

Déconfinement : la démarche cyber à adopter

Réussir sa sortie de crise en toute sécurité

52%* des employés reconnaissent contourner les règles en matière de cybersécurité pendant le télétravail, ce qui peut exposer leur organisation à des cyberattaques ou à des violations de données.

En cette période inédite, comment éviter d'éventuelles intrusions et/ou fuites de données ? Comment s'assurer que les postes de travail ne sont pas infectés avant de les reconnecter au SI ?

Crise sanitaire, Crise cyber : un parallèle évident



Enjeux sanitaires

- Identifier les foyers
- Soigner les malades
- Relancer l'activité

Enjeux cyber

- Tester
- Protéger
- Redémarrer



3 essentiels pour réussir votre déconfinement cyber

Un pack de sortie dédié à chaque étape de votre déconfinement pour une reprise d'activité en toute sécurité.

1. Tester

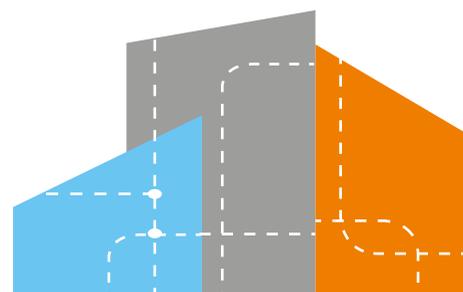
Votre SI et vos utilisateurs pour identifier vos failles de sécurité

2. Protéger

Contenir et éviter la propagation des attaques

3. Redémarrer

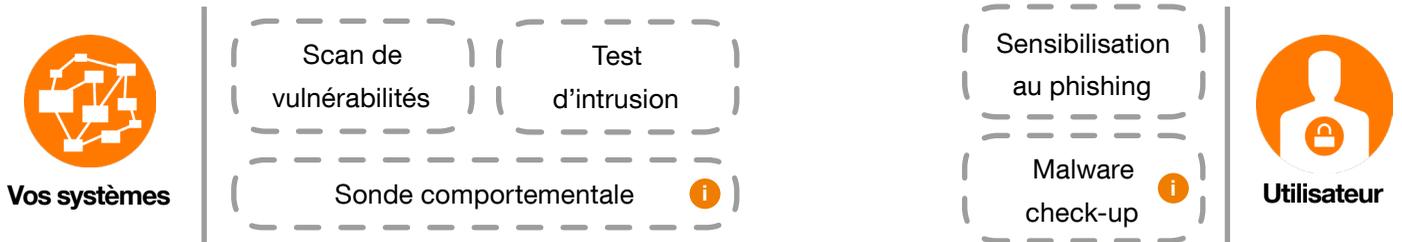
Revenir à la normale et sensibiliser vos utilisateurs aux gestes barrières



Déconfinement : tester, protéger, redémarrer

1. Tester

Tester massivement votre SI et vos utilisateurs pour identifier vos failles de sécurité.



Analyser l'état de santé de votre parc informatique et évaluer les nouveaux risques liés au déconfinement.

2. Protéger

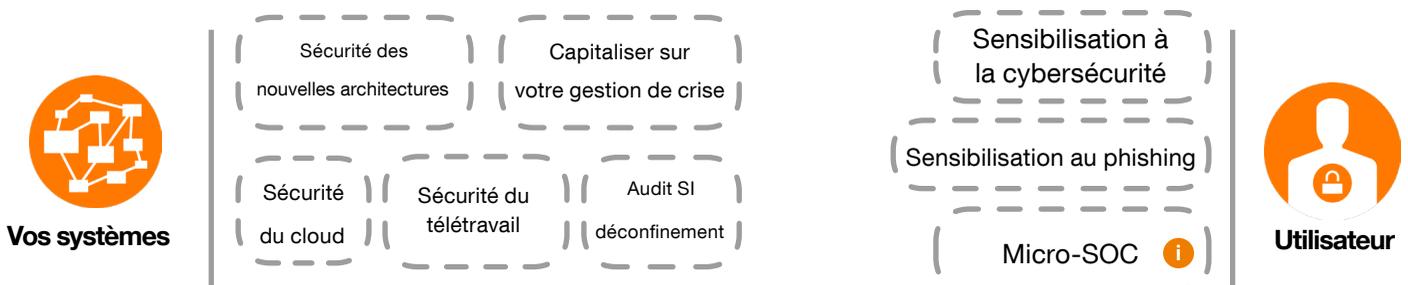
Protéger vos infrastructures (serveurs, applications, postes de travail) afin de prévenir les cyberattaques.



Protéger vos actifs critiques, détecter proactivement les menaces, être aidé dans la gestion de crise.

3. Redémarrer

La crise sanitaire a contribué à généraliser le télétravail et le besoin en agilité.



Renforcer la sécurité des nouveaux moyens mis en place. Capitaliser sur la crise. Sensibiliser les collaborateurs.

Tout comme dans un déconfinement sanitaire, vos collaborateurs doivent être responsabilisés et impliqués dans la mise en place des gestes barrières.

Pour en savoir plus, contactez : contact-fr.oecd@orange.com

Nous suivre : <https://cyberdefense.orange.com>

