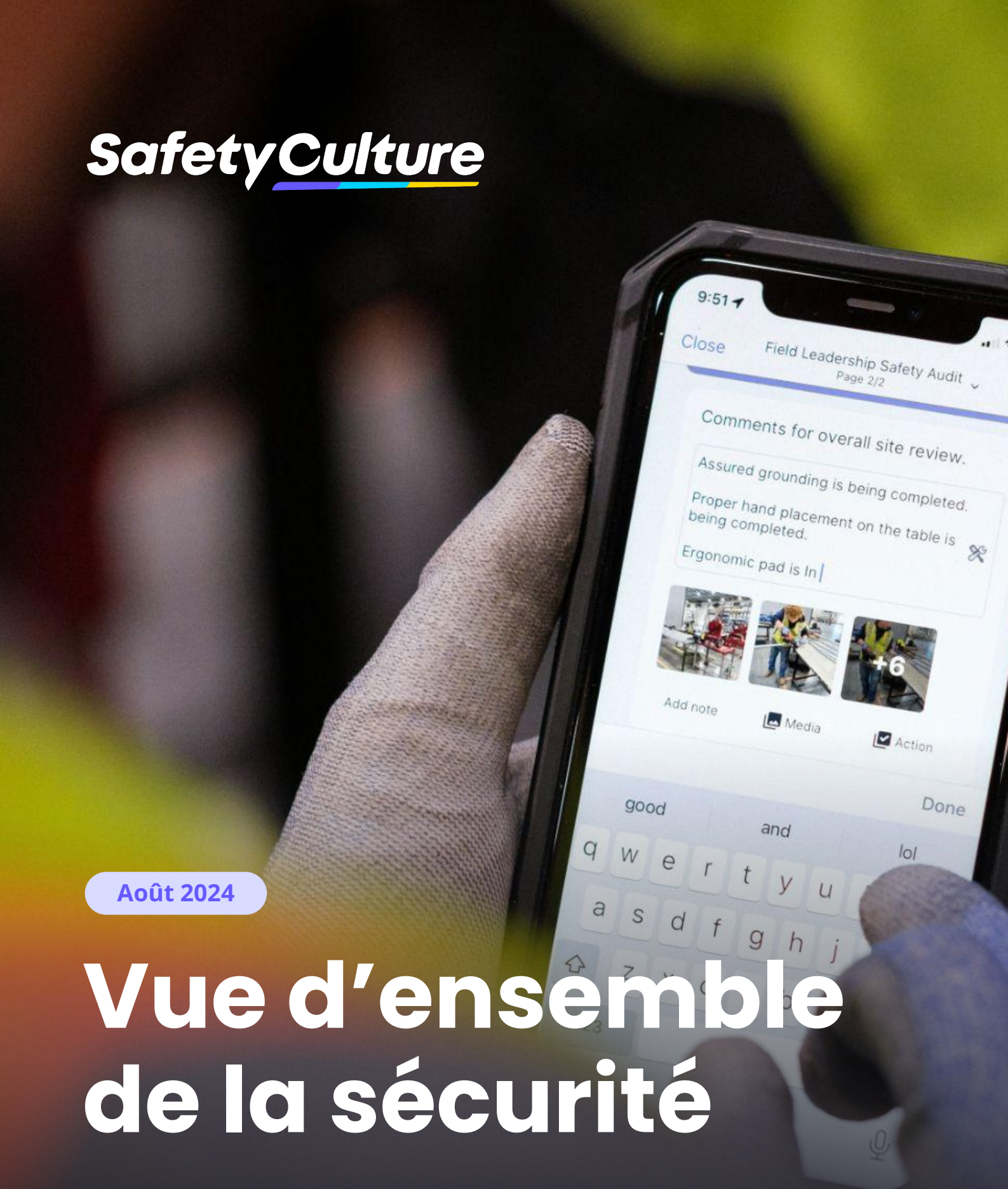
SafetyCulture



Août 2024

Vue d'ensemble de la sécurité

Comprendre la cybersécurité de SafetyCulture

Table des matières

Introduction 4

Vue d'ensemble de la cybersécurité 5

Pratiques de sécurité organisationnelles 6

Gouvernance de la sécurité
Contrôles d'accès
Sécurité des tiers
Sécurité des réseaux
Journal d'évènements et suivi
Formation de sensibilisation à la sécurité
Correctifs et gestion des vulnérabilités

Protection des données des clients 9

Restriction de l'accès aux données
Accès physique aux données
Cryptage des données
Suppression et élimination des données
Sauvegarde des données

Sécurisation de nos produits 11

Logiciel sécurisé - Pratiques de développement
Contrôle des modifications
Identification des vulnérabilités et développement de correctifs

