sosafe

Sécurité et Confiance

L'approche de SoSafe en matière de sécurité

Index

Notre approche de la sécurité

Notre motivation en matière de sécurité 3
Notre équipe 3
Audits par des organismes indépendants 4

Sécurité des opérations internes

Gestion des accès 5
Principes généraux de gestion des accès 5
Sécurité de nos points de terminaison 6

Sécurité des tâches quotidiennes

Gestion des journaux 6
Continuité des activités et gestion de la reprise après sinistrey 7
Gestion des sauvegardes 7

Assurer la sécurité des données

Centres de données 8
Cryptage des données 8
Gestion des clés 8
Contrôle de l'accès aux données clients 8
Conservation et suppression des données 9

Personnel et sécurité

Formation de sensibilisation à la sécurité 10
Programme Champions de la sécurité 10

Protection contre les menaces

Tests de sécurité 10
Gestion des vulnérabilités 11
Réponse aux incidents 11
Programme Red team 11
Programme Purple team 11

Notre approche de la sécurité

Cette section aborde l'approche adoptée par SoSafe en matière de sécurité. Elle présente les principaux points et contrôles mis en place dans un certain nombre de domaines liés à la cybersécurité pour protéger à la fois nos environnements (y compris notre plateforme cloud) et nos processus, afin de créer les produits les plus sécurisés possibles pour nos clients et nos utilisateurs.

Notre motivation en matière de sécurité

La sécurité de l'information est pour nous une priorité absolue. Nous fournissons une solution de cybersécurité ; nous nous efforçons donc d'atteindre nous-mêmes un niveau irréprochable en matière de sécurité de l'information.

Plus nous nous développerons, plus notre produit sera utilisé et plus nous aurons besoin d'un dispositif de sécurité solide et à la pointe de la technologie.

Le succès de SoSafe GmbH dépend en particulier de ce que nos données, comme celles de nos clients, sont tenues à jour, protégées contre les altérations et traitées avec la confidentialité requise.

Notre équipe

Pour répondre à nos exigences en matière de sécurité, nous avons engagé des professionnels issus de différentes branches d'activité liées à la cybersécurité. Nous recherchons d'ailleurs sans cesse de nouveaux profils qualifiés pour développer, entretenir et optimiser la structure de SoSafe, afin de la maintenir toujours au plus haut niveau. Nous voulons être les meilleurs dans le domaine de la sécurité de l'information. C'est pourquoi notre équipe se compose des personnes suivantes :

- **RSSI (Responsable de la sécurité des systèmes d'information)** - Chef de l'équipe de sécurité de l'information, responsable du contrôle et du maintien de la sécurité chez SoSafe, il veille à la bonne collaboration entre tous les membres de l'équipe de sécurité de l'information.
- **Responsable de la sécurité de l'information** - Responsable de la conformité aux exigences ISO 27001, des certifications et de la mise à jour de notre système de gestion de sécurité informatique (SMSI) et de son bon fonctionnement.
- **Responsable du plan de continuité d'activités** - Chargé de veiller à ce que les objectifs et les exigences de la gestion de la continuité des activités soient respectés.
- **Sécurité des applications** - Responsable de la sécurité de nos produits et de nos plateformes.

- **Équipe SOC** - Responsable de la gestion des incidents, des tests de surveillance, de l'analyse prédictive des attaques et de la collecte de renseignements relatifs aux menaces.
- **Sécurité offensive** - Responsable des évaluations de la « 'red team », des tests de pénétration, de l'analyse prédictive des attaques et de la collecte de renseignements relatifs aux menaces.
- **Juridique** - Responsable de la conformité aux exigences légales et aux certifications.
- **Responsable conformité** - Chargé de veiller à ce que l'entreprise, ses employés et ses projets respectent toutes les réglementations et les spécifications applicables.
- **Délégué à la protection des données** - Responsable de la conformité au RGPD pour toutes les activités de traitement des données personnelles effectuées par SoSafe.

En plus de notre équipe spécialisée, tous les employés de SoSafe suivent notre formation en ligne sur la sécurité informatique, afin de disposer de toutes les connaissances requises pour répondre à nos exigences en la matière.

