<< Service Description

Cisco Talos Incident Response Retainer Service >>

Description de service

Service de conservation de la gestion des incidents Cisco Talos Incident Response

La présente Description du 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. Service de conservation de la gestion des incidents Cisco Talos Incident Response

Le service de conservation de la gestion des incidents Cisco Talos Incident Response fournit une assistance d'urgence et des services proactifs pour évaluer, renforcer et faire évoluer le programme de préparation aux incidents du Client.

1.1 Responsabilités de Cisco

- Fournir un ou plusieurs des services suivants dans le cadre de la gestion des incidents :
    - Les interventions d'urgence aux incidents cybernétiques qui peuvent inclure le triage, la coordination, l'investigation (notamment l'analyse et les enquêtes), le confinement et les conseils pour les mesures correctives
    - L'évaluation de l'état de la préparation pour la gestion des incidents
    - Révision ou élaboration du plan de gestion des incidents
    - Révision ou élaboration du guide de gestion des incidents
    - Création et mise en œuvre d'exercices sur table
    - Recherche proactive des menaces d'adversaires dans un environnement cible
    - Évaluation des compromissions d'un environnement cible
    - Parcours d'entraînement en cyberdéfense
    - Vigie sur demande

- Exercices Purple Team
- Exercices Red Team

- Faire preuve d'efforts conformes aux usages du commerce pour a) affecter une ressource à distance par téléphone dans un délai de quatre (4) heures suivant la réception par Cisco de la notification par le Client d'un incident de sécurité et b) commencer le déploiement de personnel sur le site du Client dans un délai de vingt-quatre (24) heures suivant cette notification.

1.2 Livrables

Les livrables du service peuvent inclure une partie ou l'ensemble des éléments suivants :

- Rapport d'intervention d'urgence en cas d'incident
- Rapport d'évaluation de l'état de préparation à la gestion des incidents
- Plan de gestion des incidents
- Guide de gestion des incidents
- Rapport sur les exercices sur table
- Rapport sur la recherche proactive de menaces
- Rapport d'évaluation des compromissions
- Certificats du Service de simulation d'environnement de cyberdéfense
- Rapport de l'équipe Purple Team
- Rapport de l'équipe Red Team

1.3 Remarques et limitations

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

- Une fois que le nombre d'heures prévues dans le contrat (tel que spécifié dans le devis ou les documents de commande applicables) est utilisé, Cisco peut suspendre le travail jusqu'à ce que des heures supplémentaires soient achetées ou que d'autres dispositions écrites soient prises. Les heures inutilisées expirent à la fin de la durée de l'abonnement.

- La menace dépersonnalisée, l'indicateur de compromission, la vulnérabilité, l'attaque et les techniques utilisées (p. ex., ATT&CK), ainsi que les autres renseignements connexes que Cisco recueille auprès du Client dans le cadre des Services sont considérés comme des renseignements système. Nous les traitons conformément à notre programme de sécurité et de confidentialité mentionné dans le Guide des services.

- En raison de la diversité des situations et des problèmes pouvant se produire, des incidents peuvent nécessiter l'utilisation de divers autres services ou fonctionnalités complémentaires au présent service. Par exemple, les incidents peuvent nécessiter l'utilisation d'outils spécialisés pour améliorer la visibilité et l'accès au réseau.

- Il n'est pas garanti que l'analyse de la cause première permettra de déterminer ou de confirmer la cause fondamentale d'un incident.

- Des efforts raisonnables seront déployés afin de fournir des résultats concluants et un plan de résolution des problèmes.
- Les activités d'analyse des incidents de sécurité peuvent exiger l'achat d'heures supplémentaires par le Client.
- Un minimum de cinquante (50) heures restantes dans le cadre du contrat acheté est requis pour planifier des services proactifs. Si les heures sont inférieures à cinquante (50) heures, les services d'urgence ou le service Intelligence On-Demand seront les seules options de prestation.
- Les services de gestion des incidents peuvent donner un aperçu des lacunes d'un plan de gestion des incidents et fournir un plan de résolution. Toutefois, l'exécution de ce plan peut nécessiter l'achat des services de suivi.
- Des Services proactifs doivent être demandés et planifiés au moins quatre-vingt-dix (90) jours avant la date de fin de l'abonnement.
- Le travail peut avoir lieu après les heures ouvrables normales, comme raisonnablement déterminé par Cisco.
- Les déplacements seront déterminés à la discrétion raisonnable de Cisco. Cisco se réserve le droit de refuser de se rendre dans n'importe quel lieu, à sa discrétion.
- Pour les services d'intervention d'urgence, et lorsque cela est raisonnablement nécessaire pour fournir ou achever le service en personne, Cisco utilisera tous les efforts commerciaux raisonnables pour que le personnel commence à se déplacer vers le site du Client dans les vingt-quatre (24) heures suivant la réception de la demande écrite, si les visas ou les autres besoins en matière de voyage ne sont pas nécessaires. Si des conditions de visa et/ou de voyage sont nécessaires, le personnel Cisco continuera de travailler à distance pendant que des dispositions de voyage sont en cours (p. ex., demande de visa).