CHUBB®

Toujours une longueur d'avance : Rester informé et réagir rapidement aux points faibles

Dans le paysage numérique actuel en constante évolution, les entreprises de toutes tailles sont constamment menacées par des failles de cybersécurité. Selon la Cybersecurity Infrastructure Security Agency (CISA), 50% des vulnérabilités exploitées connues (KVE) sont exploitées dans les deux jours suivant leur identification et 75% le sont en moins d'un mois. Il est impératif d'avoir un programme de gestion des vulnérabilités en place pour agir rapidement et les corriger avant que des activités malveillantes n'entrent et ne se propagent dans le réseau d'une organisation.

Détection dynamique des vulnérabilités Chubb

Grâce à notre approche de gestion des vulnérabilités, notre équipe de Cyber Intelligence surveille, analyse et identifie régulièrement les vulnérabilités et les nouvelles menaces critiques pour aider à protéger nos assurés. Les assurés qui s'inscrivent pour recevoir des alertes sont informés par :

Un programme d'information - Il s'agit de notifications préventives à l'intention des titulaires de cyberassurance si des vulnérabilités critiques connues sont détectées dans leur environnement et ont une forte probabilité d'exploitation.

- Une communication initiale par e-mail, qui détaille l'exposition et les mesures à prendre pour y remédier.
- Des suivis, qui sont ensuite effectués par courriel et par téléphone.

Des alertes ciblées - Ces alertes sont envoyées aux titulaires de police cyber lorsque de nouvelles vulnérabilités présentant une forte probabilité d'exploitation sont découvertes et peuvent avoir une incidence sur leur environnement.

- Une communication par email contenant des renseignements sur la nouvelle menace est généralement envoyée dans les 24 heures suivant la découverte.

Solution supplémentaire de gestion des vulnérabilités cyber

En plus de notre service de sensibilisation à la gestion des vulnérabilités, tous les titulaires de police cyber sont éligibles au service gratuit suivant :

- **Surveillance externe des vulnérabilités** (en partenariat avec Bitsight) - Les titulaires de police peuvent surveiller quotidiennement les risques cyber grâce à une plateforme utilisant des mesures clés, offrant ainsi une visibilité sur la sécurité des organisations.

Pour vous inscrire au programme de sensibilisation à la gestion des vulnérabilités de Chubb et pour obtenir plus d'informations sur les services cyber de Chubb : cliquez ici.

Programme de sensibilisation aux vulnérabilités Chubb

FAQ relatives aux signaux d'alerte

FAQ générales

Quel est l'objectif du programme de sensibilisation aux vulnérabilités de Chubb ?

- L'objectif est d'informer les organisations de leur exposition à des vulnérabilités à haut risque et à d'autres erreurs de configuration graves (ports ouverts, infections par des logiciels malveillants, etc.). Chubb a adopté cette approche afin d'alerter et d'assister les assurés dans l'identification et la remédiation des problèmes liés à Internet que notre équipe de renseignement a classés comme des expositions à haut risque. De ce fait, chacune des vulnérabilités que nous identifions peut et sera identifiée en fonction des auteurs de la menace. De plus, la liste des vulnérabilités que Chubb analyse est considérée comme hautement exploitable si elles se retrouvent dans la nature.

Pourquoi Chubb m'alerte-t-il sur les vulnérabilités dans mon environnement ?

- Cette alerte constitue une composante essentielle de la relation symbiotique entre Chubb et nos assurés. Cela fait plus de cent ans que nous fournissons des services d'ingénierie des risques à nos assurés à travers le monde, ce qui rend nos assurés de meilleurs gestionnaires des risques, et Chubb un meilleur souscripteur. Le cyber n'est pas une exception. Lorsque nous identifions des vulnérabilités qui causent des pertes ou qui figurent sur des listes de renseignements sur les menaces à haut risque que nous pouvons observer dans les environnements de nos assurés, nous travaillons en priorité à réduire l'exposition à ces vulnérabilités.

Ces alertes ont-elles un impact sur la couverture ?

- Non. Cependant, une réticence à prendre des mesures pour remédier à ces vulnérabilités prioritaires pourrait avoir un impact sur la souscription de votre police à l'avenir. Par exemple, si nous constatons continuellement ces vulnérabilités et aucune réponse ou action de la part d'un assuré, nous pourrions envisager de ne pas renouveler la couverture.

S’agit-il d’un test de pénétration ?

- Ce n’est pas un test de pénétration. Il n’y a pas de scan actif ni de tentatives de pénétration dans votre environnement. Ce processus utilise des plateformes d’analyse passive externes qui allient des éléments de renseignement à source ouverte (OSINT) et une analyse passive. L’analyse passive est non intrusive et constitue une méthodologie sûre pour identifier les actifs exposés sur Internet et toutes les vulnérabilités ou erreurs de configuration potentielles qui leur sont associées.