Audits par des organismes indépendants

ISO-27001

Notre société a passé avec succès l'audit ISO 27001 et est donc certifiée ISO 27000 depuis le 20 décembre 2022. Notre objectif est de nous soumettre fréquemment à des audits menés par des organismes indépendants, dont les pratiques sont elles-mêmes garanties par des évaluations SOC1, SOC2, et/ou ISO/CEI 27001 régulières.

Télécharger le certificat ISO →

TISAX

Chez SoSafe, nous savons à quel point il est important de préserver la confidentialité, la disponibilité et l'intégrité des informations. Afin de garantir le plus haut niveau de sécurité de l'information, nous participons à la norme TISAX (Trusted Information Security Assessment Exchange) pilotée par l'association ENX pour le compte de la fédération allemande de l'industrie automobile (VDA).

Les évaluations TISAX sont menées par des prestataires de services d'audits agréés soumis à des contrôles réguliers de qualification. Veuillez noter que la procédure d'évaluation TISAX et ses résultats ne sont pas destinés au grand public. Pour consulter les résultats de notre évaluation en exclusivité, connectez-vous sur le portail ENX : https://enx.com/TISAX/tisaxassessmentresults, avec les identifiants suivants : Assessment ID ACMGNV et Scope ID S02C8M.

Sécurité des opérations internes

Pour être efficace, notre approche de la cybersécurité doit commencer par nos environnements internes. Elle se base sur les principes suivants :

Gestion des accès

Le terme « accès » désigne ici l'utilisation des systèmes informatiques, de leurs composants et des réseaux, ainsi que l'exploitation des informations.

Principes généraux de gestion des accès

- **Principe du besoin d'en connaître**
  Les employés de SoSafe ne se voient accorder que les droits ou privilèges absolument nécessaires à l'accomplissement de leurs tâches. Par conséquent, tout octroi de privilèges administratifs est restreint et doit être justifié.

- **Principe du moindre privilège**
  Les utilisateurs ne se voient accorder que les droits et privilèges absolument nécessaires à la réalisation de leurs tâches.

- **Séparation des tâches et principe du double contrôle**
  Lors de l'octroi de droits d'utilisation, il est impératif de respecter les principes de séparation des tâches et/ou de double contrôle en cas de conflit de fonctions.

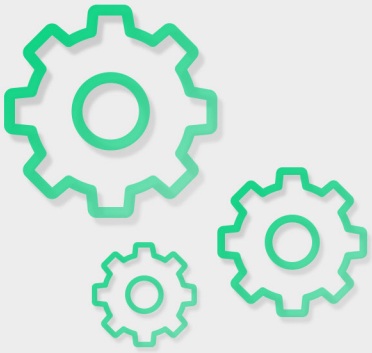
- **Administration des utilisateurs**
  L'administration des utilisateurs, groupes et autorisations est centralisée à l'aide de technologies de type SSO pour limiter au maximum le nombre de répertoires d'utilisateurs nécessitant une maintenance.

- **Octroi, ajustement et retrait des droits**
  La modification des droits d'accès se fait selon le principe des quatre yeux. Tout octroi de droit utilisateur en dehors du processus classique d'autorisation doit être documenté. Nous imposons aussi la double approbation pour les accès administratifs : cela signifie que toute demande d'accès doit être approuvée à la fois par le propriétaire de l'actif et par un supérieur hiérarchique.

  Tous les droits d'accès sont également vérifiés au moins une fois par an. Conformément à notre politique de gestion des accès, les accès administratifs sont contrôlés au moins tous les six mois ou en cas de modification significative d'un actif.

  Dans le cadre du principe du besoin d'en connaître et de la politique de moindre privilège, les comptes inactifs sont bloqués ou supprimés.

  Enfin, tous les droits d'accès sont révoqués dans les 24 heures suivant le départ d'un employé.



- **Accès au code source**
  L'accès au code source ou au référentiel est limité pour empêcher l'accès des personnes non autorisées et les risques de divulgation des secrets d'affaires. Les principes du besoin d'en connaître et de moindre privilège doivent être respectés autant que possible. Nous sommes particulièrement prudents avec les employés temporaires, tels que les étudiants, stagiaires ou développeurs externes.

- **Exigences en matière d'authentification**
  Un compte est verrouillé après six tentatives de connexion infructueuses. L'accès à distance à partir de réseaux externes publics ne peut se faire qu'en utilisant le VPN de l'entreprise, lequel crypte les informations en transit et requiert une authentification 2FA.