Gestion des incidents de sécurité 12

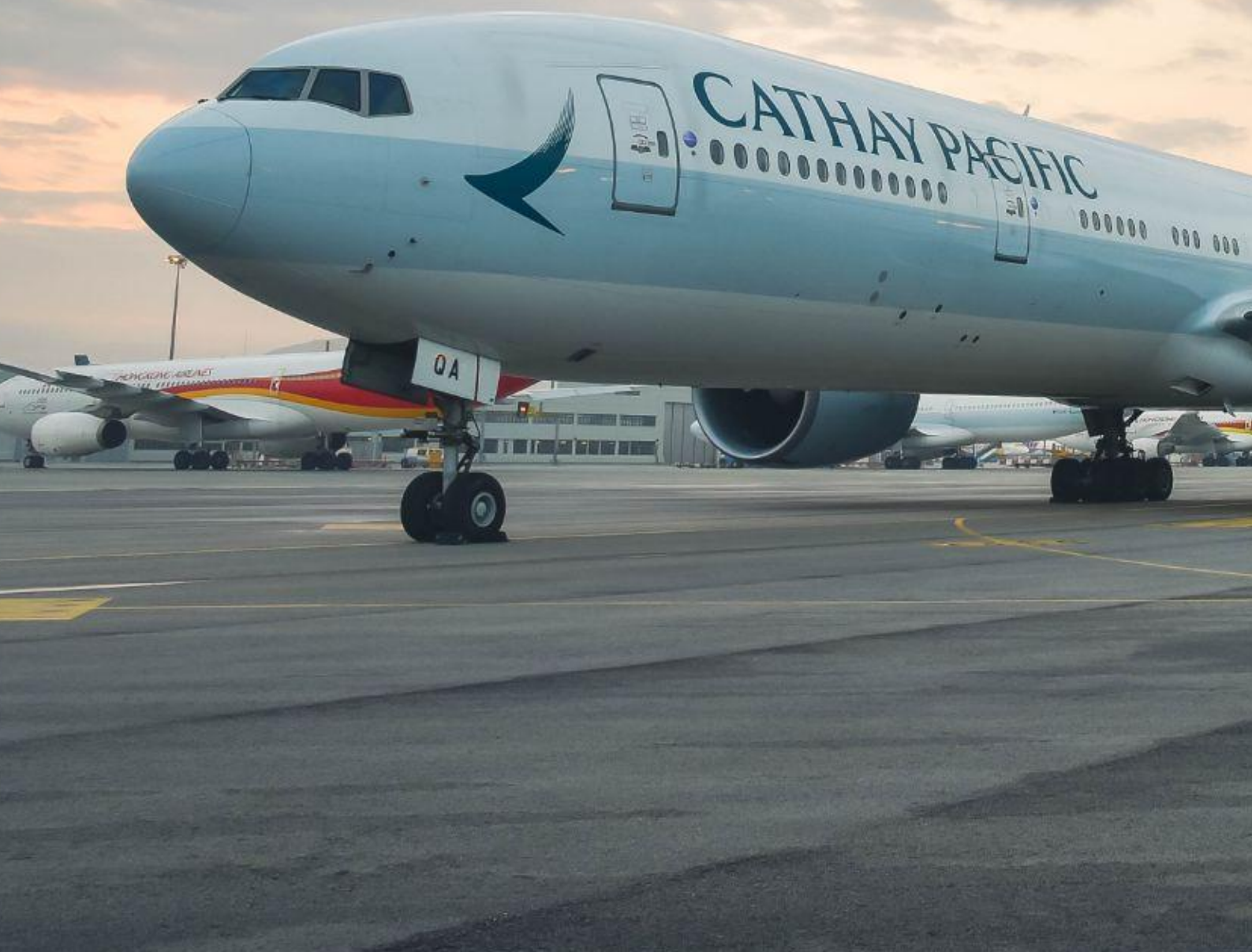
Conclusion 14

Lectures complémentaires

SafetyCulture

«Avant SafetyCulture, on devait saisir toutes les données de la liste de contrôle une fois de retour au bureau, puis faire des analyses Excel sur ces données, et enfin les partager avec l'équipe. Données analytiques nous fournit des données plus complètes et les centralise en un seul endroit facile à partager. »

Deaky Wong
Ingénieur de maintenance de ligne
Cathay Pacific



Notre mission

SafetyCulture aide les entreprises à créer des lieux de travail plus sûrs et plus performants partout dans le monde, grâce à des outils innovants et peu coûteux conçus pour les appareils mobiles.

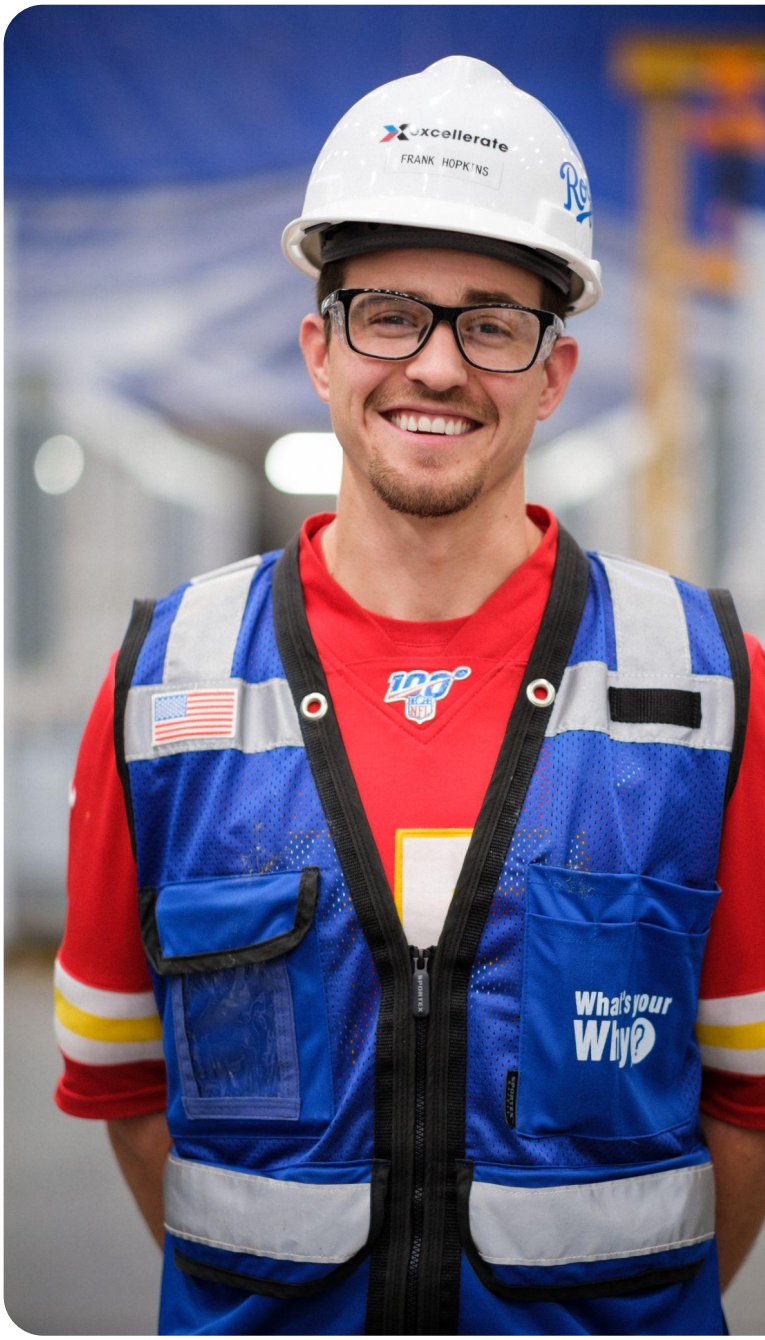
Nous accomplissons notre mission grâce à nos produits SaaS (Software-as-Service).

