

# RESPOND & RECOVER

## Réponse à incident de sécurité

### VOUS ÊTES VICTIME D'UN INCIDENT DE SÉCURITÉ CYBER ?

- Déconnectez les machines du réseau et maintenez-les sous tension.
- Ne les redémarrez pas pour ne pas perdre d'informations utiles lors de l'analyse de l'incident.
- Prévenez votre hiérarchie par téléphone / SMS ou de vive voix de préférence, évitez le mail qui peut être compromis si vous soupçonnez une prise de contrôle étendue de votre système d'information.
- Sécurisez vos sauvegardes.
- Commencez à garder une trace écrite complète et horodatée des événements et de vos actions.
- Ne prenez pas contact avec les cybercriminels.
- **Appelez-nous rapidement.**

### COMMENT CONTACTER LE CERT CWATCH ?

La cellule réponse à incident cyber est composée des analystes du CERT (Computer Emergency Response Team) CWATCH. Ce sont des professionnels qui interviennent régulièrement en réponse sur incident de sécurité. Nos experts sont à votre écoute du lundi au vendredi de 8h30 à 19h00 (CET, hors jours fériés) pour qualifier tout incident de sécurité IT et vous proposer un dispositif de réponse adapté.

- **Téléphone (à privilégier en cas d'urgence) : +33 (0)1 83 75 36 94**
- **Email : [alerte@cwatch.almond.eu](mailto:alerte@cwatch.almond.eu)**

#### DÉTECTION

Vous contactez le CERT CWATCH dès que vous soupçonnez qu'un incident est en cours.

#### QUALIFICATION

Un expert CWATCH vous rappelle pour qualifier l'incident.

#### DISPOSITIF DE RÉPONSE

Le CERT CWATCH vous propose un dispositif initial de réponse.

#### ACCORD

Vous nous confirmez formellement votre accord pour démarrer le dispositif de réponse.

#### DÉMARRAGE

Nous démarrons les opérations de réponse en intervenant à distance ou sur site : collecte, analyse, réaction & remédiation.

#### RÉVISION

Avec la compréhension progressive de l'incident de sécurité, les experts du SOC révisent régulièrement avec vous la stratégie de réponse.

- [contact@almond.eu](mailto:contact@almond.eu)
- [www.almond.eu](http://www.almond.eu)



# RESPOND & RECOVER

## Réponse à incident de sécurité

### L'ÉQUIPE DU CERT CWATCH VOUS AIDE

L'équipe de réponse à incident de sécurité du CERT CWATCH est une équipe d'experts pluridisciplinaires disposant de l'outillage et des compétences, et en capacité d'intervenir à distance et sur site pour :

- Confirmer l'incident de sécurité et le caractère malveillant.
- Déterminer le périmètre impacté.
- Identifier le mode opératoire de l'attaquant, la séquence des événements et les vulnérabilités et autres failles qui ont été exploitées.
- Proposer des mesures conservatoires et/ou correctives adaptées.
- Collecter et stocker de façon sécurisée les preuves et traces techniques liées à l'incident.
- Présenter la chronologie exhaustive de l'incident, des indicateurs de compromission et les renseignements disponibles sur les acteurs.

**Nous pouvons également vous conseiller sur la gestion de crise, la communication interne et externe, le déclenchement des assurances, la notification des incidents et les dépôts de plainte.**

OFFRES	OPEN	OPEN PRÉPAYÉ	CONFORT GRADE 1	CONFORT GRADE 2	CONFORT GRADE 3
Formule	Sans abonnement, ouvert à toutes les entreprises.	Précommande d'au moins 6 tickets valables 1 an, permettant de bénéficier d'un tarif préférentiel sur les journées d'intervention	Abonnement annuel donnant accès à : <ul style="list-style-type: none"> <li>• des SLA courtes</li> <li>• un tarif préférentiel sur les journées d'intervention</li> </ul>	Abonnement annuel donnant accès à : <ul style="list-style-type: none"> <li>• une provision de 4 tickets valables 1 an*</li> <li>• des SLA courtes</li> <li>• un tarif préférentiel sur les journées d'intervention</li> </ul>	Abonnement donnant accès à des services supplémentaires : <ul style="list-style-type: none"> <li>• une provision de 4 tickets valables 1 an*</li> <li>• des SLA courtes</li> <li>• un tarif préférentiel sur les journées d'intervention</li> <li>• Analyse préventive de postes VIP (SLA JO+5) : 4 par an</li> <li>• Analyse de fichier (Sandbox) (SLA JO+2) : 5 par an</li> <li>• Analyse de mails suspects (SLA JO+2) : 10 par an</li> </ul>
Accès au CERT CWATCH pour signaler un incident	Jours ouvrés 8h30 - 19h00				
Démarrage des opérations de réponse à distance	Selon disponibilités, en général démarrage JO+1 après réception des données. Nécessite une validation formelle de la proposition de dispositif d'intervention initiale avant démarrage des opérations		SLA garantissant une réponse à HO+4 Et une intervention à JO+1		
Intervention sur site	Selon disponibilités		Arrivée JO+1 en France métropolitaine (sous réserve de situation sanitaire) Départ en JO+2 hors France métropolitaine (sous réserve des contraintes de visa / vaccination / recommandations du Ministère des Affaires Etrangères)		

\*Un supplément est à prévoir sur les interventions sur site liées aux tickets

Formules applicables au 1<sup>er</sup> janvier 2023

Une offre sur mesure pour les **fonds d'investissement** est possible, discutons-en !