Sécurité de nos points de terminaison

ATous nos périphériques, ainsi que nos plateformes de stockage et de partage des fichiers, sont dotés d'une sécurité spécifique.

Les employés de SoSafe travaillent sur des appareils mobiles appartenant à l'entreprise (équipés d'un antivirus adapté) afin de protéger au maximum les actifs de la société. Nous utilisons, à cet effet, un logiciel de gestion des appareils mobiles qui ne peut pas être désactivé par les utilisateurs.

Pour garantir le même niveau de sécurité avec les collaborateurs externes, nous leur fournissons des appareils mobiles en fonction de leurs responsabilités et de leurs besoins en matière d'accès. Il peut, par exemple, s'agir de machines virtuelles ou d'appareils mobiles entièrement gérés par SoSafe.

Tous les employés sont formés à l'utilisation conforme de ces appareils mobiles.

Sécurité des tâches quotidiennes

Gestion des journaux

- **Activités de journalisation obligatoires**
  Tous les hôtes et les équipements du réseau génèrent des journaux de sécurité pour tous les composants du système.

  Tous les hôtes et les équipements du réseau émettent des alertes en cas d'échec du traitement des journaux de sécurité, par exemple en cas d'erreur logicielle ou matérielle, de défaillance des mécanismes de géné ration des journaux, ou de dépassement des capacités de stockage. Toutes les alertes doivent se faire en temps réel si possible.

- **Journalisation centralisée**
  Les événements liés à la sécurité sont transférés vers un service de journalisation en temps réel (ou aussi rapidement que la technologie le permet). Pour préserver l'intégrité des journaux de l'infrastructure consolidée, ceux-ci sont, par exemple, sauvegardés en lecture seule.

→ **Activités de surveillance obligatoires**
Nous développons et exploitons des processus (tels que notre système SIEM, par exemple) qui contrôlent les journaux de tous les systèmes afin d'identifier toute éventuelle anomalie ou activité suspecte. Nous avons recours à des études de référence et à des outils de surveillance automatisés pour générer des alertes lorsque des exceptions sont détectées.

→ **Personnel autorisé**
Par mesure de sécurité, l'accès aux journaux est accordé uniquement aux personnes qui en ont réellement besoin dans le cadre de leurs fonctions et les fichiers sont protégés contre les modifications non autorisées suivant le principe du besoin d'en connaître. L'historique des accès aux systèmes de gestion des journaux est également sauvegardé.

→ **Conformité**
Les données sont enregistrées de manière sécurisée dans le respect des prescriptions en matière de conservation des journaux, ainsi que des exigences commerciales, légales et réglementaires (p. ex. : RGPD, loi fédérale allemande sur la protection des données (Bundesdatenschutzgesetz)).

Tout journal contenant des informations personnelles identifiables doit être approuvé par notre DPD.

→ **Conservation**
Les fichiers journaux créés dans le cadre de la surveillance décrite dans le présent document sont conservés pendant au moins 90 jours et restent accessibles durant cette période.

Continuité des activités et gestion de la reprise après sinistre

Nous avons mis en place un plan de gestion de la continuité des activités. Ce plan est décrit dans une politique de gestion de la continuité des activités et se fonde sur la norme ISO 22301:2019 Gestion de la continuité des activités.

Gestion des sauvegardes

Nous appliquons un plan de sauvegarde complet pour tous nos actifs, avec des politiques de sauvegarde et des exigences spécifiques pour chacun d'entre eux.

Nous avons également défini des exigences spécifiques pour nos bases de données contenant des données clients.

Calendrier
La base de données est sauvegardée toutes les nuits dans son intégralité et fait l'objet d'enregistrements continus par flux WAL (Write-Ahead Logging).

Objectifs en matière de temps de récupération

- Une récupération complète (en cas de crash de la base de données) nécessiterait entre 1h et 1h30, selon la taille du WAL.
- En cas de perte partielle de données, nous pouvons générer une copie entièrement fonctionnelle de la production en 1 heure et récupérer les données nécessaires.

Assurer la sécurité des données

Centres de données

SoSafe héberge ses données et celles de ses clients dans plusieurs centres de données du même fournisseur, un centre de données certifié ISO 27001 avec un niveau de sécurité physique très élevé. Les risques en matière de sécurité physique sont très limités, car notre entreprise se base sur l'informatique dématérialisée. De plus, le centre de données applique de nombreuses mesures de sécurité pour protéger les données des clients selon les normes les plus strictes.