Nos produits sont utilisés plus de 50 000 fois par jour par plus de 27 000 entreprises dans le monde, dans de nombreuses industries et des domaines variés. L'approche décrite ici est utilisée pour nos différents produits et services.

Nous sommes fiers que SafetyCulture soit considéré comme un leader mondial dans le domaine de la sécurité et de la qualité, et nous savons à quel point il est important d'aider nos clients à améliorer leurs opérations quotidiennes.

Notre approche de la cybersécurité est un pilier essentiel pour maintenir notre statut de leader dans ce domaine. Ce document donne une vue d'ensemble de la manière dont notre organisation aborde les questions de cybersécurité.

SafetyCulture est certifié ISO 27001:2024 et nous respectons les critères des services fiduciaires de l'AICPA, ce qui témoigne de notre attachement à la sécurité de nos clients.



Vue d'ensemble

Programme de cybersécurité

SafetyCulture a mis en place un programme de cybersécurité actif, solide et en constante amélioration pour garantir la sécurité de notre organisation et des produits que nous fournissons.
Le programme de cybersécurité de SafetyCulture utilise de nombreux contrôles au niveau technique et opérationnel pour garantir une approche efficace de défense et de protection contre les cyberattaques et sécuriser les données traitées par nos produits Software-as-a-Services (SaaS).

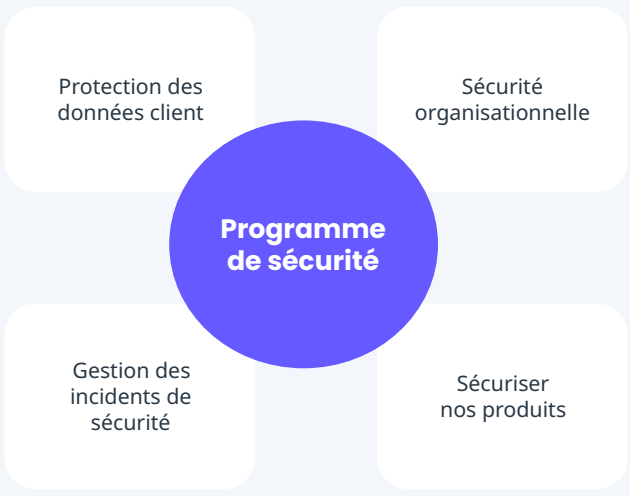
Principales fonctionnalités :

- Un programme de sécurité aligné sur les normes de meilleures pratiques de l'industrie, y compris l'utilisation de plates-formes cloud conformes à des critères de sécurité fiables, notamment ISO 27001 et SOC 2.
- L'accent est mis sur le respect des principes de base, en reconnaissant que les principes de base de la sécurité restent les plus importants. Cela comprend les éléments suivants :

  ➔ Former notre personnel à l'importance de la sécurité.
  ➔ Disposer d'une équipe de sécurité spécialisée chargée de protéger notre organisation contre les menaces réelles et imminentes qui pèsent sur nos activités et les données que les clients nous confient.
  ➔ Employer des mécanismes solides pour garantir que l'accès aux systèmes de SafetyCulture et aux données des clients est soigneusement contrôlé.
  ➔ Chiffrer les données des clients que nous détenons (tant en transit qu'au repos) en utilisant des mécanismes de cryptage solides.
  ➔ S'assurer que nous appliquons des correctifs aux vulnérabilités de notre environnement informatique et de nos produits aussi rapidement que possible afin de minimiser les possibilités d'exploitation par les cyber-attaquants.
  ➔ Surveiller et tester activement notre environnement informatique et nos produits pour détecter les vulnérabilités et y remédier le plus rapidement possible.
  ➔ Disposer d'un processus défini pour fournir une prise en charge et une réponse efficaces en cas d'incident de sécurité.

