CWATCH sur Azure Sentinel

Services managés de cybersécurité simples, complets et accessibles

| Nous contacter : commerce@almond.consulting

Azure Sentinel

Extorsion et ransomware, vol de données, mise hors service d'activité sensible : le niveau de menace cyber est très élevé pour les entreprises de toute taille et de tout secteur d'activité.

Pourquoi utiliser les services SOC / CERT Almond CWATCH ?

- Anticipation des menaces
- Protection de votre système d'information
- Surveillance et détection des attaques au plus tôt
- Traitement des incidents pour en réduire les impacts sur votre business

Les services CWATCH en bref

Les services CWATCH sont les **services managés SOC / CERT** délivrés par Almond basés sur les technologies **Microsoft Azure Sentinel** et **Microsoft Defender** visant à anticiper, déployer une défense active adaptée à des menaces et un système d'information en constante évolution et être à vos côtés en cas d'incident majeur.

L'offre de services CWATCH

1 Anticiper et protéger

- Anticiper les menaces qui vous concernent et vous préparer
- Réduire la surface d'attaque et les vulnérabilités

Adversaires identifiés, gestion de crise préparée et bonne posture de sécurité

2 Détecter les attaques

- SOC CWATCH basé sur SIEM cloud Azure Sentinel
- Surveiller et détecter les attaques au plus tôt
- Veille et vigilance externe

Identifier et casser au plus tôt les opérations de vos adversaires

3 Répondre aux incidents de sécurité

- CERT CWATCH
- Répondre aux incidents de sécurité majeur et rétablir dans les meilleures conditions vos opérations

Investiguer, contenir & éradiquer la menace et rétablir vos opérations

> ***« Almond nous accompagne depuis 4 ans avec une solution cyber défense complète, basée sur des services managés SOC et un CERT accessibles et efficaces »***
>
> D. Couderc - DSI Groupe Artémis - Financière Pinault

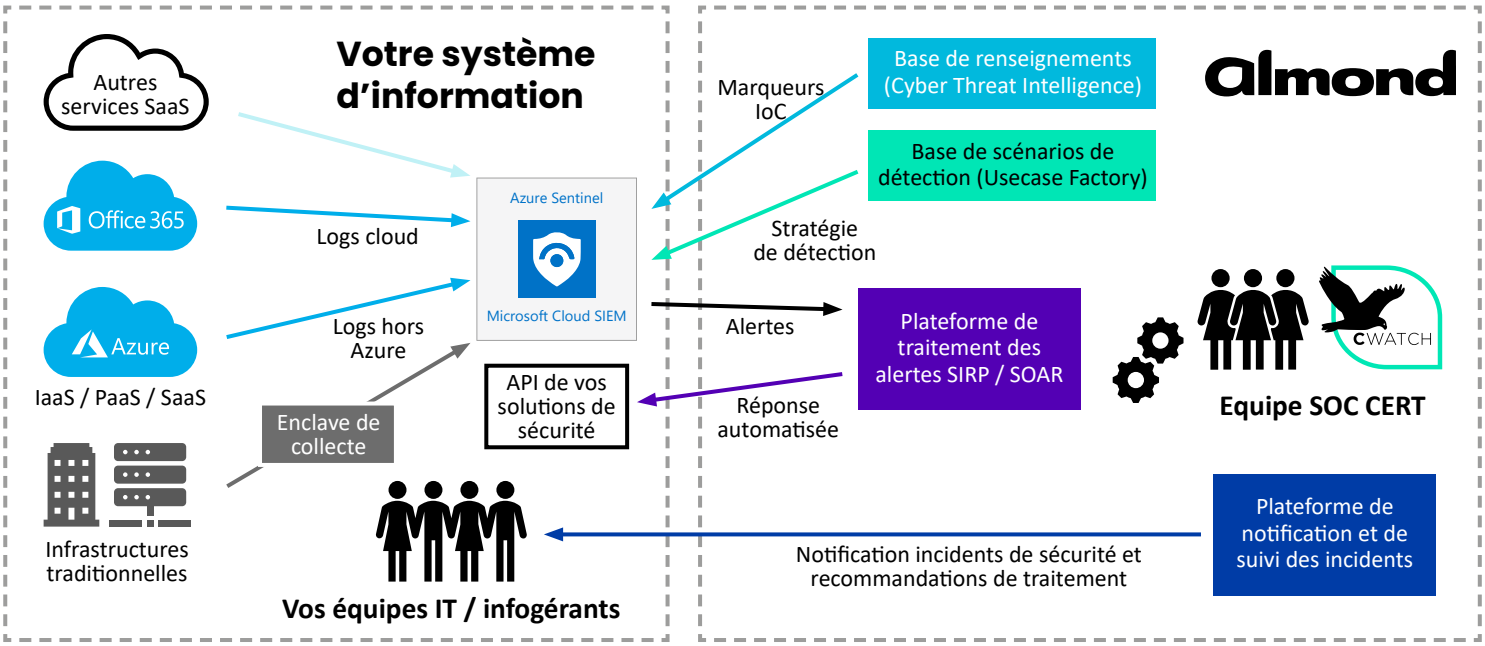
GROUPE ARTEMIS

CWATCH sur Azure Sentinel

Services managés de cybersécurité simples, complets et accessibles

| Nous contacter : commerce@almond.consulting

Architecture de principe



Les services managés SOC & CERT CWATCH

ANTICIPATION

- Conseil programme cyber défense
- Veille en menace et appréciation des risques (Ebios RM) avec les experts GRC
- Campagne de phishing Sensibilisation sécurité et exercice de gestion de crise
- Participation audit redteam / purpleteam
- 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…)

DÉTECTION

- 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

RÉACTION

- 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