« Cisco Talos Incident Response Retainer Service »
Service de conservation de la gestion des incidents Cisco Talos Incident Response

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.

Le Service de conservation de la gestion des incidents Cisco Talos Incident Response est axé sur la préparation et la gestion des incidents à l'aide d'activités ciblées qui évaluent le processus de préparation et de gestion. Le Service de conservation de la gestion des incidents Cisco Talos Incident Response est offert en deux (2) variantes, qui sont décrites ci-dessous. Le Client recevra la version des Services fournis dans un devis.

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.

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
    - Le Service de simulation d'environnement de cyberdéfense propose un atelier de formation technique spécialisée d'au plus 10 étudiants d'une durée de 3 jours, visant à aider le personnel de sécurité du Client à acquérir les compétences et l'expérience nécessaires pour contrer les cybermenaces modernes
    - Vigie sur demande
    - Évaluation de l'architecture de sécurité du réseau

  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 et b) commencer le déploiement de personnel sur le site du Client dans un délai de vingt-quatre (24) heures.

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

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

La version Enhanced du Service de conservation de la gestion des incidents Cisco Talos Incident Response (IR) est axée sur la préparation et la gestion des incidents à l'aide d'activités ciblées qui évaluent les capacités de prévention, de détection et de réponse aux incidents.

Responsabilités de Cisco :

- Fournir un ou plusieurs des services suivants dans le cadre de la gestion des incidents :
    - Interventions d'urgence
    - 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
    - Le Service de simulation d'environnement de cyberdéfense propose un atelier de formation technique spécialisée d'au plus 10 étudiants d'une durée de 3 jours, visant à aider le personnel de sécurité du Client à acquérir les compétences et l'expérience nécessaires pour contrer les cybermenaces modernes
    - Vigie sur demande
    - Évaluation de l'architecture de sécurité du réseau
    - Exercices Purple 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 et b) commencer le déploiement de personnel sur le site du Client dans un délai de vingt-quatre (24) heures.

Livrable

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

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

Remarques et limitations

Les remarques et les limites suivantes s'appliquent aux 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 d'incidents peuvent parfois nécessiter des heures supplémentaires, auquel cas le Client doit acheter des quantités supplémentaires de ce livrable.
- Un minimum de cinquante (50) heures est requis pour planifier des services proactifs. Si les heures sont inférieures à cinquante (50) heures, les services d'urgence seront la seule option 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 du Contrat d'abonnement.
- Le travail peut avoir lieu après les heures ouvrables normales, comme déterminé par Cisco.
- 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 (par exemple, demande de visa).
- Cisco se réserve le droit de refuser les déplacements vers n'importe quel endroit qui est réputé, selon l'opinion raisonnable de Cisco, dangereux, illicite ou susceptible de nécessiter un transfert de propriété intellectuelle forcée par Cisco.