Cyber Risk Monitoring*.

Fiche d'information

Mesurez votre niveau de sécurité et votre exposition aux risques grâce à une visibilité complète et des mises à jour quotidiennes. Comblez les écarts observés et exploitez nos données pour rentabiliser au maximum votre investissement en sécurité.

Niveau 1 : Analyse « outside-in » – Vue globale de l'extérieur.

Cette première étape consiste à dresser un diagnostic de l'entreprise d'un point de vue externe. Grâce à BitSight, nous collectons les données à partir de sources publiques sur Internet. Les vecteurs de risque externes sont ensuite évalués pour établir un score de sécurité. Verizon propose également un reporting quotidien entièrement automatisé via son portail de sécurité unifiée.

- Plus de 200 sources de données publiques en ligne
- Rapport quotidien automatisé
- Sources de données fiables – BitSight, Recorded Future et Rapport d'enquête Verizon sur les compromissions de données (DBIR)

Vecteurs de risque

Analyse les vecteurs de risque au moyen de BitSight, ainsi que des informations de Recorded Future (RF) et du Rapport d'enquête Verizon sur les compromissions de données. Ces vecteurs se divisent en quatre grandes catégories : systèmes compromis, problèmes de rigueur des contrôles, comportements des utilisateurs et divulgations publiques de données.

- Infections par botnet
- Propagation de spams
- Malwares
- Communications non sollicitées
- Systèmes potentiellement infectés
- Ports ouverts
- Configuration/certificats SSL/TLS
- En-têtes d'applications web
- Authentification SPF (Sender Policy Framework)
- Authentification DKIM (Domain Keys Identified Mail)
- Fréquence d'installation des correctifs
- Logiciels serveurs, PC et mobiles
- Systèmes non sécurisés
- Enregistrements DNSSEC
- Partage de fichiers
- Identifiants exposés
- Violations de données publiques
- Threat Intelligence du dark web

*Anciennement Verizon Risk Report

Niveau 2 : Analyse « inside-out » – Évaluation des rouages internes de l'entreprise.

Le deuxième niveau de Cyber Risk Monitoring consiste à établir un bilan interne destiné à affiner votre score de sécurité. Nous passons au crible vos terminaux et infrastructures à la recherche de malwares, programmes indésirables et outils à double usage.

- Évaluation des données internes en complément des analyses de niveau 1
- Diagnostic des terminaux et infrastructures pour identifier les risques et évaluer le niveau de sécurité
- Sources de données fiables (Tanium et Cylance en complément des sources du niveau 1)

Vecteurs de risque

Comprend les vecteurs de risque internes collectés par Tanium et Cylance, en complément des vecteurs externes de niveau 1. Les vecteurs de niveau 2 se répartissent également en quatre catégories : malwares, programmes indésirables, outils à double usage et problèmes d'infrastructure.

- Présence anormale de services
- Logiciels en fin de vie
- Versions de firmwares vulnérables
- Systèmes en mauvais état
- Réseaux Wi-Fi visibles par les terminaux
- Outils hébergés sur deux réseaux
- Connexions inhabituelles
- Politiques d'audit et anomalies/mots de passe mal configurés
- Comportements utilisateurs inappropriés
- Problèmes de certificats SSL
- Segmentation du réseau
- Connexions non autorisées
- Risques liés aux applications
- Symptômes d'une éventuelle compromission
- Terminaux infectés par des malwares : ransomwares, chevaux de Troie, faux antivirus, backdoors, virus, téléchargeurs, rootkits, virus du type Infostealer, résidus, vers, exploits, droppers, bots
- Terminaux infectés par des programmes potentiellement indésirables : adwares, jeux, générateurs de clés, barres d'outils, outils de script, outils d'accès à distance, PUP corrompus, outils de piratage, applications mobiles
- Terminaux infectés par des outils à double usage ou d'accès à distance, casseurs de mots de passe, outils de monitoring

verizon

Niveau 3 : Visibilité à 360° – Examen des aspects culturels et procéduraux

Pour obtenir une visibilité totale, les bilans de risque internes et externes sont complétés par un examen approfondi de la culture et des processus de sécurité de l'entreprise. Nous combinons ici la puissance des outils automatisés à l'expertise de nos équipes pour vous fournir une vue intégrale de votre environnement de sécurité et votre exposition au risque.

- Évaluation de la culture et des comportements, processus et politiques, en complément des analyses de niveau 1 et 2
- 100 heures de services professionnels pour mettre à exécution les pistes d'amélioration identifiées
- Bilan complet du dispositif de sécurité

Vecteurs de risque

Comprend les vecteurs de risque externes de niveau 1, les vecteurs de risque internes de niveau 2 ainsi que les vecteurs liés à la culture et aux processus de l'entreprise. Ces derniers sont identifiés par le biais d'un audit sur mesure réalisé par Verizon. Ces vecteurs supplémentaires comprennent :

- Vulnérabilités externes
- Réputation des adresses IP
- NetFlow
- Applications web
- Vulnérabilités internes
- Filtres de messagerie
- Pare-feu
- Terminaux
- Phishing
- Inspection de sécurité physique
- Politiques, processus et procédures
- Réseaux Wi-Fi

Vendor Risk Dashboard.

Avec la généralisation des technologies cloud et des pratiques d'externalisation, l'entreprise digitale se projette aujourd'hui bien au-delà de son périmètre pour s'étendre à de nombreuses entités tierces. Or, chacune de ces structures représente une porte d'entrée potentielle sur votre réseau. Sachant que la force de votre sécurité dépend de son maillon le plus faible, votre surface de risque n'en est que décuplée. Une simple compromission de la sécurité d'un de vos fournisseurs suffirait ainsi à exposer des données clients ou internes critiques, avec des répercussions graves sur votre image de marque, voire la pérennité même de votre entreprise.

Le Vendor Risk Dashboard établit un bilan de sécurité de vos fournisseurs et partenaires. Avec ce tableau de bord, vous obtenez une vision complète de votre sécurité grâce à une Threat Intelligence personnalisée et des scores de risques pour chacun des tiers désignés.

Les notifications immédiates vous permettent d'identifier en amont les problèmes potentiels, d'allouer les ressources plus efficacement et de collaborer avec les acteurs de votre supply chain pour lutter contre les menaces les plus dangereuses. Les rapports créés peuvent également servir à mesurer l'exposition aux risques d'une entreprise en vue d'une éventuelle opération de fusion-acquisition, puis de définir des actions correctives.

Dans le tableau de bord, vous pouvez définir un coefficient de menace et de sécurité correspondant au secteur du fournisseur sélectionné. Vous pouvez également créer des groupes de fournisseurs, consulter les vecteurs de menace prioritaires et visualiser graphiquement les scores agrégés de tous les fournisseurs et groupes de fournisseurs.

Portfolio Management.

Le service Portfolio Management est proposé en option. Il offre une vue synthétique de vos filiales, succursales, etc., avec possibilité d'approfondir vos analyses. Pour une consultation encore plus rapide du portefeuille, vous pouvez passer d'une filiale à l'autre sans avoir à vous déconnecter. Le Portfolio Dashboard affiche divers graphiques représentant les différents niveaux de sécurité et d'exposition aux menaces de l'ensemble du portefeuille. Le Manage Portfolio affiche quant à lui vos filiales et succursales sous forme hiérarchisée.

Plus d'infos.

Cyber Risk Monitoring optimise le développement et l'évaluation de votre stratégie de sécurité. Plus d'infos sur : enterprise.verizon.com/fr-fr/products/security/cyber-risk-monitoring

verizon