IT Maker
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 ?

- **Déconnecter** (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 compromission étendue.
- **Sécurisez** vos sauvegardes.
- **Commencez à garder une trace écrite complète et chronologique** de tout ce qui s'est passé.
- **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 9h00 à18h30
(heures ouvrées françaises et hors jours fériés) pour qualifier tout incident de sécurité IT et vous proposer un dispositif de réponse adapté. Les clients SOC Active 24x7 ont la possibilité de déclencher un incident par téléphone en 24x7.

- **Téléphone (à toujours privilégier en cas d'urgence) : +33 (0)1 83 75 36 94**
- **Email :** incident@soc.provadys.com **Web** : https://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 RÉPONSES
- 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 vous la stratégie de réponse.

IT Maker provadys

SOC Open

Respond & Recover
Réponse à incident de sécurité

Comment 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.

	SOC Open	SOC Confort	SOC Active	SOC Active 24x7
			Services ouverts aux clients Protect et/ou Detect	
Prix de l'abonnement annuel	Gratuit	9 500€ (1)	Crédits SOC pour couvrir les opérations	19 500€ (frais d'accès au service 24x7)
Accès au SOC Provadys pour signaler un incident	Jours ouvrés 9h /18h30			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 ouvrées (système d'astreinte en HNO)
Intervention sur site	Selon disponibilités	Maximum JO+1 en France métropolitaine Départ en JO+2 hors France métropolitaine (2)		
Nombre de tickets d'intervention à distance	Aucun (3)	10	Crédits SOC	10
Prix d' 1 journée d'intervention sur site en heures ouvrées	1 500€ (4)(5)	1 250€ (4)(5)	1 200€ / 120 Crédits SOC (4) (5)	
Prix d' 1 journée d'intervention à distance en heures ouvrées	1 200€ (5)	1 050€ (5)	1 000€ / 100 Crédits SOC (5)	

(1) Correspondant en totalité à des tickets d'intervention prépayés à un tarif préférentiel
(2) Sous réserve des contraintes de visa, de vaccination et des recommandations du ministère des affaires étrangères
(3) Nécessite une validation formelle de la proposition de dispositif d'intervention initiale avant démarrage des opérations
(4) Frais déplacement hors Ile de France facturés au réel
(5) La facturation des interventions en HNO est majorée

Be Smart, Be SOC, Be Safe

Paris | Sophia - Antipolis | Nantes
provadys.com