet de présenter ainsi d’expliquer les relations entre ces dernières.

La table ‘EMPLOYEES’ contient toutes les informations personnelles des employés de l'entreprise, notamment leurs identifiants, noms, postes et coordonnées. Chaque employé est une ressource essentielle dans la gestion et l’exécution des audits de sécurité.

Dans la table ‘SYSTEMS’ sont répertoriés tous les systèmes informatiques de l'organisation. Ces systèmes, qu'ils soient des serveurs, des réseaux ou des bases de données, sont des actifs critiques qui nécessitent un suivi et des audits réguliers pour garantir leur sécurité.

La table ‘DEPARTMENT’ décrit les différents départements de l’entreprise, tels que l’IT, les Ressources Humaines ou le Marketing. Chaque département est responsable de certains systèmes et peut avoir des employés dédiés à leur gestion et à leur sécurité.

C’est dans la table ‘SECURITY\_AUDITS’ que sont enregistrés tous les audits de sécurité réalisés au sein de l'entreprise. Chaque audit est documenté avec des informations comme la date de l’audit, l’employé en charge, le système audité, et toute autre donnée pertinente liée à la vérification de la sécurité.

La table ‘VULNERABILITIES\_DETECTED’ enregistre lorsqu'un audit identifie une vulnérabilité, celle-ci est enregistrée dans cette table. Chaque vulnérabilité est liée à un audit spécifique et à un système précis, permettant de suivre les failles de sécurité détectées et leur résolution.

Nous observons de nombreuses relations entre les tables :

* Chaque employé est associé à un département, ce qui permet de définir quelles équipes sont responsables de quels systèmes et audits.
* Un système appartient à un département et peut être géré par un ou plusieurs employés, ce qui facilite la gestion des responsabilités en matière de sécurité.
* Les audits de sécurité sont réalisés par des employés sur des systèmes spécifiques, souvent dans le cadre des activités de leur département. Cela garantit un suivi précis des contrôles de sécurité, en tenant compte des équipes et des actifs audités.
* Lors d'un audit, si des failles sont découvertes, elles sont enregistrées comme des vulnérabilités spécifiques, liées à l'audit réalisé et au système concerné, permettant ainsi une traçabilité des problèmes et une gestion efficace des risques.