Description du service

« Cisco Technical Security Assessment Service Subscription » Abonnement au Service d'évaluation de la sécurité technique de Cisco

La présente Description de service fait partie de l'Accord de services (tel que défini dans le Guide des services) et décrit les divers Services que Cisco vous fournit. Les termes commençant par une majuscule, sauf s'ils sont définis dans le présent document, ont la signification qui leur est donnée dans le Guide des services.

1. Résumé

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

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

2. Crédits de service

La quantité d'unités de crédit de service (les « Crédits ») achetées est celle indiquée sur le Devis. Vous pouvez échanger des Crédits contre la prestation d'activités du Service d'évaluation technique de Cisco. Vous avez le droit d'utiliser le nombre de Crédits indiqué sur le Devis chaque année pendant la Durée des services. Si Vous choisissez une Durée de service non standard, Vos Crédits seront calculés au prorata. Par exemple, un abonnement de cent (100) crédits avec une Durée de service de trente (30) mois Vous donne droit aux éléments suivants :

- Année 1 (12 mois) – 100 crédits
- Année 2 (12 mois) – 100 crédits
- Année 3 (6 mois) – 50 crédits

À titre de référence, chaque activité ci-dessous nécessite cinq (5) Crédits :

- Cisco effectue un test d'intrusion interne poursuivant un objectif dans un environnement contenant jusqu'à cinq cents (500) adresses IP actives;
- Cisco effectue un test d'intrusion externe sur un maximum de soixante-quatre (64) adresses IP actives;
- Cisco effectue un test d'intrusion des applications sur un maximum de quinze (15) pages dynamiques ou de points terminaux et un (1) rôle;
- Cisco effectue une vérification de la conception ou de la configuration d'un maximum de cinq (5) appareils.

Lorsque le Client demande une activité, Cisco définit avec le Client l'étendue de l'activité et les conditions de crédit. Les crédits requis correspondent à la longueur et à la complexité de l'activité que Cisco effectuera. Cisco documente la portée de l'activité et les exigences en matière de Crédits dans un Document des exigences de la solution (« DES »). Le Client approuvera le DES avant que Cisco ne démarre toute activité. Si le solde de crédits du Client n'est pas suffisant pour l'activité proposée, Cisco travaille avec le Client pour affiner l'étendue de l'activité (le cas échéant) ou suggérer d'autres options pour atteindre l'objectif du Client, notamment l'achat de crédits supplémentaires.

3. Remarques et limitations

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

3.1 Cisco s'efforce d'attribuer uniformément les ressources tout au long de la Durée des services.

3.2 Une fois les Crédits de n'importe quelle année utilisés, Cisco peut suspendre le travail jusqu'à ce que des Crédits supplémentaires soient achetés ou que d'autres dispositions soient conclues par écrit.

3.3 Les Crédits inutilisés expirent à la fin de la période d'abonnement aux Services correspondante d'un an.

3.4 Les activités doivent être demandées par le Client et planifiées au moins quatre-vingt-dix (90) jours avant la fin de la Durée des services.

3.5 Le Client répondra à tout DES dans les dix (10) jours ouvrables, et au plus tard cinq (5) jours ouvrables avant la date de début de livraison proposée.

3.6 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.

3.7 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.

3.8 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.

3.9 Cisco fait des efforts jugés raisonnables afin de fournir des résultats et un plan de résolution des problèmes.

3.10 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.

3.11 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.

3.12 Le travail peut avoir lieu après les heures de travail, à la discrétion de Cisco.

3.13 Les frais de déplacement seront fixés à l'entière discrétion de Cisco.

3.14 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.

3.15 Tous les renseignements que Cisco recueille auprès du Client dans le cadre des Services sont considérés comme des informations système. Nous les traiterons conformément au Guide des services.

3.16 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.