Cryptage des données

Toutes les données clients exploitées par nos produits sont cryptées lors de leur transit sur des réseaux publics, en utilisant au minimum TLS 1.2 pour les protéger de toute divulgation ou modification non autorisée. Notre implémentation de TLS impose l'utilisation de codes de chiffrement puissants lorsque le navigateur le permet. Tous nos systèmes et lecteurs de données contenant des informations clients utilisent le cryptage « full-disk AES encryption at rest », conformément aux normes du secteur, et suivent les directives du BSI (Office fédéral allemand pour la sécurité de l'information) lors de la sélection des procédures cryptographiques, des algorithmes et de la longueur des clés.

Gestion des clés

SoSafe a recours aux technologies de pointe pour générer, stocker, archiver, récupérer, distribuer, prélever et supprimer les clés en toute sécurité, conformément aux recommandations du National Institute of Standards and Technology (NIST) américain.

Les clés privées sont stockées dans un gestionnaire de mots de passe qui interdit tout accès non autorisé.

Contrôle de l'accès aux données clients

Bien que nous traitions toutes les données client comme hautement confidentielles et que nous ayons mis en place des contrôles stricts à cet effet, nous n'exigeons pas des clients qu'ils nous fournissent certaines catégories spéciales de données à caractère personnel. Chez SoSafe, seuls certains employés autorisés ont accès aux données client stockées dans nos systèmes. L'accès complet n'est accordé qu'à quelques groupes bénéficiant de privilèges correspondants, à moins d'une demande spécifique ayant fait l'objet d'un examen spécial avant validation (demandes d'accès aux données par les clients, avec

authentification 2FA supplémentaire, par exemple). Tout accès non autorisé ou inapproprié aux données clients déclenche notre processus de gestion des incidents de sécurité qui inclut l'obligation de notifier les clients concernés en cas de violation de la politique.

Conservation et suppression des données

→ **Données clients**
Seules les données principales des clients (dans la mesure où elles sont considérées comme des données à caractère personnel) sont conservées pendant 10 ans conformément à l'article 147 du code fiscal allemand et à l'article 257 du code du commerce allemand.

L'archivage des données clients se fait trois mois après l'expiration des licences (dans le but de garantir la qualité des données pour les licences ultérieures). Ce délai peut être prolongé ou raccourci à la demande du client.

Quatre semaines avant l'archivage, nous envoyons un rappel à notre interlocuteur agréé chez le client pour lui permettre de télécharger les rapports/certificats.

SoSafe conserve une preuve de destruction, conformément à la norme ISO 27001 relative à la suppression et à l'élimination des données. Celle-ci stipule, en effet, que tout support de stockage doit faire l'objet d'un contrôle avant sa mise au rebut ou sa réutilisation afin de garantir que toutes les données confidentielles et tous les logiciels sous licence ont bien été supprimés ou écrasés de manière sécurisée.

Lorsque des données clients sont effacées du logiciel de gestion SoSafe, un rapport précisant la date et la nature de la suppression est généré. Ce rapport de suppression est conservé et peut être présenté au client sur demande.

→ **Données des employés du client**
Un client peut à tout moment supprimer tout ou partie des données relatives à l'un de ses employés, depuis le panneau de contrôle. L'accès de l'utilisateur à nos formations en ligne sera désactivé à la fin de la période de licence.

Les données personnelles des participants à une simulation de phishing ou à une campagne de formation en ligne sont automatiquement supprimées de la base de données utilisateurs lorsque le client est archivé (trois mois après l'expiration de la licence).

Si nécessaire, les données peuvent être récupérées jusqu'à 28 jours après suppression à partir de sauvegardes.

→ **Active Directory**
Si des utilisateurs sont désactivés par le client dans Active Directory (AD) ou perdent le droit d'utiliser l'application de formation en ligne SoSafe, ils seront également désactivés sur la plateforme SoSafe. Ils ne pourront donc plus se connecter et ne seront plus pris en compte pour les cam-

pagnes de phishing. Si les utilisateurs sont réactivés dans AD ou que leurs droits d'utiliser l'application de formation en ligne SoSafe sont restaurés dans les 30 jours, leur accès sera réactivé et ils pourront reprendre là où ils s'étaient arrêtés.

