Abonnement au Service d'évaluation de la sécurité technique de Cisco

Ce document doit être lu conjointement avec le document décrivant comment Cisco fournit ses services (« Prestation de services par Cisco »), qui est intégré par renvoi au présent document.

L'abonnement au Service d'évaluation de la sécurité technique de Cisco (les « Services ») permet au Client d'accéder à un ensemble de services d'évaluation de la sécurité que le Client peut utiliser pour évaluer sa cybersécurité.

Service d'évaluation de la sécurité technique de Cisco

Les activités peuvent comporter un ou plusieurs des éléments suivants :

- Tests d'intrusion
- Piratage électronique
- Modélisation des menaces
- Évaluation de la configuration ou de la version
- Évaluation de l'architecture de sécurité
- Évaluation de la sécurité du développement et de l'exploitation
- Évaluation des opérations de sécurité

Les activités prévues sont examinées et mises à jour chaque trimestre par le Client et Cisco.

Consommation des droits d'abonnement

La quantité d'unités de crédit d'abonnement (les « Crédits ») achetées est celle indiquée sur le Devis.

Chacun des éléments suivants consommera cinq (5) Crédits :

- Cisco effectue un test d'intrusion interne poursuivant un objectif dans un environnement contenant jusqu'à 500 adresses IP actives;
- Cisco effectue un test d'intrusion externe sur un maximum de 64 adresses IP actives;
- Cisco effectue un test d'intrusion des applications sur un maximum de quinze pages dynamiques ou de points terminaux et un rôle;
- Cisco effectue une vérification de la conception ou de la configuration d'un maximum de cinq appareils.

Lorsque le Client demande des activités, Cisco valide que le Client dispose de suffisamment de Crédits pour de telles activités. Si le solde créditeur du Client n'est pas suffisant, Cisco travaille avec le Client pour définir et affiner l'étendue de l'activité, le cas échéant. Les crédits requis sont proportionnels à la longueur et à la complexité de l'évaluation en cours. Cisco documente la portée de l'activité et les exigences en matière de crédits dans un Document des exigences de la solution (« DES ») qui doit être approuvé par le Client avant le début d'une activité.

Remarques et limitations

Les remarques et les limites suivantes s'appliquent aux services :

- Cisco s'efforce d'attribuer uniformément les ressources tout au long de la durée de l'abonnement aux Services.
- Une fois les Crédits utilisés, Cisco peut suspendre le travail jusqu'à ce que des Crédits supplémentaires soient achetés ou que d'autres dispositions soient conclues par écrit. Les Crédits inutilisés expirent à la fin de la durée de l'abonnement.
- Les activités doivent être demandées par le Client et planifiées au moins quatre-vingt-dix (90) jours avant la date de fin de l'abonnement.
- Le Client autorise expressément Cisco à effectuer des tests d'intrusion ou à simuler d'autres types de cyberattaques dans son environnement, comme indiqué dans le DES pour cette activité. Le Client fournit à Cisco une attestation d'agence ou des documents semblables comme preuve de cette autorisation à la demande de Cisco.
- Le Client n'est pas autorisé à signaler les activités de test, les outils ou l'infrastructure de Cisco utilisés en relation avec les Services comme malveillants à l'intention de tiers.
- Le Client indique à Cisco les conditions préalables pour chaque activité, comme il est indiqué dans le DES approuvé correspondant. Il peut s'agir de connecter des équipements Cisco à des réseaux, de configurer des dispositifs pour autoriser l'accès à Cisco ou de fournir les renseignements d'authentification demandés pour accéder aux systèmes.
- Cisco fait des efforts jugés raisonnables afin de fournir des résultats et un plan de résolution des problèmes.
- Les Services peuvent fournir des renseignements sur les vulnérabilités, les faiblesses et les capacités, mais les résoudre n'entre pas dans le cadre des Services.
- Si, au cours d'une activité, une défaillance ou un problème grave est découvert dans l'environnement du Client qui, selon Cisco, est susceptible d'affecter l'état opérationnel de l'environnement ou l'exécution de la mission, Cisco peut générer un Avis de défaillance de sécurité (« ADS »). Le cas échéant, Cisco peut suspendre ses activités jusqu'à ce que le Client ait consulté l'ADS et ait demandé à Cisco de reprendre ses activités. Dans ce cas, Cisco peut générer une Demande de modification qui peut nécessiter des Crédits supplémentaires.
- Le travail peut avoir lieu après les heures de travail normales, comme déterminé par Cisco.
- Les frais de déplacement seront fixés à l'entière discrétion de Cisco.
- Le Client reste responsable de la sécurité de ses environnements.
- Cisco utilise des processus et des technologies commercialement raisonnables pour évaluer la cybersécurité du Client, mais Cisco ne garantit pas que toutes les vulnérabilités et faiblesses de l'environnement du Client seront détectées.
- Les vulnérabilités, les faiblesses et les autres renseignements connexes que Cisco recueille auprès du Client dans le cadre des Services sont considérées comme des renseignements système. Nous les traitons conformément à notre programme de sécurité et de confidentialité mentionné à la section Comment Cisco fournit les services.
- Des renseignements relatifs à la politique d'entreprise Cisco en matière de divulgation des vulnérabilités de sécurité découvertes dans le cadre des Services Cisco sont disponibles à l'adresse : https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html#dsvdpcsd.