Security Scorecard

FICHE TECHNIQUE

Service managé MAX

Opérationnaliser la gestion de la sécurité de la chaîne d'approvisionnement

Problématique

La sécurité de la chaîne d'approvisionnement est fragilisée par un manque de visibilité sur les risques, des évaluations ponctuelles et un volume important de données dépourvues de contexte. Ces vulnérabilités sont accentuées par des processus inefficaces, une responsabilité floue dans la gestion des incidents et un manque d'expertise technique. Les organisations sont ainsi mal équipées pour faire face aux menaces émergentes, gérer leurs fournisseurs et répondre efficacement aux risques.

Solution

La solution MAX de SecurityScorecard est un service managé de détection et de réponse aux risques liés à la chaîne d'approvisionnement (Supply Chain Detection and Response, SCDR).

Pilotée par des experts et alimentée par les dernières technologies de threat intelligence, elle vous permet de reprendre le contrôle sans avoir à gérer ni la communication avec les fournisseurs, ni leur surveillance. Nous prenons en charge l'ensemble (ou une partie, selon les besoins) du cycle de vie des risques cyber au sein de votre supply chain. Vos équipes peuvent ainsi se consacrer à d'autres projets essentiels.

Évaluer

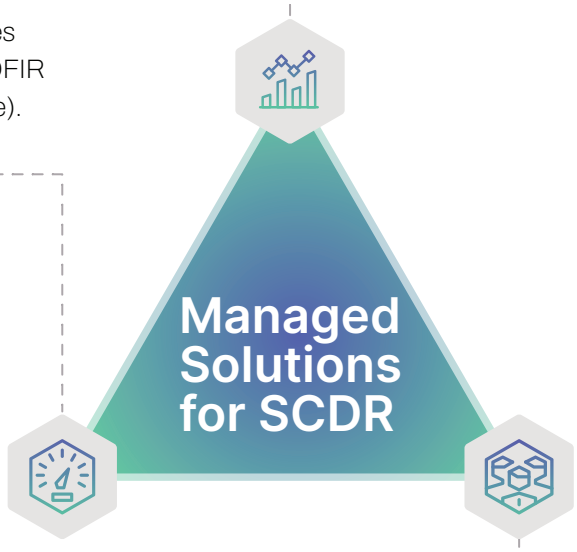
Analyse instantanée de la sécurité des fournisseurs selon des principes de DFIR (digital forensic and incident response).

Monitorer

Visibilité continue et en temps réel des risques cyber de la chaîne d'approvisionnement, y compris les nouvelles vulnérabilités zero-day.

Répondre

Prise de contact directe avec les fournisseurs pour éliminer rapidement les risques.



AVANTAGES MÉTIER

Prévenir les brèches de sécurité

Répondez aux incidents au sein de la chaîne d'approvisionnement en identifiant et en corrigeant les vulnérabilités critiques. Vous limitez alors les points d'entrée potentiels pour les attaquants, et les empêchez d'exploiter les failles des systèmes tiers pour infiltrer votre réseau.

Renforcer les équipes internes

Déléguer les tâches routinières permet à vos équipes de gagner en efficacité opérationnelle et de libérer du temps pour des projets plus complexes.

Favoriser la collaboration avec les fournisseurs

En aidant vos fournisseurs à résoudre leurs problèmes de sécurité, vous renforcez la collaboration et démontrez votre engagement envers leur succès et leur résilience. Vous établissez ainsi des relations plus solides et durables.

SecurityScorecard.com
info@securityscorecard.io

©2025 SecurityScorecard Inc. All Rights Reserved.

Résultats

75%
de réduction des brèches de sécurité liées aux tiers

100%
de remédiation des incidents Zero-Day

3x
moins de fournisseurs à haut risque

2x
plus de remédiation des problèmes détectés

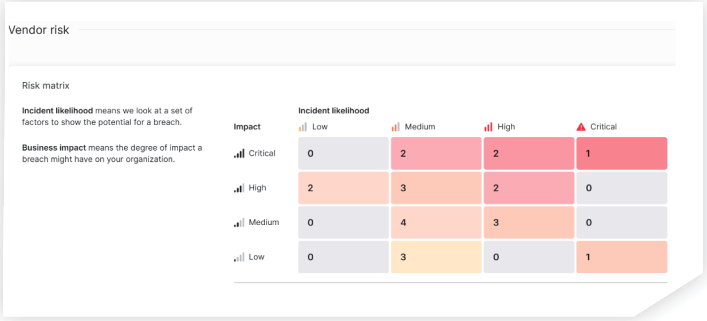
Un service délivré par le Vendor Risk Operations Center (VROC) de SecurityScorecard