Mener une vérification préalable pour s'assurer que nos fournisseurs de services respectent les normes de l'industrie en matière de sécurité - nous savons que la sécurité de nos partenaires nous affecte directement, ainsi que nos clients, et nous choisissons donc très soigneusement nos partenaires.

La suite de ce document donne une vue d'ensemble des différents aspects de notre programme de sécurité.



Pratiques de sécurité organisationnelle

Notre approche de la sécurité en tant qu'entreprise s’aligne sur les meilleures pratiques recommandées dans les normes reconnues telles que NIST, ISO 27001 et SOC.

Gouvernance de la sécurité

SafetyCulture dispose d'un ensemble documenté de politiques, de normes et de procédures qui définissent notre approche de la sécurité en tant qu'organisation. Ces politiques et procédures sont partagées avec tout le personnel et sont revues et mises à jour au moins une fois par an (et plus fréquemment lorsque des changements importants sont nécessaires) afin de garantir que notre approche de la sécurité reste à jour.

Notre priorité est la responsabilité de la sécurité dans l'ensemble de notre entreprise. Ainsi, nous avons mis en place un forum de gestion de la sécurité de l'information composé des parties prenantes clés de SafetyCulture qui se réunissent régulièrement pour examiner et discuter des questions liées à la sécurité, et prendre toute décision ayant une influence sur notre approche de la cybersécurité.

SafetyCulture est certifié ISO 27001:2024 et nous respectons les critères des services fiduciaires de l'AICPA, ce qui témoigne de notre attachement à la sécurité de nos clients.

Contrôles d'accès

Nous veillons à ce que l'accès aux systèmes de notre environnement informatique, ainsi qu'aux plateformes sur le cloud, soit limité aux employés qui ont spécifiquement besoin de cet accès pour leur travail. Les autorisations d'accès à nos systèmes sont régulièrement revues, au cas par cas.

Tous les accès des administrateurs à notre infrastructure nécessitent une authentification multifactorielle à l'aide de comptes uniques, et tous les accès et modifications sont surveillés et consignés.

Les autorisations d'accès à nos systèmes sont régulièrement examinées, au cas par cas, et modifiées rapidement. L'accès aux systèmes est revu lorsqu'un employé change de rôle et lorsqu'un employé quitte l'entreprise, l'accès aux systèmes est immédiatement supprimé dans le cadre de notre processus d’implémentation.

Sécurité des tiers

Les pratiques de sécurité des tiers que nous engageons sont examinées au début (en particulier pour tout engagement sensible) et de manière continue pour s'assurer que ces pratiques répondent aux normes de l'industrie et sont conformes à nos propres politiques et procédures de sécurité, ainsi qu'à notre politique de confidentialité. En ce qui concerne les accords avec des tiers qui doivent avoir accès à nos systèmes ou à nos données, nous veillons à ce que l'accès soit spécifiquement limité à l'objectif pour lequel ils ont été engagés.

Amazon Web Services (AWS) est notre principal fournisseur et nous nous engageons auprès d'eux en utilisant le modèle de responsabilité partagée pour la sécurité et la conformité, ce qui garantit une définition claire de la responsabilité de chacun en matière de sécurité.
AWS est accrédité et conforme à un grand nombre des dernières normes de l'industrie - plus d'informations peuvent être trouvées ici : https://aws.amazon.com/artifact

Pour le traitement des données financières et des données relatives aux cartes de crédit, SafetyCulture utilise plusieurs partenaires (Chargify, eWay et Stripe) dont les pratiques de sécurité sont conformes à la norme de sécurité de l'industrie des cartes de paiement (PCI-DSS). Nos employés n'ont pas d'accès direct aux données de facturation.

Sécurité des réseaux

Les réseaux d'entreprise de SafetyCulture sont protégés par des pare-feux ainsi que par un système de détection d'intrusion (IDS) et un système de prévention d'intrusion (IPS) au périmètre fourni par des dispositifs de sécurité de réseau dédiés, afin que nous puissions détecter et protéger tout trafic malveillant.

Pour nos plateformes basées sur le cloud, nous utilisons principalement Amazon Web Services (AWS) qui fournit une stratégie de défense à plusieurs niveaux contre les attaques externes. Au niveau de l'infrastructure, AWS utilise des stratégies telles que le contrôle de l'accès aux dispositifs du réseau, la séparation des données à l'aide de pare-feux et de cloud privés virtuels pour filtrer le trafic malveillant, tout cela étant consigné et contrôlé pour prévenir les attaques basées sur le réseau. Au niveau des applications, nous utilisons le pare-feu d'application Web (WAF) et la protection contre les attaques collectives par saturation de service (DDoS) pour prévenir les attaques contre nos produits.

Nous séparons nos environnements de développement, de test et de production.

Journal d’évènements et suivi

SafetyCulture utilise un système de journalisation centralisé qui inclut les événements d'audit d'accès aux applications. Ces journaux sont conservés pendant 90 jours. Nous utilisons également les journaux d'Amazon ELB pour suivre les demandes d'accès aux services (réussies ou non). Les journaux stockés dans AWS ne peuvent pas être modifiés et l'accès est limité aux personnes qui en ont la nécessité pour leur rôle.
Nous sommes conscients de l'importance d'examiner régulièrement les journaux afin d'identifier les activités malveillantes des utilisateurs et les vulnérabilités potentielles de nos produits. C’est pourquoi nous avons mis en place une surveillance automatisée qui nous alerte sur des types spécifiques d'événements potentiellement malveillants au sein de notre infrastructure mondiale.