FAQ relatives aux signaux d’alerte

Pourquoi reçois-je cela ?

- Vous recevez cette alerte car vous vous êtes inscrit au programme de sensibilisation aux vulnérabilités de Chubb, disponible pour nos assurés en tant que service complémentaire avec leur police Cyber. Cela concerne soit une vulnérabilité exploité connue (KEV), soit toute autre découverte de cybersécurité sévère qui a été détectée via des outils de scan externes non intrusifs tels que BitSight et Security Scorecard. L’alerte comprend des informations que l’équipe informatique de l’assuré peut utiliser pour identifier et remédier à l’exposition.

Que faire si je ne comprends pas ces alertes ?

- L’équipe de renseignement cybernétique de Chubb est heureuse de discuter de ce processus et des détails de l’alerte avec quiconque dans votre organisation. Vous pouvez également la transmettre à votre spécialiste interne de la sécurité informatique ou à un MSP tiers qui supervise votre environnement pour toute clarification et/ou information.

Je ne sais pas ce que c’est ou quoi en faire, pouvez-vous m’aider ?

- Oui, vous pouvez demander un appel de support général avec l’équipe de conseil en risques cybernétique de Chubb en contactant Cyber@chubb.com.
- Veuillez-vous assurer d’ajouter un commentaire indiquant que vous avez reçu une alerte de vulnérabilité et que vous souhaitez en discuter.

Ce n’est pas mon adresse IP. Une action est-elle nécessaire ?

- Veuillez transférer l’alerte à Cyber@Chubb.com en notant les adresses IP incorrectement attribuées, et nous mettrons à jour nos dossiers pour indiquer qu’elles sont liées à un objet non assuré. Si vous le souhaitez, l’équipe de conseil en risques cybernétique de Chubb peut fournir des instructions à votre équipe informatique pour soumettre une demande concernant ces constatations via Bitsight ou Security Scorecard afin de prévenir de futures alertes automatisées concernant ces IP incorrectement attribuées.

Ce n’est pas mon domaine.

- Veuillez contacter Cyber@Chubb.com en confirmant le domaine correct, et Chubb s’assurera que votre police est mise à jour pour le refléter. Nous mettrons ensuite à jour nos dossiers pour montrer que la vulnérabilité est liée à un actif non assuré et fermerons le cas associé.

Tous les services de cybersécurité sont susceptibles d'évoluer. Les modifications apportées à l'offre de services seront reflétées sur le formulaire en ligne des services de cybersécurité locaux. Il appartient aux souscripteurs de police d'examiner les conditions spécifiques de chaque prestataire externe de cybersécurité afin de garantir leur éligibilité et de se tenir informés des changements susceptibles d'intervenir.

SERVICES DE CYBERSECURITE PROPOSÉS PAR DES PRESTATAIRES EXTERNES :
Surveillance des vulnérabilités externes, Gestionnaire de mots de passe sécurisé

Les services de cybersécurité décrits ci-dessus sont proposés par des prestataires externes sans frais supplémentaires pour les souscripteurs de police Chubb pendant la période initiale indiquée, à condition que le souscripteur de la police soit un nouvel abonné/client des services de cybersécurité proposés par le prestataire externe choisi et que le souscripteur de la police remplisse par ailleurs les conditions d'éligibilité précisées. Après l'expiration de la période initiale indiquée, les souscripteurs peuvent avoir la possibilité de conserver leurs services de cybersécurité à un tarif réduit lors du renouvellement. Veuillez noter que la réduction accordée peut varier selon les produits et services. Les réductions sur les produits et services proposés par les prestataires externes de cybersécurité sont applicables uniquement pour les souscripteurs de police Chubb en vigueur et sont soumises à la réglementation applicable. Les produits et services fournis par des prestaires extérieurs sont soumis aux termes du contrat que le souscripteur de la police conclut avec le prestataire externe. Chubb n'est pas impliquée dans la décision du souscripteur de la police d'acheter des services et n'est pas responsable des produits ou services fournis par un prestataire externe.

Le contenu de ce document est fourni à titre d'information uniquement, et ne constitue ni des conseils personnalisés ni une recommandation de produits ou de services à quelque particulier ou entreprise que ce soit.

Chubb European Group SE, entreprise régie par le Code des assurances, au capital social de 896 176 662 euros, sise La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, immatriculée au RCS de Nanterre sous le numéro 450 327 374.

Nous utilisons les renseignements personnels que vous nous fournissez [ou, le cas échéant, à votre courtier d'assurance] à des fins de souscription, d'administration des polices, de gestion des sinistres et d'autres fins d'assurance, comme nous l'avons décrit plus loin dans notre politique de confidentialité principale, disponible ici: www.chubb.com/fr-fr/footer/politique-de-confidentialite-en-ligne.html