Le VROC de SecurityScorecard est composé de professionnels de la cybersécurité disposant d'une forte expérience en matière d'investigations dans les secteurs public et privé, avec une expertise en enquêtes juridico-informatiques, en réponse aux incidents, en détection des menaces et en gestion des risques liés aux tiers.

Fonctionnement

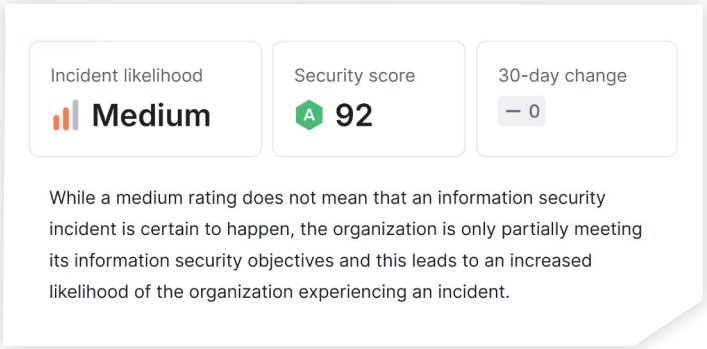
Identification des fournisseurs

Mise en œuvre de politiques et de workflows selon les exigences propres à votre entreprise. Les fournisseurs sont tenus informés de vos attentes en matière de sécurité.



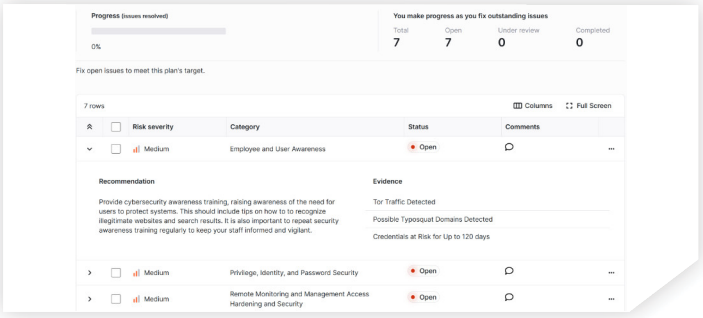
Évaluation de la sécurité

Évaluation de la probabilité d'un incident susceptible de compromettre la confidentialité, la disponibilité ou l'intégrité des informations. Cette analyse permet d'identifier les failles (passées et actuelles) exploitables par des acteurs malveillants.



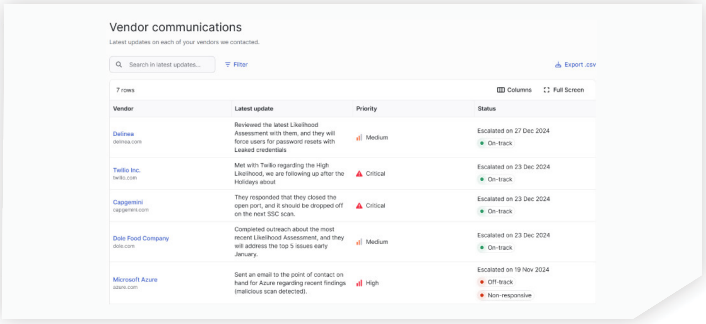
Identification des besoins de remédiation

Élaboration et priorisation de plans d'action pour remédier aux problèmes qui augmentent la probabilité d'incidents. Ces plans s'appuient sur les résultats des évaluations et les réponses aux questionnaires de sécurité afin d'orienter efficacement les échanges avec les fournisseurs.



