FORTRA™

GUIDE (TERRANOVA SECURITY)

Le pouvoir d'un rapport personnalisé en matière de formation de sensibilisation à la sécurité

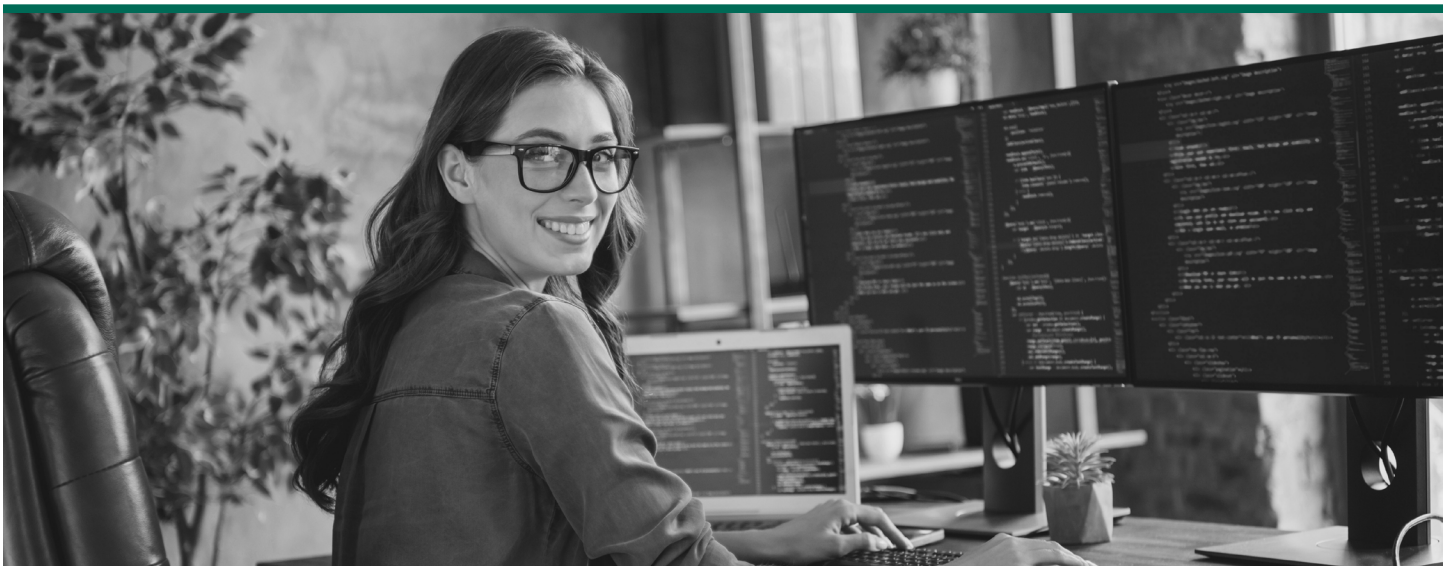
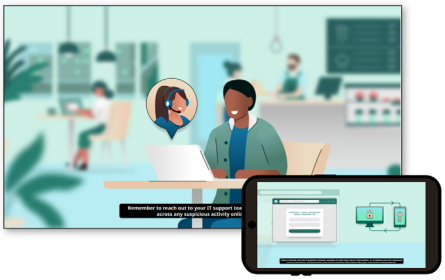
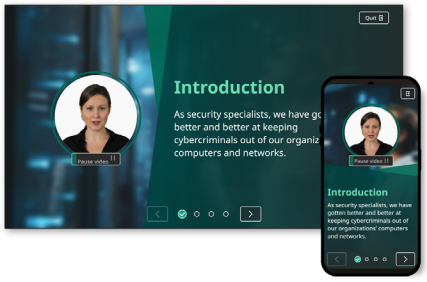


TABLE DES MATIÈRES





INTRODUCTION

Un programme de formation solide et polyvalent qui évolue dans le temps n'est efficace que si les données qui le sous-tendent sont les bonnes. Ce qui distingue les analyses de base des connaissances utilisables et fondées sur les données est leur degré de personnalisation par rapport à la stratégie globale de votre organisation.

