Cyber Incident Response

Assistance d'urgence dans la gestion de vos incidents de sécurité

Description succincte :
Accompagnement global à chaque étape d'une réponse sur incident : détection, confinement, reconstruction et gestion de crise.

Bénéfices client :
Vous gérez vos incidents de sécurité critiques et assurez leur confinement puis la remise en état de votre système par nos experts CSIRT (CyberSecurity Incident Response Team).

Famille de services associés :
- Advanced Incident Response

AIRBUS

Description du service

Description détaillée	• Préparation de la réponse à incident avec les outils appropriés. • Réponse à incident conforme au processus « SANS » et aux bonnes pratiques. • Détection et analyse en profondeur des cyber menaces et des APT sur votre réseau et sur vos points d'accès. • Recommandations et support au confinement. • Supervision continue pendant et après la crise sur site et à distance. • Elaboration d'un ensemble de règles de détection confidentielles et personnalisées pour identifier les attaques ciblées et furtives. • Support et coordination des activités par un manager en réponse à incident dédié. • Support à la remise en état et amélioration de la protection en place. • Support à l'élaboration d'une stratégie et de processus de prévention des incidents, prenant en considération les retours d'expérience. • Support à la gestion de la communication autour des incidents en interne et en externe (sur demande). Un service d'assistance est également inclus dans l'offre de base.
Engagement et délais	Réactivité pour la première intervention sur site.
Suivi opérationnel	• Réunion de lancement. • Rapports techniques hebdomadaires ou au cas par cas si nécessaire. • Point d'étape à la fin de chaque phase du processus de réponse à incident.
Livrables	• Rapport détaillé d'investigation : - Synthèse - Evaluation de la menace - Historique de l'attaque et persistance - Recommandation de confinement - Recommandation de remise en état • Rapports d'analyses sur les codes malveillants (sur demande). • Règles de détection (sur demande). Un portail web dédié et sécurisé est disponible pour accéder aux documents.
Offres disponibles	Devis sur demande adapté selon : • Détection et analyse des cyber menaces. • Confinement et remise en état.

Airbus CyberSecurity
Metapole 1, boulevard Jean Moulin / CS 40001 / 78996 Elancourt Cedex / France
Willy-Messerschmitt-Str. 1 / 82024 Taufkirchen / Germany
Quadrant House / Celtic Springs / Coedkernew / South Wales NP10 8FZ / United Kingdom
Etihad Towers T3 / Corniche Road, 19th floor / P.O.Box: 72186 / Abu Dhabi / United Arab Emirates
www.airbus-cyber-security.com / contact.cybersecurity@airbus.com