Sécuriser vos données financières avec Kyriba

KYRIBA FACT SHEET

La fraude et les cyberattaques augmentant à la fois en fréquence et en sophistication, il est important de s'associer à Kyriba pour renforcer la sécurité de vos données stratégiques.

287

Nombre moyen de jours pour identifier et contrôler une fraude au sein des entreprises

– Ponemon Institute

40 %

des répondants révèlent avoir été confrontés à une attaque de leur Cloud au cours de l'année dernière

– Thales Data Threat Report, 2021

4,24 millions $

Coût moyen d'un vol de données en 2021

– Ponemon Institute

1,2 milliard $

d'amendes émises en 2021 pour non-conformité au RGPD

– DLA Piper Jan, 2021

Comment Kyriba vous accompagne

Fort d'une expérience de plus de 20 ans dans les solutions Cloud de trésorerie et de finance, notre approche globale et complète permettra à votre entreprise d'être en sécurité et d'accroitre le niveau de vigilance sur tous vos contrôles, vos données, et vos processus opérationnels.

Centre de cyberdéfense de Kyriba

Nos experts en sécurité du centre cyberdéfense de Kyriba fournissent une assistance mondiale, 24 heures sur 24 et 7 jours sur 7.

L'objectif du centre de cyberdéfense et de l'équipe de réponse aux incidents de sécurité (CSIRT) est de détecter et de réagir aux incidents de sécurité informatique, de déterminer leur portée et leur risque, de répondre de manière appropriée à l'incident, de communiquer les résultats et le risque à toutes les parties prenantes, et de réduire l'impact et la probabilité que l'incident se reproduise. Au cœur du CCD, Kyriba utilise Splunk comme système de gestion de l'information et des événements de sécurité (SIEM).

Renseignements sur les menaces

- Analyse du Dark Web à la recherche d'informations compromettantes et sensibles, notamment les adresses e-mail, les noms d'utilisateur et les mots de passe
- Renforcement contre les ransomwares, le vol d'informations d'identification, l'abus de marque et d'autres activités malveillantes tant cybernétiques que physiques
- Exploitation de sources industrielles qui fournissent des informations pertinentes sur les cybermenaces en temps réel

Prévention des pertes de données (DLP - Data Loss Prevention)

La DLP se concentre sur la détection et la prévention de la fuite, de la perte ou de l'utilisation abusive de données, que ce soit par le biais de brèches, d'exfiltration ou d'accès non autorisée. L'approche de Kyriba en matière de DLP représente un outil extrêmement efficace pour protéger les données de nos clients.

Protections contre les DDoS

Amazon Web Services (AWS) Shield vous protège contre les attaques DDoS qui sont des attaques par déni de service distribué et qui représentent une arme de cybersécurité visant à perturber le fonctionnement des services ou à extorquer de l'argent aux organisations ciblées. Les attaques DDos les plus courantes et les plus fréquentes se retrouvant au niveau de la couche réseau et de la couche de transport qui visent votre site Web ou vos applications.

Cryptage

Kyriba utilise le cryptage AWS pour toutes vos données stockées. Cela permet de crypter automatiquement toutes les données de blocs et de fichiers à l'aide d'un cryptage de 256 bits avant de les stocker sur des disques virtuels. Toutes les données sont également cryptées lorsqu'elles sont en transit.

Fonctionnalités et capacités de sécurité

La sécurité de Kyriba est riche en fonctionnalités et peut être utilisée pour renforcer votre cadre de contrôles financiers, et rendre les audits et le suivi de la sécurité plus simples et rapides.

Authentification unique (SSO)

L'authentification unique (SSO) permet à un utilisateur de se connecter en utilisant le nom d'utilisateur et le mot de passe qui lui ont été attribués par son entreprise. L'authentification unique s'appuie sur le standard SAML 2.0 pour l'authentification LDAP et les API Rest pour gérer les autorisations. Tous les contrôles de mots de passe sont gérés en interne par l'équipe IT et selon la politique de sécurité informatique de l'entreprise.

Authentification multifactorielle (MFA)

L'authentification multi facteurs est un outil efficace de prévention de la fraude lorsqu'il est utilisé seul ou, idéalement, en combinaison avec d'autres fonctionnalités de sécurité comme l'authentification unique ou le filtrage IP. L'authentification multi facteurs crée un mot de passe à usage unique et généré de façon aléatoire à l'aide du

smartphone de l'utilisateur, d'un jeton ou d'un certificat numérique SWIFT 3SKey.

Filtrage des adresses IP

Le filtrage d'adresses IP est une mesure de sécurité qui donne aux clients la possibilité de restreindre l'identification à une liste prédéfinie ou à des séries d'adresses IP paramétrées et conservées par l'administrateur de la sécurité du système. Lorsqu'il est utilisé seul, le filtrage IP constitue un outil de prévention de la fraude efficace.

Centre de contrôle Kyriba

Le maintien du contrôle des workflows de trésorerie est important pour la surveillance des erreurs, perturbations et activités suspectes. Le centre de contrôle Kyriba est en charge de la surveillance de l'ensemble de vos activités sur la plateforme de Kyriba. Il sert également à la détection précoce des utilisations non autorisées et des fraudes potentielles.

Réseau privé virtuel

Kyriba peut également mettre en place et administrer un réseau privé virtuel (VPN) pour chaque client, dans le but que les utilisateurs accèdent uniquement à Kyriba par le biais d'un réseau dédié géré par la société. Extended Security est habituellement utilisée avec le filtrage IP et l'authentification multi facteurs (MFA), afin de personnaliser le niveau de protection pour l'ensemble des utilisateurs de la plateforme.

Prise en charge des certificats 3SKey

Kyriba intègre les signatures numériques dans le cadre des fonctionnalités de sécurité standard. Des outils d'identité personnelle sont fournis, permettant à l'utilisateur de signer numériquement des messages et des documents, ainsi que d'approuver des transactions au sein du système. Kyriba prend en charge le format de signature numérique SWIFT 3SKey. Les signatures numériques peuvent être utilisées pour approuver et/ou authentifier les paiements envoyés à vos banques depuis Kyriba, mais aussi pour authentifier les paiements envoyés via des canaux non bancaires. Ce système peut aussi être utilisé comme une option d'authentification multi facteurs pour se connecter à l'application Kyriba.

Assurances, certifications et conformité

Qu'il s'agisse de tests anti-intrusion, de piratage éthique ou d'audits et de rapports relatifs aux normes du secteur, Kyriba s'assure de la conformité de son approche, grâce aux certifications de sécurité obtenues et ce, en lien avec les engagement contractuels pris avec ses clients. L'équipe Risque et Conformité de Kyriba renouvelle ces certifications annuellement :

- Certification ISO27001 du système de gestion de la sécurité de l'information (SGSI) de Kyriba
- Conformité SOC 1 et SOC 2 / Type I et II
- Certification SWIFT L2BA (fournisseur AL2)/ CSP AL2 et Conformité Service Bureau
- Test anti-intrusion / Piratage éthique
- Exercices Red Team fréquents avec une société de cyberdéfense de premier plan
- Engagement

Priorité à la confidentialité

Notre équipe chargée de la protection et de la confidentialité est tenue informée des lois et des tendances émergentes dans le monde entier, afin que vos organisations soient toujours en conformité.