KEEPER

Fiche technique

Satisfaire facilement aux exigences de l'annexe A.9 de la norme ISO 27001 avec Keeper

ISO 27001 est une norme internationale pour la sécurité de l'information qui fournit un cadre et des lignes directrices pour l'établissement, la mise en œuvre et la gestion de systèmes de gestion de la sécurité de l'information. La norme ISO 27001 a été conçue pour aider les entreprises à protéger les ressources critiques et à se conformer aux exigences réglementaires nécessaires à leur secteur d'activité.

Dans le cadre de la mise en conformité avec la norme ISO 27001, les organisations sont tenues de limiter l'accès des employés aux seules informations pertinentes pour leur rôle, afin de réduire le risque que des données parviennent à des utilisateurs non autorisés et soient ainsi exposées.

En s'appuyant sur les solutions de cybersécurité de Keeper Security, les organisations de toutes tailles peuvent facilement et à moindre coût adhérer à l'annexe A.9 de la norme ISO 27001 et renforcer leur posture de sécurité.

Exigences	Solution
A.9.1.1 : Politique de contrôle d'accès	La politique de contrôle d'accès définit les règles et les procédures visant à garantir la sécurité des ressources informationnelles et à appliquer le principe du moindre privilège. Keeper assure le respect des contrôles d'accès basés sur les rôles (RBAC) définis par les administrateurs afin de garantir le moindre privilège dans l'ensemble de l'organisation. Le module ARAM (Advanced Reporting and Alerts Module) de Keeper fournit aux organisations des rapports clairs sur l'accès aux ressources à privilèges
A.9.2.1 : Enregistrement et désinscription des utilisateurs	Les organisations doivent s'assurer qu'il existe un processus formel régissant la manière dont les utilisateurs reçoivent l'accès, ainsi que la manière dont l'accès est révoqué pour les fichiers et les services de l'entreprise. Le RBAC de Keeper définit les politiques d'accès des utilisateurs au niveau des rôles et applique le principe du moindre privilège. Keeper dispose également d'un accès limité dans le temps, permettant aux utilisateurs de partager des enregistrements pendant une période déterminée, l'accès étant automatiquement révoqué à l'expiration de cette période. Associé à la rotation de mot de passe de Keeper Secrets Manager, les utilisateurs et les administrateurs peuvent s'assurer que le destinataire ne dispose jamais d'un accès permanent. Le déclassement des utilisateurs de la plateforme Keeper est simple. Les administrateurs peuvent rapidement et facilement supprimer les utilisateurs et transférer le contenu de leur coffre-fort à un membre approprié de l'équipe, assurant ainsi la continuité des opérations de l'entreprise.
A.9.2.2 : Fourniture d'accès aux utilisateurs	Un système, de préférence automatisé, est nécessaire pour attribuer et révoquer les droits dans l'ensemble de l'organisation. Keeper SSO Connect permet une gestion centralisée des accès, permettant aux équipes informatiques de surveiller et de contrôler l'accès des utilisateurs aux ressources autorisées. Cette approche simplifie la gestion des accès, améliore la visibilité et garantit la conformité des politiques de sécurité.
A.9.2.3 : Gestion des droits d'accès à privilèges	L'accès à privilèges accorde des droits aux administrateurs du système et aux personnes ayant accès à des informations sensibles. Les utilisateurs à privilèges sont souvent des administrateurs informatiques et de sécurité, des professionnels des ressources humaines, des cadres de haut niveau ou d'autres personnes qui ont besoin d'accéder à des systèmes à privilèges. La norme ISO 27001 exige un examen régulier des comptes d'administrateur et un registre de tous les droits à privilèges. Keeper fournit une gestion des mots de passe, des secrets et des connexions à privilèges à l'échelle de l'entreprise dans une plateforme unifiée. La solution de Keeper permet aux organisations d'obtenir une visibilité, une sécurité, un contrôle et des rapports complets sur chaque utilisateur à privilèges sur chaque appareil.