Au bout de 30 jours, les utilisateurs désactivés, ainsi que leurs données de progression, sont supprimés. Si un utilisateur est ensuite réactivé dans AD, un nouveau profil utilisateur sera créé sur la plateforme SoSafe, et l'utilisateur n'aura pas accès à ses données antérieures.

Personnel et sécurité

Formation de sensibilisation à la sécurité

Nous veillons à ce que tous les employés de SoSafe reçoivent une formation de sensibilisation à la sécurité durant leur période d'intégration, puis tout au long de leur contrat de travail. La sécurité reste ainsi une priorité pour tous les membres de nos équipes. La formation de nos employés est complétée par des simulations de phishing régulières qui les sensibilisent et les préparent aux menaces réelles. Notre programme de sensibilisation à la sécurité aborde, entre autres thématiques, les menaces et les escroqueries, la sécurité des processus de travail, les comportements à risque, ainsi que les questions relatives à la conformité et à la réglementation.

Programme Champions de la sécurité

Notre programme Champions de la sécurité vise à renforcer la culture de la cybersécurité au sein de SoSafe pour renforcer la sensibilisation, mais aussi pour accélérer et améliorer le développement et la mise sur le marché de nos produits sur le plan de la sécurité.

Notre programme cible principalement les départements de développement des produits et d'ingénierie où les « champions de la sécurité » veillent au respect de nos objectifs de sécurité et à l'application rigoureuse des contrôles de sécurité lors du développement des logiciels.

Protection contre les menaces

Tests de sécurité

Les tests de sécurité constituent un aspect essentiel du cycle de développement. Ils sont réalisés durant l'implémentation et pendant la phase de test du Secure Development Life Cycle (SDLC).

Au cours de la phase d'implémentation, nous procédons à des tests de sécurité à l'aide de nos outils et suivant une approche « shift-left ». L'objectif est de s'assurer que le code écrit par les développeurs est sécurisé. De plus, toutes les bibliothèques open-source externes utilisées avec notre produit font l'objet de contrôles stricts et réguliers.

Au cours de la phase de test, les tests de sécurité sont assurés par les ingénieurs en sécurité des applications. Toutes les fonctionnalités importantes sont également testées de manière dynamique.

Gestion des vulnérabilités

→ **Analyse des vulnérabilités**
Notre plateforme fait l'objet d'une surveillance continue qui assure l'analyse automatique des vulnérabilités et la prise en charge immédiate des vulnérabilités repérées.

→ **Analyse des bibliothèques open-source externes**
Les bibliothèques open-source externes que nous utilisons sont continuellement analysées par notre Software Composition Analysis (SCA). Toute vulnérabilité repérée est signalée à l'équipe correspondante pour correction. Les bibliothèques sont corrigées conformément aux accords SLA définis en fonction de la gravité des vulnérabilités.

Réponse aux incidents

→ **Test de réponse aux incidents de sécurité**
Pour pouvoir réagir efficacement en cas d'attaque réelle, toutes les parties prenantes doivent savoir à l'avance comment réagir. À cet effet, il est indispensable de simuler fréquemment ce type d'incident de sécurité et d'apprendre à y faire face.

Programme Red team

Nous avons récemment créé une Red team (équipe dédiée à la sécurité offensive), intégrée à l'équipe de sécurité, afin de renforcer notre approche de la sécurité par des tests plus poussés sur les protections, les procédures et les réponses. Nous suivons ainsi l'évolution des nouvelles stratégies et techniques de nos adversaires, et veillons à nous protéger contre tout nouveau type de menace.

La Red team soutient l'équipe de sécurité de différentes manières : tests de pénétration, exercices et simulation d'attaques avancées.

Programme Purple team

L'une des valeurs fondamentales de notre équipe de sécurité, c'est la collaboration. Nous voulons nous assurer que nous disposons de contrôles de sécurité bien définis et configurés, et que nous sommes capables de détecter et de répondre à tout éventuel incident de sécurité. Pour ce faire, nous avons instauré un circuit continu de communication permettant à l'équipe SOC et à la Red team d'échanger leurs commentaires et leurs retours. Nous réalisons également des évaluations dédiées à la Purple team en y incluant tous les participants concernés.