

# Les 5 conseils cyber pour une chaîne d'approvisionnement sécurisée

La cybercriminalité coûtera à l'économie mondiale environ **5,2 trillions de dollars entre 2020 et 2025**. Les incidents de cybersécurité font aujourd'hui partie des **3 premiers risques depuis 3 ans\***.

Dans ce contexte, la sécurité de nos clients et partenaires est notre priorité. Les règles suivantes permettront à la fois d'**améliorer la résilience de votre entreprise face aux cyber attaques et de développer une relation de confiance** avec Thales.

La coopération entre Thales et ses fournisseurs est un élément clé, elle se construit en :

- Répondant à un questionnaire d'évaluation de la maturité cyber,
- Prenant en compte les nouvelles clauses contractuelles cyber,
- Mettant en oeuvre (si nécessaire) des actions pour améliorer votre résilience cyber.

Nous vous remercions par avance pour votre engagement.  
Bien cordialement.

## "Construisons ensemble un avenir de confiance"



**Roque Carmona**  
SVP, Directeur  
des Achats Groupe



**Stéphane Lenco**  
VP, Directeur de la Sécurité  
des Systèmes d'Information  
Groupe



### Définir comment gérer la cybersécurité



#### POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Caractériser un **ensemble de règles de cybersécurité** pour **protéger vos informations, produits et services** des risques de cybersécurité.



#### ORGANISATION DE LA SÉCURITÉ DE L'INFORMATION

Nommez un **responsable de la sécurité** et identifiez un **point de contact sécurité** pour Thales.



#### COMPETENCES (EN MATIÈRE DE SECURITE)

**Formez votre personnel** aux règles de cybersécurité.



# 2

## Sécuriser les accès aux sites et protéger les données

GESTION DES ACTIFS ET DES DONNÉES PERSONNELLES

**Maintenez un inventaire des biens et des données personnelles,** de façon à en assurer une gestion sécurisée.



SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

**Contrôlez les accès à vos sites** afin d'éviter les intrusions, les dommages physiques, les vols d'informations ou de biens / matériels.



CONTRÔLE D'ACCÈS

Assurez-vous que tous **les utilisateurs** de vos réseaux et appareils possèdent **un identifiant individuel** et utilisent un **mot de passe fort**. Les droits **d'administrateur** sont uniquement réservés à **quelques personnes**.



# 3

## Construire et fournir des produits et services cybersécurisés

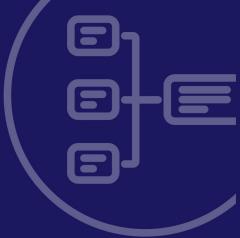


ACQUISITION, DÉVELOPPEMENT ET MAINTENANCE DES SYSTÈMES D'INFORMATION

- Veillez à ce que **les produits ou services que vous délivrez**, aient été conçus et codés en respectant **les règles fondamentales en matière de cybersécurité**, afin d'éviter les attaques faciles des pirates informatiques
- Faites des **évaluations de vulnérabilité** de vos produits et services de façon régulière (au moins 1 fois par an) et pendant toute leur durée de vie.
- Fournissez régulièrement **des mises à jour de sécurité** de vos produits et services, et ce pendant toute leur durée de vie.
- Utilisez des outils de **détection de logiciels malveillants** lors de vos échanges avec des tierces parties et **avant chaque livraison**.

# 4

## Protéger les systèmes en opération



### SÉCURITÉ D'EXPLOITATION



#### GESTION DE LA CONTINUITÉ D'ACTIVITÉ

Mettez en œuvre des dispositifs de **continuité et de reprise d'activité**, notamment pour faire face à d'éventuels sinistres.

- Protégez **tous vos systèmes et équipements contre les logiciels malveillants** à l'aide de solutions anti-virus, et **maintenez-les à jour**.
- **Enregistrez** les événements de sécurité, **contrôlez et auditez** vos systèmes afin d'être en mesure de réagir en cas d'incident.
- Effectuez des **mises à jour de sécurité régulières** sur l'ensemble de vos systèmes, en suivant les recommandations des éditeurs de logiciel.

# 5

## Communiquer



### GESTION DES INCIDENTS LIÉS À LA SÉCURITÉ DE L'INFORMATION

**Un incident cyber** est susceptible de se produire à tout instant malgré toute la vigilance dont vous aurez pu faire preuve. **Soyez prêt à communiquer** cette information à **vos parties prenantes, le plus rapidement possible**.  
**Pour Thales, contactez immédiatement le CSIRT (Computer Security Incident Response Team)** à l'adresse : [cert@thalesgroup.com](mailto:cert@thalesgroup.com).

Les incidents suivants doivent être immédiatement signalés :

- Les incidents cybers de type rançonlogiciels, virus, intrusions informatiques, fraudes au Président, escroqueries aux fournisseurs... qui pourraient avoir un impact sur les livraisons de produits et services à Thales.
- Les incidents cybers qui peuvent se propager aux systèmes et aux réseaux Thales.
- Les failles et vulnérabilités qui pourraient être découvertes sur les produits déjà livrés à Thales.

Utilisez l'unique **point de contact mondial** pour signaler les incidents de cybersécurité susceptibles d'avoir une incidence sur l'une des entités Thales : contactez immédiatement le **Thales CSIRT (Computer Security Incident Response Team)** à [cert@thalesgroup.com](mailto:cert@thalesgroup.com).