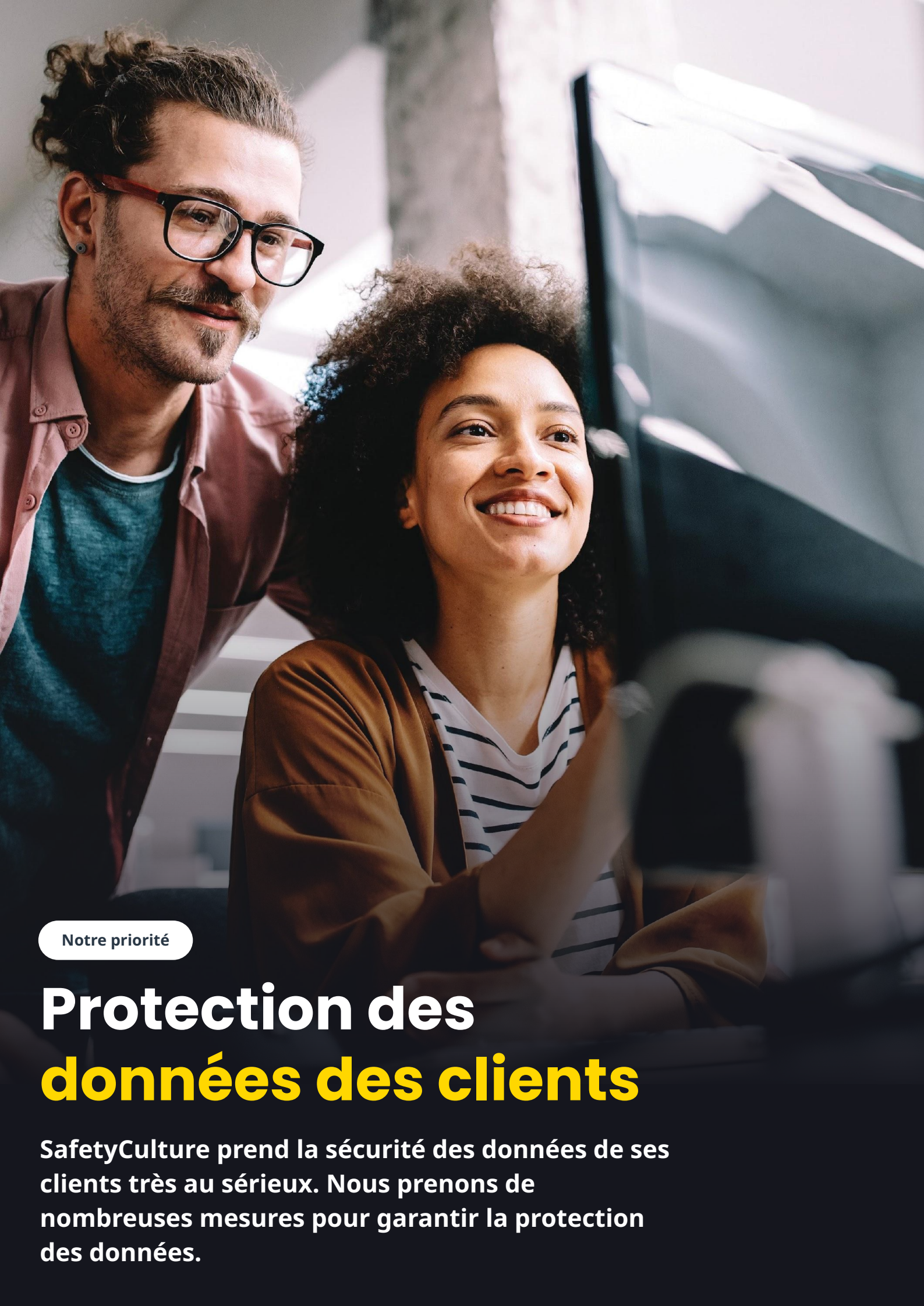
Formation de sensibilisation à la sécurité

Tous les membres du personnel de SafetyCulture suivent une formation annuelle de sensibilisation à la sécurité, aussi bien pour les rôles techniques que non techniques. Des supports de formation à la sécurité sont également élaborés spécifiquement pour certains membres du personnel, si nécessaire, afin de faire face aux défis en matière de sécurité propres à chaque rôle.

Correctifs et gestion des vulnérabilités

La mise en place de correctifs dans notre environnement informatique est l'une des mesures fondamentales pour éviter une éventuelle violation de la sécurité. Pour y parvenir :

- Nous déployons d'abord des correctifs pour les vulnérabilités les plus critiques, ceux-ci étant déployés dans notre environnement de non-production pour un test initial avant d'être rapidement diffusés dans l'environnement informatique.
- Nous utilisons des solutions de gestion des appareils mobiles (MDM) pour garantir l’installation rapide et efficace des correctifs importants.
- Nous utilisons AWS System Manager pour déployer régulièrement des correctifs pour notre infrastructure basée sur le cloud.
- Nos appareils sont sécurisés à l'aide de technologies de sécurité des terminaux afin de détecter et de prévenir les menaces à la sécurité, notamment les virus et les attaques de logiciels malveillants, et de surveiller les activités malveillantes.



Notre priorité

Protection des données des clients

SafetyCulture prend la sécurité des données de ses clients très au sérieux. Nous prenons de nombreuses mesures pour garantir la protection des données.

