Cyberdefense

Crisis Resilience Suite
Contrôler la crise cyber

Face à une crise cyber avérée, la coordination stratégique entre la direction exécutive, le service communication et les équipes techniques devient l'élément pivot.

La réalité de la menace cyber impose d'intervenir via une approche complète, élaborée conjointement avec nos clients pour anticiper et maîtriser leurs incidents rapidement.

Nos experts Orange Cyberdefense sont dotés d'une expérience pointue et peuvent intervenir rapidement pour vous aider à gérer une crise cyber, tant sur le plan technique qu'opérationnel. C'est pourquoi nous proposons différents abonnements qui garantissent des délais d'interventions de nos experts en cas d'attaque avérée.

330 000
PME et TPE attaquées en France en 2022. Ce sont les entreprises les plus touchées.

30% du CA
c'est ce que peux coûter une cyberattaque, en plus d'une perte de confiance des clients et des partenaires.

Comment mettre sous contrôle la crise cyber ?

Etape n°1 Qualifiez l'événement

Il s'agit **d'analyser la nature de la cyberattaque** pour comprendre son déroulement, son ampleur et lister les actifs touchés. Cela, pour saisir l'étendue de l'attaque, donner plus de visibilité aux équipes et mettre en place une stratégie de continuité d'activité.

Etape n°2 Rassemblez les parties prenantes internes au sein d'une cellule de crise

Définie au préalable, **elle doit intégrer les fonctions ayant un rôle à jouer** pour traiter la crise au sens large. Formée et entraînée, des objectifs clairs de sortie de crise lui sont attribuée ainsi qu'une stratégie permettant de les atteindre.

Etape n°3 Prenez des décisions

Bien qu'une situation de crise cyber est incertaine il faut éviter l'immobilisme. Il faut agir en prenant **des décisions éclairées** au regard d'une analyse des bénéfices contre les risques, puis déployer des plans d'action pour remédier aux impacts identifiés, de manière proactive.

Etape n°4 Mobilisez des experts en réponse à incident

Différents partenaires et prestataires doivent être impliqués en fonction de la nature de la cyberattaque, de vos obligations légales, et de vos contraintes réglementaires et au plus proche de vos enjeux opérationnels pour répondre au mieux à l'incident.

Etape n°5 informez les parties prenantes

Dès les premiers instants, il est impératif de **créer des canaux de communication distincts et formalisés** pour diffuser rapidement les informations et donner des indications sur la marche à suivre.

Notre proposition

1 Qualification et assistance

Réagir à un incident détecté et intervenir rapidement sur l'environnement compromis pour le contenir

- Mise à disposition d'un numéro d'urgence (24/7)
- Evaluation des besoins du client pour gérer la crise.

Résultat : un accompagnement personnalisé dans la maîtrise de l'imprévisible pour identifier et isoler l'attaque en fonction de vos besoins et de votre contexte d'affaires.

2 Mise sous contrôle

Piloter la crise en cours et déployer efficacement les actions de maîtrise tout en assurant une continuité d'activité

- Pilotage du plan de réponse à incident et surveillance du SI pendant la durée de la crise
- Déclenchement des dispositifs de continuité (PCA, PSI …).
- Définition des actions de mise en sécurité du SI et du plan de remédiation
- Coordination des services de Réponse à Incident (CSIRT)
- Définition d'une stratégie de communication de crise.

Résultat : une réponse rapide, cohérente et coordonnée qui endigue l'attaque en cours, préserve les actifs et la réputation, et réduit les coûts associés à la crise.

3 Investigation numérique

Comprendre l'origine et la portée de l'attaque, évaluer les impacts et identifier les vulnérabilités du SI

- Identification de la nature et de l'origine de la compromission (indicateurs, réseau et système)
- Cartographie des faits réalisés par l'agent de menace, du périmètre impacté (données, activités)
- Emission d'un rapport d'investigation sur toute la durée de la cyberattaque et de recommandations pour la reconstruction et la sécurisation des SI
- Analyse post-crise de l'impact réputationnel.

Résultat : une vision holistique de la situation et une réponse agile qui guideront l'amélioration de la posture de sécurité pour mieux anticiper et contrôler les incidents cyber à venir.

Nos abonnements

		Standard	Advanced	Premium
		Service Level Agreement (SLA)		
Contrôler la crise	Qualification et assistance	**8h – 18h 5/7** SLA : intervention +2h (inc. 1 jour d'inter.)	**8h – 18h 5/7** SLA : intervention +2h (inc. 1 jour d'inter.)	**8h – 18h 7/7** SLA : intervention +2h (inc. 1 jour d'inter.)
	Gestion de crise	**8h – 18h 5/7** Pas de SLA - **Best effort**. TJM réduit 1200 €/j	**8h – 18h 5/7** SLA : Intervention **+5h**. TJM réduit 1200 €/j	**8h – 18h 7/7** SLA : Intervention **+3h**.TJM réduit 1200 €/j
	Investigation numérique (CSIRT)	**8h – 18h 5/7** Pas de SLA - **Best effort**. TJM réduit 1400 €/j	**8h – 18h 5/7** SLA : Interv. **+3h**. TJM réduit 1400 €/j	**8h – 18h 7/7** SLA : Interv. **+2h**. TJM réduit 1400 €/j
	Onboarding	✓	✓	✓
	Suivi tri/semestriel	✓	✓	✓
Anticiper et prévenir	Prestations intégrées (au choix chaque année)	▪ Check-up Cyber ▪ Sensibilisation à la gestion de crise ▪ Pool jusqu'à 1 jour d'accompagnement	▪ CERT - Diagnostic de l'Active Directory (AD) ▪ Check-up Cyber ▪ Sensibilisation à la gestion de crise ▪ Pool jusqu'à 2 jours d'accompagnement	▪ Audit cyber-résilience ▪ Audit tech. ransomware ▪ Check-up Office 365 ▪ Pool jusqu'à 7 jours d'accompagnement
	Prix €/HT/an	6k €/an	15k €/an	30k €/an