provadys

SOC Open

Respond & Recover
Réponse à incident de sécurité

Fiche à destination du Responsable Sécurité de l'entreprise

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 SOC Provadys. 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)** : 01 83 75 36 94
- **Email** : incident@soc.provadys.com

Détection
- Vous contactez le SOC dès que vous soupçonnez qu'un incident est en cours.

Qualification
- Un expert Provadys vous rappelle pour qualifier l'incident.

Dispositif de réponse
- Le SOC Provadys 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 Provadys révisent régulièrement avec vousla stratégie de réponse.

Be Smart, Be SOC, Be Safe

Paris | Nantes | Strasbourg
provadys.com

provadys

SOC Open

Respond & Recover
Réponse à incident de sécurité

Fiche à destination du Responsable Sécurité de l'entreprise

Comment le SOC Provadys peut vous aider ?

L'équipe de réponse à incident de sécurité du SOC Provadys 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	CONFORT	ACTIVE	ACTIVE 24x7
Prix de l'abonnement annuel	Gratuit	9 600€ Correspondant à 10 tickets d'intervention prépayés à un tarif préférentiel	Gratuit pour les clients SOC Provadys PROTECT / DETECT	15 000€ de frais d'accès au service 24x7 Service ouvert aux clients SOC Provadys PROTECT / DETECT
Accès au SOC Provadys pour signaler un incident	Jours ouvrés 8h30 - 19h00			24x7 (système d'astreinte en HNO)
Démarrage des opérations de réponse à distance	Maximum JO+1 après réception des données	Maximum 4h ouvrées		Maximum 4h (système d'astreinte en HNO)
Intervention sur site	Selon disponibilités	Arrivée JO+1 en France métropolitaine Départ en JO+2 hors France métropolitaine (sous réserve des contraintes de visa, de vaccination et des recommandations du Ministère des Affaires Etrangères)		
Nombre de tickets d'intervention à distance 1 jour d'intervention HO à distance = 1 ticket 1 jour d'intervention HO sur site = 1,25 tickets	Aucun Nécessite une validation formelle de la proposition de dispositif d'intervention initiale avant démarrage des opérations	10 tickets	Aucun, mais vous disposez de tarifs préférentiels et le démarrage des opérations est accéléré par la prise en compte dans votre contrat SOC	
Prix Ticket d'intervention sur site / heures ouvrées	1 500€	1 200€ Au-delà des 10 tickets inclus dans le pack	1 125€	
Prix Ticket d'intervention à distance / heures ouvrées	1 200€	960€	900€	

Tarifs applicables au 1er avril 2019

Be Smart, Be SOC, Be Safe

Paris | Nantes | Strasbourg
provadys.com