Anforderung	Lösung
A.9.2.4 : Gestion des informations secrètes d'authentification des utilisateurs	Les informations secrètes d'authentification doivent être fortement chiffrées et utiliser des mécanismes supplémentaires pour renforcer la sécurité. Ces systèmes doivent être gérés efficacement et rester confidentiels. Keeper Secrets Manager (KSM) est une plateforme Zero-Knowledge et cloud-based entièrement gérée pour sécuriser les secrets tels que les clés API, les mots de passe de base de données, les clés d'accès, les certificats et tout type de données confidentielles. KSM stocke tous les secrets et les identifiants dans Keeper Vault, avec un chiffrement au niveau de l'enregistrement pour le chiffrement le plus sûr disponible. Les administrateurs peuvent appliquer des mesures de sécurité supplémentaires, notamment l'authentification multifacteur (MFA) et la rotation des identifiants, afin de garantir que les secrets sont toujours protégés.
A.9.4.1 : Restriction de l'accès à l'information	Les politiques de contrôle d'accès doivent s'appliquer à tous les systèmes de l'entreprise et des mesures doivent être prises pour refléter les différents niveaux de restriction d'accès au sein de l'organisation. Keeper fournit les éléments suivants pour l'adhérence : • Contrôles d'accès basés sur les rôles • Partage granulaire pour appliquer des règles telles que la lecture seule ou le stockage obligatoire des identifiants dans un dossier partagé, ainsi que la possibilité de révoquer l'accès au partage et de limiter les utilisateurs au partage ou à la réception d'identifiants en interne • Contrôles d'accès à privilèges pour les informations et les données sensibles
A.9.4.2 : Procédures de connexion sécurisées	Les organisations devraient appliquer d'autres méthodes que les mots de passe pour sécuriser les procédures de connexion. Les tentatives réussies et échouées doivent être enregistrées. Keeper propose plusieurs options au-delà des mots de passe pour les méthodes de connexion. Keeper prend en charge une gamme de solutions MFA, stocke et remplit automatiquement les clés d'accès et aide les organisations qui utilisent des solutions d'authentification unique (SSO) à inclure l'accès à leurs coffre-forts par l'intermédiaire de leur fournisseur SSO, assurant ainsi un accès transparent et sécurisé. Keeper ARAM permet aux équipes de prendre en charge la conformité et l'audit avec plus de 200 types d'événements différents, y compris les tentatives de connexion réussies et échouées, avec des rapports personnalisés, des notifications en temps réel et l'intégration dans des solutions SIEM tierces.
A.9.4.3 : Solution de gestion des mots de passe	Les organisations devraient déployer un système de gestion des mots de passe pour générer et appliquer des mots de passe forts et pour faciliter les procédures de récupération. Keeper est le leader du secteur en matière de certification de sécurité et de conformité et chiffre au niveau de l'enregistrement, offrant ainsi la sécurité la plus robuste disponible dans le secteur. Chaque utilisateur de Keeper a un accès facile pour créer des mots de passe et des phrases secrètes pour tous les enregistrements, ce qui garantit que des mots de passe sécurisés sont utilisés. BreachWatch by Keeper permet de surveiller le Dark Web afin d'alerter les utilisateurs et les administrateurs lorsque des identifiants ont été exposés.
A.9.4.5 : Contrôle d'accès au code source des programmes	Le code source est constamment menacé par les cybercriminels qui tentent d'accéder aux systèmes de l'entreprise. Les organisations sont tenues de mettre en place un contrôle d'accès strict pour protéger ces systèmes. Keeper Secrets Manager sécurise votre environnement et élimine la prolifération des secrets en supprimant les identifiants hard-coded dans le code source, les fichiers de configuration et les systèmes CI/CD. Les utilisateurs et les administrateurs doivent stocker en toute sécurité tous les identifiants dans leur Keeper Vault afin d'éliminer la prolifération et de fournir des rapports et des alertes simples. Les utilisateurs de Keeper peuvent gérer un nombre illimité de secrets, d'applications et d'environnements.