Protection des données des clients

Restriction de l'accès aux données

SafetyCulture prend de nombreuses mesures pour protéger les données des clients contre un accès ou une utilisation inappropriés par des personnes non autorisées (externes ou internes). Les données des clients sont uniquement stockées dans notre environnement de production, et l'accès à ces données est limité aux seuls employés de SafetyCulture qui ont besoin d'y accéder pour effectuer leurs tâches standard. L'accès aux données des clients est géré à l'aide d'outils de contrôle d'accès et d'authentification (y compris l'utilisation de l'authentification à deux facteurs) fournis par Amazon Web Services et nos autres partenaires du cloud.

Les données des clients ne sont utilisées qu'à des fins compatibles avec la fourniture des services contractuels, comme le dépannage des demandes d'assistance technique. Pour de plus amples informations, veuillez consulter la politique de confidentialité de SafetyCulture à l'adresse suivante :https://safetyculture.com/fr/aspects-juridiques/politique-de-confidentialite/

Dans les rares cas où l'assistance de SafetyCulture doit accéder à des données spécifiques de clients (généralement à des fins de dépannage ou d'assistance), SafetyCulture demandera le consentement du client avant d'accéder à ces données.

Nous ne stockons ni ne mettons en cache les données financières des clients utilisées pour la facturation des services de SafetyCulture et nos employés n'ont pas d'accès direct aux données de facturation.

Accès physique aux données

Toutes les données des clients sont hébergées sur une infrastructure fournie par Amazon Web Services, qui assure la sécurité de ses sites en appliquant les contrôles des meilleures pratiques de l'industrie, comme indiqué sur son site Web consacré à la sécurité et à la conformité, que vous trouverez ici https://aws.amazon.com/fr/architecture/security-identity-compliance/?nc1=h_ls&cards-all.sort-by=item.additionalFields.sortDate&cards-all.sort-order=desc&awsf.content-type=*all&awsf.methodology=*all

Aucune donnée sur les clients n'est stockée dans nos bureaux.

Cryptage des données

SafetyCulture a mis en place des mécanismes pour garantir que les données de nos clients sont toujours protégées.

Au repos, toutes les données des clients stockées dans les systèmes sont cryptées à l'aide d'AES-256 avec des clés gérées par le service de gestion des clés d'Amazon Web Services. Toutes les données sont stockées en toute sécurité et soumises aux politiques et procédures de sécurité d'AWS.

Pour protéger les données en transit, SafetyCulture utilise le protocole TLS (Transport Layer Security) et applique une norme minimale de TLS v1.2 utilisant des clés de chiffrement de 128 bits. Nous prenons en charge les connexions avec des clés de chiffrement allant jusqu'à 256 bits pour une utilisation avec un chiffrement AES.

Sauvegarde des données

Les données de SafetyCulture sont sauvegardées à intervalles réguliers sur différentes solutions de stockage de données cryptées fournies par Amazon Web Services. Les sauvegardes sont répliquées sur plusieurs sites AWS dans la région du client (APAC, USA ou UE).

L'accès aux sauvegardes de données est limité à certains employés de SafetyCulture et seulement lorsque cet accès est nécessaire dans le cadre de leur fonction.

Suppression et élimination des données

Nos données clients sont stockées dans Amazon Web Services (AWS), et soumises aux procédures de suppression et d'élimination d'AWS. Ces procédures comprennent un processus sécurisé pour formater de manière systématique les supports retirés et pour détruire tout matériel qui n'est plus utilisé dans leur centre de données.

Tout matériel appartenant à SafetyCulture et contenant des données confidentielles est soumis à une destruction logique des données conforme aux normes industrielles avant d'être recyclé.

Sécurisation de nos produits

Chez la majorité des clients, la principale expérience de SafetyCulture se fait lors de l'utilisation de nos produits. En conséquence, la sécurité constitue une partie importante de la manière dont nos produits sont développés et leur fonctionnement.

Pratiques de développement de logiciels sécurisés

Dans le cadre de notre processus de développement de produits, chaque changement de code et d'infrastructure est stocké dans un système de contrôle des sources, versionné, examiné puis son impact est évalué avant la mise en production du changement. Cet examen comprend le respect des meilleures pratiques en matière de sécurité. Nous séparons également nos environnements de développement, de test et de production, et n'utilisons pas les données des clients dans nos environnements hors-production.

Contrôle des modifications

Toutes les modifications apportées aux produits SafetyCulture sont activement testées au cours de leur développement afin de garantir que l'impact sur les utilisateurs finaux est évalué avant le déploiement, et toutes les modifications importantes sont incluses dans les notes de mise à jour de la production.

SafetyCulture utilise des systèmes de suivi des modifications et de contrôle des versions pour surveiller et gérer activement les modifications apportées à la base de code ou à la configuration de ses produits. Nous utilisons un processus automatisé pour déployer les changements dans nos environnements et nous pouvons les annuler si nécessaire. Nous utilisons Amazon CloudTrail pour suivre les changements de configuration sous-jacents de la plateforme cloud utilisée par nos produits.

Identification des vulnérabilités et développement de correctifs

Nous travaillons sans relâche pour minimiser le nombre de vulnérabilités de nos produits, et nous prenons des mesures proactives pour assurer le traitement des vulnérabilités aussi rapidement que possible. À cette fin, SafetyCulture procède à des tests de pénétration annuels et teste activement les vulnérabilités de ses applications. Nous avons mis en place un programme privé de primes aux bugs en reconnaissance du fait qu'une communauté de chercheurs en sécurité indépendants, incitée à tester nos produits de manière continue pour identifier toute observation potentielle, ne peut que renforcer la sécurité de nos produits.