Les points de données de haut niveau, comme le nombre total d'utilisateurs qui ont commencé ou achevé une formation, ne vous donneront qu'une idée générale de sa performance. En d'autres mots, est-ce que le fait de savoir que 60 % des employés ont achevé une formation permet aux dirigeants d'une organisation de prendre des décisions informées pour réduire le niveau de risques envers la cybersécurité?

La réponse à cette question se complique encore si elle s'applique à un effectif plus important et, souvent, plus réparti. Le degré de difficulté de la prise de décision sans l'information à l'appui d'objectifs stratégiques particuliers augmente alors de façon exponentielle.

Pour favoriser l'optimisation et l'innovation en matière de sensibilisation à la sécurité pour une base d'employés diversifiée, vos points de vue analytiques doivent être adaptables pour fournir l'information dont vous avez besoin pour réussir. Ce niveau de rapport personnalisé, qui répartit les données par région géographique ou par service au sein d'une organisation, fournit de l'information claire et alignée sur vos objectifs de cybersécurité trimestriels ou annuels.

Des analyses spécifiques et pertinentes vous permettent également d'exploiter pleinement le potentiel de vos données, avec des ventilations plus détaillées de la performance liée aux formations, aux simulations et aux initiatives connexes. Mais, surtout, le rapport personnalisé permet à votre organisation d'adapter les visualisations de données à ses besoins spécifiques.

> **Vos objectifs et votre stratégie sont différents de ceux d'autres organisations de votre secteur de l'industrie, de votre région ou de votre taille. Ils évolueront également avec le temps.**
>
> **Donc, pourquoi se contenter de rapports rigides qui ne tiennent pas compte de la réalité?**

La différence entre un rapport générique et un rapport personnalisé

Dans une ère de transformation numérique accélérée, plusieurs dirigeants et responsables de la cybersécurité ne peuvent compter que sur les données d'un rapport générique pour tenter d'obtenir une vue approfondie de l'efficacité d'un programme de formation à un moment donné. Toutefois, comme les statistiques globales ne peuvent être obtenues que d'un point de vue de haut niveau, la performance à long terme en matière de sensibilisation à la sécurité est à la merci de ces restrictions.

Un format de rapport fournissant des analyses en sensibilisation à la sécurité puissantes et utilisables va beaucoup plus loin que des mesures statiques du genre « test passé/test échoué ». En effet, ces analyses vous permettent d'adapter à vos besoins différents tableaux de bord en les personnalisant pour en tirer la bonne information, au bon moment.

L'accès à des rapports adaptables vous permet d'obtenir des données très pointues sur ce que vous voulez mesurer. L'accès à divers filtres et paramètres aide à cerner les données spécifiques sur des formations, des simulations, des filtres personnalisés et bien d'autres éléments. Par conséquent, votre organisation peut se concentrer sur les enjeux de certaines campagnes et les associer à des programmes de formation ou des objectifs d'entreprise plus larges.

Sans ce niveau de personnalisation d'un rapport, cibler les bons comportements des utilisateurs et bénéficier d'une réduction importante du risque pour la sécurité de l'information s'avère beaucoup plus difficile.

Bref, les analyses génériques produites par des outils de rapport de base offrent aux responsables de la cybersécurité et aux dirigeants un portrait aussi détaillé que la vue depuis le hublot d'un avion. Vous pourrez identifier certains points importants, mais sans plus. Il vous sera très difficile, voire impossible, de discerner des détails plus petits comme les rues ou l'architecture d'une ville.

Conseil d'expert de Terranova Security

Pour que vos données deviennent un actif pour vous, elles doivent être parfaitement adaptées aux objectifs de votre entreprise et à la stratégie qui les soutient pour alimenter votre progression.

