SOC CERT CWATCH

Toutes les entreprises, quelles que soient leur taille et leur activité, sont désormais confrontées régulièrement à des cyber-attaques et doivent se préparer, déployer une défense active, adaptée à des menaces et un système d'information en constante évolution et savoir sur qui compter en cas d'incident majeur.

L'OFFRE DE SERVICES CWATCH

01.

Anticiper les menaces qui vous concernent et vous préparer

02.

Participer à la protection de votre système d'information en réduisant sa surface d'attaque et les vulnérabilités

03.

Surveiller et détecter les attaques au plus tôt

04.

Être à vos côtés dans la réponse aux incidents de sécurité pour les analyser, endiguer, éradiquer et rétablir dans les meilleures conditions vos opérations

LES SERVICES MANAGÉS SOC & CERT

ANTICIPATION

- Conseil programme cyber défense
- Veille en menace et appréciation des risques (Ebios RM)
- Sensibilisation sécurité et exercice de gestion de crise
- Campagne de phishing
- Audit pentest & redteam
- Evaluation continue (Security Rating®)

SERVICES MANAGÉS

PROTECTION

- Veille en vulnérabilité et scan de vulnérabilité managé
- Optimisation des fonctions sécurité de solutions (WAF, IDS/IPS, EDR...)
- Mise à disposition flux cyber threat intelligence (IoC / marqueurs techniques)

DETECTION

- Services de vigilance externe :
  - Détection d'événements de sécurité sur vos actifs techniques externes
  - Détection de l'usurpation de vos actifs légitimes
  - Détection d'exposition d'informations sensibles sur Internet
- Services de détection d'attaques internes :
  - Surveillance et détection par corrélation de logs / SIEM
  - Collecte / centralisation des logs sur datalake local ou mutualisé Almond

REACTION

- Intervention sur demande du CERT
  - Réponse à incident majeur
  - Forensic
  - Reverse engineering de malware
  - Recherche de compromission
  - Gestion de crise
- Mise en place et opération de CSIRT internes dédiés
- Solutions de réponse automatisée

vcolin@almond.eu
www.almond.eu