Lorsqu'une vulnérabilité est identifiée (en interne ou en externe), celle-ci est suivie et classée par ordre de priorité en fonction de la gravité potentielle de l'impact sur nos clients. Pour les observations critiques, nos développeurs peuvent travailler 24 heures sur 24 jusqu'à ce que l'observation soit résolue.

Les correctifs pour les observations sont développés et diffusés dans l'environnement de production par un processus d'intégration continue (CI/CD) et appliqués dès que possible.

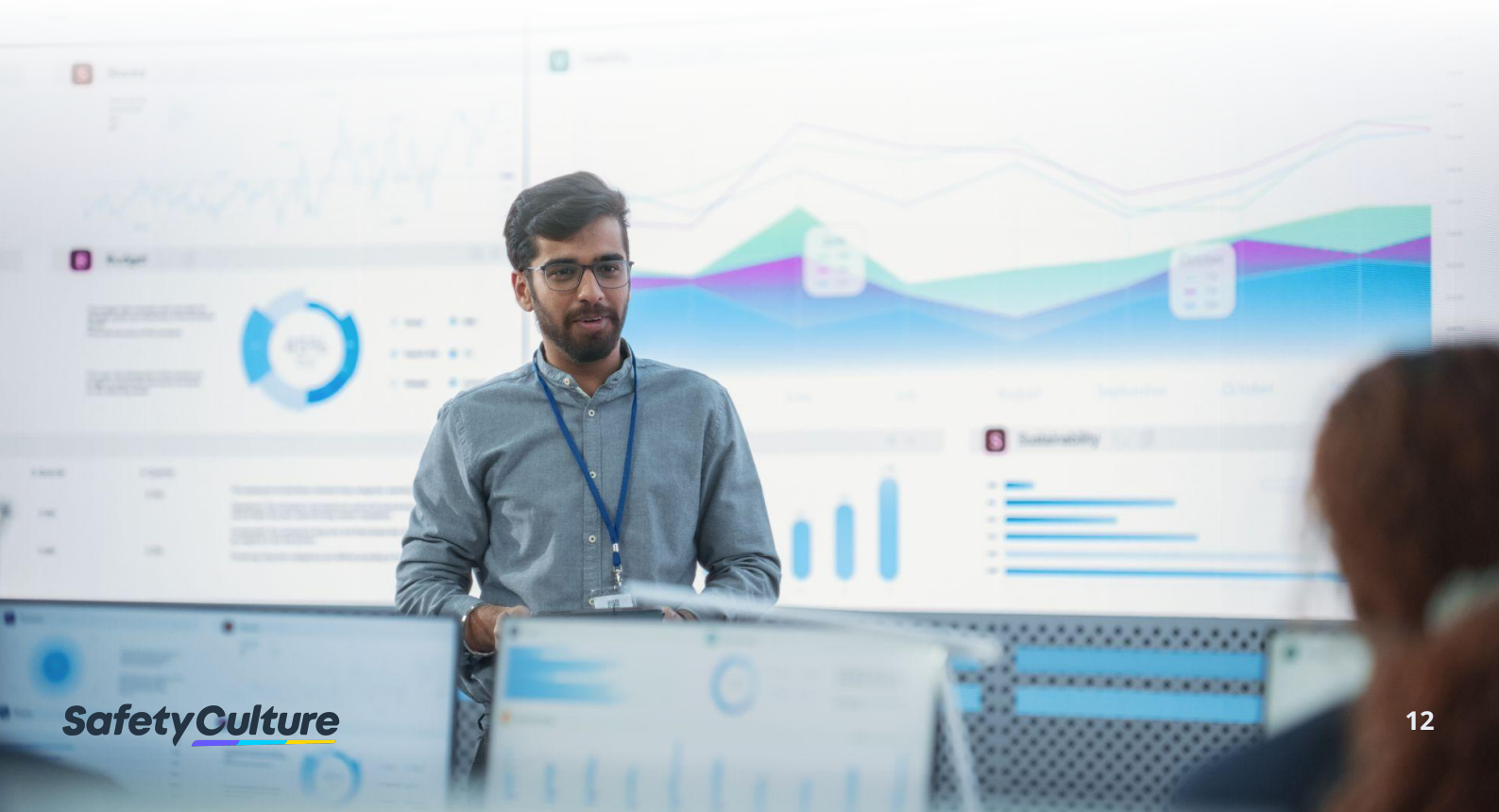
Gestion des incidents de sécurité

Bien que nous fassions tout notre possible pour prévenir tout incident de sécurité, nous devons également être prêts à gérer ces incidents s'ils se produisent afin de minimiser l'impact potentiel sur nos clients et sur SafetyCulture.

Nous avons mis en place une série de mesures, notamment :

- Une procédure de gestion des incidents documentée qui définit notre processus de traitement de la confidentialité, de l'intégrité et de la disponibilité de notre environnement et de nos produits informatiques.
- Une organisation à l'échelle mondiale pour la prise en charge de nos clients pendant un incident.
- Des plans de reprise après sinistre et des stratégies d'urgence qui peuvent être exécutés pour nous aider à maintenir la continuité des opérations pendant un incident. Cela inclut l'utilisation de plusieurs zones de disponibilité géographique fournies par Amazon Web Services et la réplication des données sur plusieurs systèmes dans chaque zone. Ces mesures garantissent un accès continu aux données pendant les incidents affectant la disponibilité du système et fournissent une redondance des données en cas de défaillance du système ou du stockage des données.