Comment les connaissances basées sur les données entraînent le succès de votre formation de sensibilisation à la sécurité

Dans le contexte commercial actuel où la transformation numérique accélérée est la norme, les connaissances détaillées basées sur les données sont essentielles pour libérer le plein potentiel de votre programme de sensibilisation à la sécurité.

Des études récentes démontrent que les organisations fortement axées sur les données sont trois fois plus susceptibles de faire état d'une meilleure prise de décisions. Or, ce genre d'optimisation n'arrive pas par accident. Baser un rapport sur les bons indicateurs et en tirer les données les plus exactes possibles est une partie critique de toute initiative.

Pour soutenir efficacement le changement de comportement et, avec le temps, aider à garder en sécurité l'information sensible personnelle ou d'entreprise, votre programme de sensibilisation à la sécurité doit être :

SPÉCIFIQUE

Vos tableaux de bord doivent utiliser des paramètres spécifiques (p. ex. un cours ou une simulation en particulier, une région ou un service) pour dégager et afficher des analyses pertinentes qui alimenteront votre rapport.

À JOUR

Idéalement, votre plateforme analytique devrait être capable de fournir des mises à jour en temps réel, reflétant les agissements les plus récents des utilisateurs.

AXÉ SUR L'OBJECTIF

Chaque donnée que vous recueillez doit être utile à votre stratégie globale de formation de sensibilisation à la sécurité, de même qu'à tout objectif commercial qui y est associé. Ces réalités uniques et utilisables doivent se refléter dans vos analyses.

Face à l'ampleur des enjeux dans le monde des cybermenaces, l'utilisation des données dont vous disposez est vitale pour façonner un avenir cybersécuritaire pour votre organisation et tous ses employés.

Conseil d'expert de Terranova Security

L'optimisation s'inscrit dans le cadre de la formation en cinq étapes de Terranova Security pour la sensibilisation à la sécurité, qui aide les organisations à tirer le maximum de leur investissement dans la cybersécurité auprès de leurs utilisateurs.

Bâtir un tableau de bord personnalisé : par où commencer

Si votre organisation ne fait qu'amorcer son parcours de sensibilisation à la sécurité, ou si votre cadre actuel d'analyse et de rapport ne donne pas de résultats satisfaisants, il peut être difficile de savoir par où commencer.

Quels paramètres devriez-vous cibler dans vos tableaux de bord? Comment vous assurer d'en tirer des connaissances exactes et pertinentes, qui soutiendront de façon cohérente vos initiatives de sécurité de l'information?

Lorsque vous créez un tableau de bord personnalisé, il est important de commencer avec les éléments fondamentaux de votre programme de formation et de bâtir votre centre d'analyse à partir de là. Examinez d'abord votre stratégie d'ensemble et posez-vous ces questions :

- Quels comportements des utilisateurs votre organisation cible-t-elle avec ses formations ou ses simulations d'hameçonnage?
- Parmi ces comportements, lesquels sont liés à vos plus grandes priorités en matière de formation de sensibilisation à la sécurité?
- Quelles sont les initiatives que vous avez déployées, ou que vous comptez déployer, pour soutenir directement ces priorités?
- Quels sont les objectifs de chaque initiative (p. ex. formation, simulation, campagne en continu)?
- Concernant ces objectifs, quels paramètres sont les plus importants pour définir chaque initiative?

En associant des paramètres spécifiques à chaque aspect d'un programme de sensibilisation à la sécurité, la direction de votre organisation peut rapidement quantifier le progrès mensuel ou trimestriel vers l'atteinte de vos objectifs de cybersécurité. À mesure que votre programme prend de l'importance, qu'il évolue ou même qu'il se multiplie avec le temps, il sera plus facile d'ajuster le format de votre tableau de bord en conséquence.