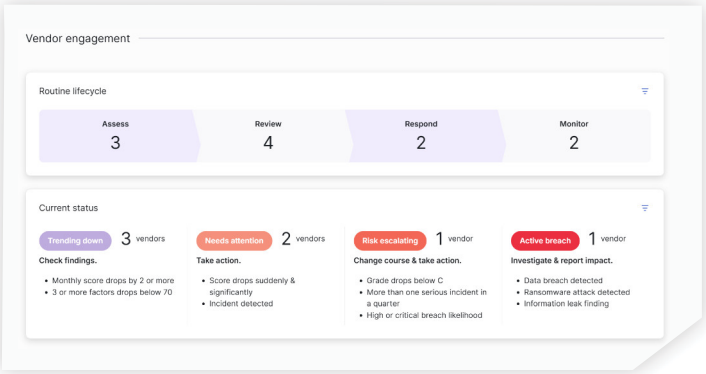
Remédiation avec les fournisseurs

Collaboration directe avec les fournisseurs pour résoudre les problèmes identifiés et renforcer leur posture de cybersécurité. Les progrès ou le manque de réactivité des fournisseurs sont suivis de près afin d'assurer une résolution dans les meilleurs délais.



Monitoring continu des menaces émergentes

Analyse continue de l'exposition des surfaces d'attaque et du comportement des acteurs malveillants pour détecter les vulnérabilités exploitables. Les évaluations et échanges avec les fournisseurs sont relancés dès qu'ils sont impactés par ces menaces.



Options de service

Trois niveaux de services pour répondre aux besoins de votre entreprise

	SILVER Gérer et surveiller les fournisseurs non stratégiques	GOLD Externaliser la gestion des fournisseurs ; conserver la gestion de la communication	PLATINUM Externaliser la gestion des fournisseurs et les communications
Tableau de bord MAX	●	●	●
Configuration de la plateforme	●	●	●
Évaluation de la probabilité d'incident	*Annuelle*	*Deux fois par an*	*Trimestrielle*
Alertes en cas d'incident cyber	*Hebdomadaires*	*Quotidiennes*	*Quotidiennes*
Établissement de rapports	●	●	●
Ajout de nouveaux fournisseurs		●	●
Rapport de vulnérabilités Zero-Day		●	●
Remédiation avec le(s) fournisseur(s)			●

Tableau de bord MAX
Portail client pour consulter les risques liés à la supply chain, communiquer avec les équipes MAX, et suivre les progrès réalisés.

Configuration de la plateforme
Déploiement et gestion de la plateforme SecurityScorecard par une équipe d'experts en réponse aux incidents, digital forensics, analyses SOC et gestion des risques tiers (TPRM). SecurityScorecard prend en charge l'ajout et la classification des fournisseurs ainsi que la mise en place de règles d'automatisation et alertes.

Évaluation de la probabilité d'incident
Analyse approfondie des données d'exposition de la surface d'attaque collectées par SecurityScorecard, aboutissant à une évaluation globale de la probabilité (High, Medium, Low) de compromission d'un fournisseur. Les recommandations d'amélioration précisent les actions nécessaires pour prévenir les violations.

Alertes en cas d'incident cyber
Notifications en cas de compromission avérée ou de risque imminent affectant un fournisseur. Ce rapport comprend notamment des violations non divulguées à grande échelle par les fournisseurs, des preuves de fuites d'identifiants ou des indications de services exposés.

Rapports réguliers
Rapports hebdomadaires et mensuels sur l'état et les résultats du programme de gestion des risques de la chaîne d'approvisionnement.

Ajout de nouveaux fournisseurs
Invitation des fournisseurs à rejoindre la plateforme SecurityScorecard pour la remédiation. SecurityScorecard rencontre également personnellement les fournisseurs afin de présenter vos attentes de sécurité à leur égard.

Détection et réponse aux Zero-Day
Récapitulatif de l'exposition aux vulnérabilités zero-day émergentes. SecurityScorecard identifie les fournisseurs concernés et formule des recommandations ciblées pour renforcer les défenses.

Remédiation avec le fournisseur
Élaboration d'un plan d'action visant à résoudre les problèmes identifiés lors des évaluations de probabilité d'incident. SecurityScorecard accompagne les fournisseurs avec des recommandations ciblées et assure le suivi de la mise en œuvre des correctifs.

EN SAVOIR PLUS:
securityscorecard.com/platform/max

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io

©2025 SecurityScorecard Inc. All Rights Reserved.