SafetyCulture avertit rapidement les clients concernés des incidents majeurs ayant un impact sur la disponibilité des services ou des données de SafetyCulture et de tout incident affectant la confidentialité et l'intégrité de leurs données, conformément à la politique de confidentialité de SafetyCulture disponible à cette adresse : https://safetyculture.com/fr/aspects-juridiques/politique-de-confidentialite/

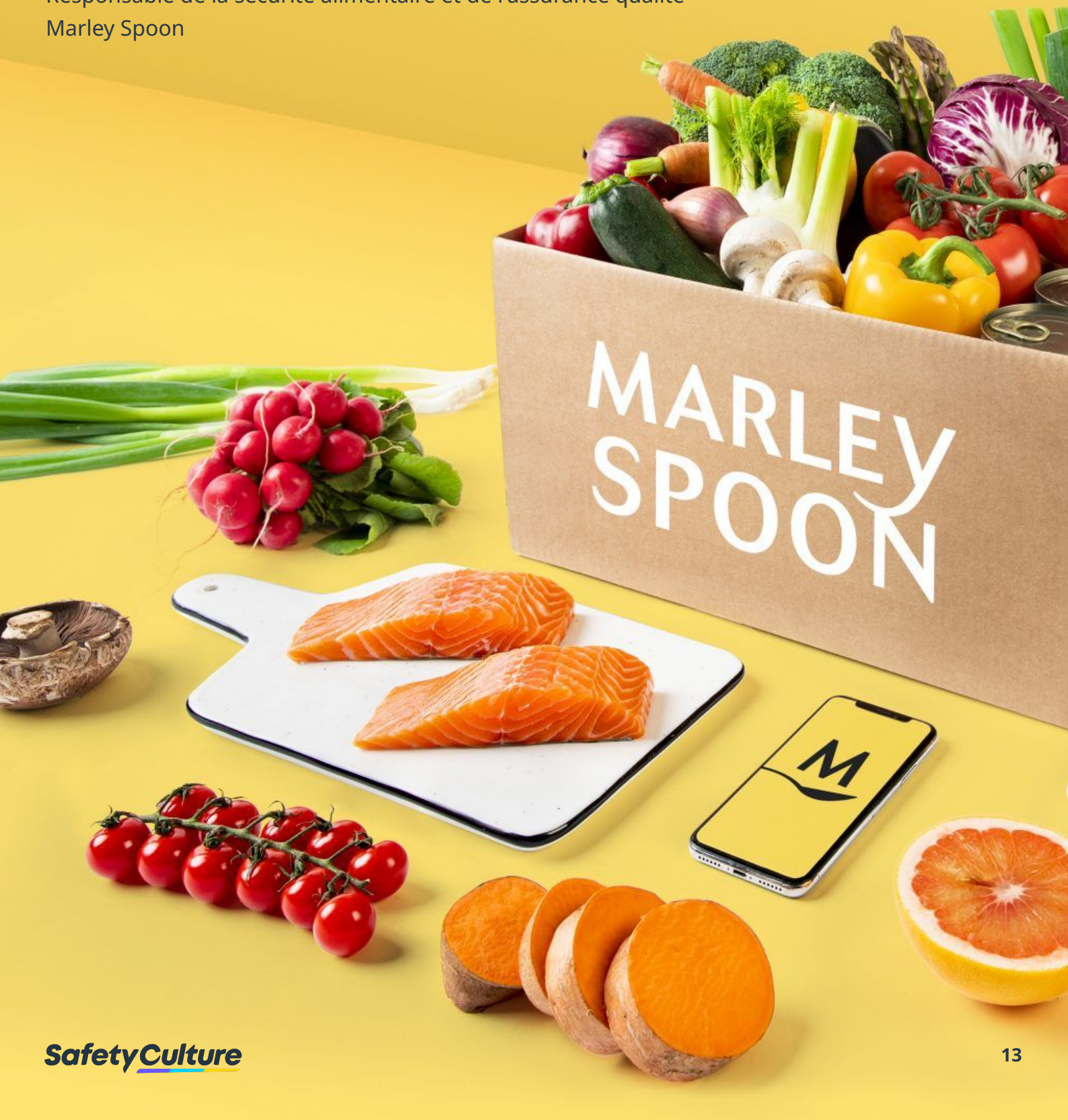


«Les données que nous capturons à l'aide de SafetyCulture nous permettent d'avoir une visibilité sur tout ce que nous faisons. Si une exception se présente ou un processus doit être amélioré, nous n'avons qu'à approfondir pour trouver la solution.»

Sofia Dias

Responsable de la sécurité alimentaire et de l'assurance qualité

Marley Spoon



Remarques

SafetyCulture considère la cybersécurité comme un élément fondamental de son activité et de ses services fournis aux entreprises du monde entier. Bien que les contrôles et les mesures que nous avons mis en place aillent bien au-delà de ce qui est couvert ici, ce contenu fournit un aperçu global de notre approche multifacette et de notre engagement envers la sécurité.

En cas de questions sur ce contenu ou si vous souhaitez obtenir plus d'informations sur notre approche en matière de prise en charge, de sécurité ou de confidentialité, veuillez nous contacter en utilisant les méthodes

- **Soutien :** support@safetyculture.com
- **Confidentialité :** privacy@safetyculture.com

Pour signaler tout problème de sécurité, veuillez-nous contacter à l'adresse security@safetyculture.com

Lectures complémentaires

Notre page de sécurité : https://www.safetyculture.com/fr/securite/

Notre portail sur la confidentialité:
https://safetyculture.com/fr/aspects-juridiques/portail-de-confidentialite/

Notre page de statut des services https://status.safetyculture.com/