Conseil d'expert de Terranova Security

Terranova Security recommande de ne pas surcharger votre tableau de bord global dans sa forme initiale, en mettant l'accent sur les paramètres essentiels et les repères dont vous avez besoin. Une fois que vos tableaux de bord ont pris forme, vous pourrez toujours peaufiner les détails pour inclure des informations additionnelles ou différentes.

Bâtir un tableau de bord personnalisé de rapport : les éléments clés

En personnalisant votre format de rapport sur votre programme de sensibilisation à la sécurité, il est essentiel de bien comprendre les principaux éléments du programme. En maîtrisant ces informations, vous pourrez structurer efficacement vos analyses et en tirer tous les points de données essentiels sur votre programme de formation.

Peu importe la taille de votre organisation ou son secteur d'activités, Terranova Security recommande la création de tableaux de bord qui couvrent les éléments suivants :

Formations de sensibilisation à la sécurité

Créez des tableaux de bord qui vous permettent d'approfondir et de distiller l'information importante liée à ces formations pour obtenir des observations détaillées et utilisables.

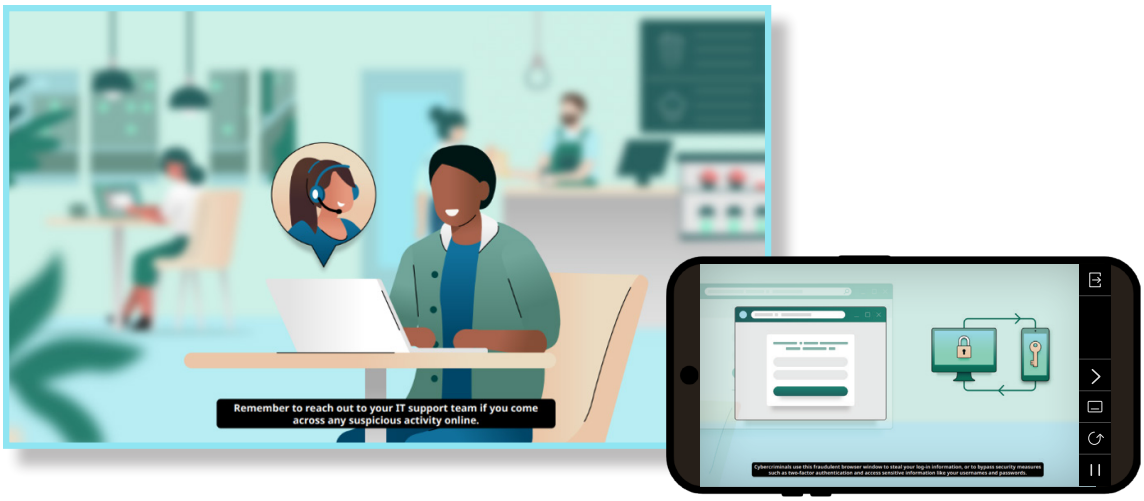
Des données ventilées et filtrées

Assurez-vous que votre équipe de direction peut filtrer ses données ventilées au moyen des analyses de tableaux de bord selon la région, le service, le progrès de l'utilisateur, et d'autres paramètres.

En choisissant chaque élément de votre tableau de bord, optez pour le style de visualisation qui correspond au type de données représentées. De plus, considérez quels intervenants verront l'information et choisissez la visualisation en conséquence.

Conseil d'expert de Terranova Security

Vous pouvez donner un style différent à chaque segment de données qui est représenté. Par exemple, utilisez un graphique à barres au lieu d'une tarte ou d'un graphique linéaire dans la plateforme de sensibilisation à la sécurité pour obtenir une visualisation et une communication claires et concises.



Bâtir un tableau de bord personnalisé : les prochaines étapes

Une fois votre premier tableau de bord monté avec des données exactes et à jour, votre travail n'est pas encore terminé.

Le centre de formation de sensibilisation à la sécurité de votre organisation doit croître et évoluer parallèlement à vos programmes de formation et à vos objectifs généraux de cybersécurité. C'est pourquoi chaque tableau de bord et widget doit refléter les principaux changements aux éléments clés de votre programme de sensibilisation à la sécurité.

