Respond & Recover
Réponse à incident de sécurité

Vous êtes victime d'un incident de sécurité cyber ?

- Déconnectez (quand c'est possible) 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 nous contacter ?

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. Les clients Active 24x7 ont la possibilité de déclencher le dispositif de réponse par téléphone en 24x7.

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

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.