Terranova Security recommande de créer une courte liste de vérification que votre organisation pourra utiliser régulièrement afin de tirer le maximum de vos données de rapport.

- Y a-t-il des nouveaux objectifs en cybersécurité ou des paramètres essentiels qui ne sont pas représentés par un widget ou un tableau de bord?
- Parmi vos actifs existants en matière de rapport, y a-t-il certaines données recueillies qui ne sont plus pertinentes ou qui n'appuient plus directement une initiative ou un objectif de formation?
- Parmi les données recueillies, certaines sont-elles trop générales, inexactes ou incomplètes?

Gardez en tête que ces questions ne sont qu'un point de départ et ne forment en rien une liste exhaustive. La liste de vérification est également un outil évolutif qui doit être mis à jour régulièrement, parallèlement à votre programme de formation de sensibilisation à la sécurité. Pour une plus grande exactitude dans vos rapports, coordonnez-vous avec les intervenants impliqués dans la campagne et vérifiez avec eux s'ils obtiennent toute l'information nécessaire.

Conseil d'expert de Terranova Security

Des informations de rapport claires et concises sont essentielles pour la réussite de votre programme de sensibilisation à la sécurité. Évaluez et raffinez vos tableaux de bord de rapport au moins chaque trimestre, en retirant toute information non pertinente et en vérifiant si toutes les données représentées soutiennent vos objectifs de cybersécurité.

La plateforme de sensibilisation à la sécurité de Terranova Security : des tableaux de bord et des rapports

Obtenez les formats de rapports personnalisables et ventilés dont vous avez besoin pour prendre de meilleures décisions, fondées sur les données, avec le tableau de bord global de Terranova Security et ses capacités améliorées de rapport.

Utilisez l'interface flexible et basée sur les widgets pour créer des tableaux de bord de rapports totalement adaptables, affichant vos données les plus importantes concernant vos formations de sensibilisation à la sécurité.

Les options variées de visualisation et les mises à jour des données en temps réel vous permettent de recueillir des renseignements spécifiques au sujet de votre formation, qui serviront à votre équipe de direction pour renforcer la protection des données de votre organisation.

Avec le tableau de bord global de Terranova Security, vos principales analyses sont concentrées dans un nœud central rationalisé pour faciliter la cueillette des données et leur représentation. Ainsi, repérer et évaluer l'information essentielle sur vos initiatives de sensibilisation à la sécurité se fait en quelques clics.

Allez au-delà des rapports génériques « bons pour tous », et obtenez des informations ventilées reflétant précisément la performance et les réalisations de votre formation de sensibilisation à la sécurité. En disposant de meilleures données, vous pouvez rapidement identifier des zones d'amélioration, ajuster rapidement vos objectifs, et abaisser instantanément le niveau du risque planant sur votre cybersécurité.

Les détails sont importants. Faites en sorte que votre organisation dispose de détails pertinents en adoptant la solution de formation hautement reconnue dans l'industrie de Terranova Security.

Réservez une démo personnalisée dès aujourd'hui!

Découvrez la fonctionnalité Tableau de bord global et pourquoi elle est indispensable pour développer et optimiser votre programme de sensibilisation à la sécurité.

DEMANDER UNE DÉMO

FORTRA™

Fortra.com

À propos de Fortra

Fournisseur de logiciels de cybersécurité unique sur le marché, Fortra propose à ses clients un futur à la fois plus simple et plus résilient. Nos experts et notre portefeuille, riche de solutions évolutives et intégrées, offrent aux entreprises du monde entier une maîtrise et un équilibre accrus. Acteurs du changement positif, nous vous accompagnons à chaque étape de votre parcours de cybersécurité et vous aidons à garder l'esprit serein. Pour en savoir plus, rendez-vous sur fortra.com/fr.