Focus : Sécurité des données et cybersécurité | Gouvernance & normes

Gouvernance

Un comité stratégique de sécurité (comité semestriel) a été lancé en 2025, avec la participation du vice-président, responsable de la cybersécurité et du RSSI du groupe, ainsi que des membres du groupe EXCOM. Les principales tâches de ce comité sont les suivantes :

- Donner un aperçu de la cybervie quotidienne via des indicateurs stratégiques clés et un statut sur les principaux projets,
- État de la maturité de la cybersécurité dans le Groupe,
- Examiner l'impact des mesures de cybersécurité mises en œuvre sur les risques,
- Validation des orientations et décisions par le SEVP Opérations & Performance.

Organisation

La direction de la cybersécurité du Groupe (GCD) rassemble la gestion de la sécurité des systèmes d'information/technologies de l'information, des technologies opérationnelles et des produits et solutions, avec pour objectifs stratégiques et opérationnels de fournir et renforcer :

- Une vision unifiée pour la cohérence stratégique,
- Une meilleure gestion des risques,
- Proactivité et résilience contre les cyberattaques,
- Optimisation des ressources et des compétences,
- Accélération de l'innovation sécurisée et de la transformation numérique,
- Facilitation et suivi de la conformité réglementaire,
- Réduction des coûts et optimisation de l'investissement.

Cette cyber-fonction opérationnelle décentralisée renforce la compétitivité de Thales en assurant une cybersécurité intégrée à tous ses systèmes et solutions d'information – tant ceux livrés aux clients que les moyens utilisés pour les construire –, protéger les actifs et transformer la cybersécurité en un moteur de valeur stratégique.

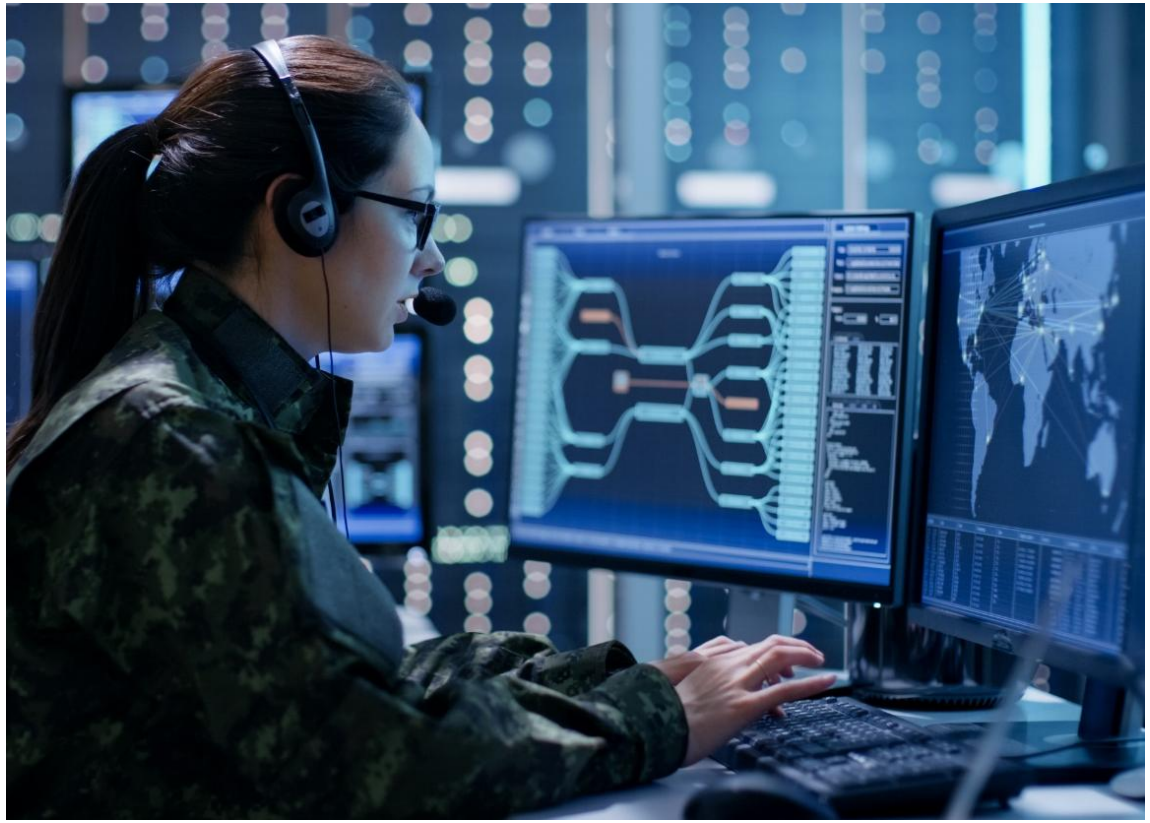
Normes internationales et audits internes

Cette organisation est conçue conformément aux normes et meilleures pratiques reconnues à l'échelle internationale. Elle reflète en particulier les principes :

- Le cadre de cybersécurité du NIST (CSF) ;
- La norme ISO/IEC 27001.

Ces deux cadres sont mis en évidence car ils figurent parmi les plus reconnus au niveau international, tout en restant ouverts à d'autres modèles de référence pour soutenir l'amélioration continue de nos activités de cybersécurité et de nos systèmes de sécurité de l'information.

De plus, les équipes d'audit interne du Groupe effectuent des audits réguliers en interne et avec des partenaires tiers. Thales maintient également un programme mondial d'évaluation des fournisseurs afin de garantir des normes de sécurité cohérentes dans toute la chaîne d'approvisionnement.



Focus : Sécurité des données et cybersécurité | Politiques et programmes

Documents clés

Pour structurer ses efforts en matière de sécurité des données et de cybersécurité, Thales a mis en œuvre plusieurs politiques et directives :

- Mémo organisationel pour la cybersécurité,
- Politique de protection des données personnelles,
- Règles d'entreprise contraignantes (REC) sur les données personnelles,
- Politique de sécurité des systèmes d'information (PSSI),
- Politique de gestion des crises cyber,
- Gouvernance de la cybersécurité pour les produits et solutions,
- 9 règles ou déploiements des fondamentaux de la cybersécurité,
- Processus de cyber-évaluation de la chaîne d'approvisionnement…

De plus, tous les collaborateurs bénéficient d'une orientation et de ressources pour les aider à assumer leurs responsabilités en matière de données, conformément à la charte informatique et à la politique de sécurité du Groupe.

Voir également (site web de Thales):
Règles d'entreprise contraignantes
Politique de protection des données personnelles
Sécurité des données
Protection des données : Comment être conforme aux recommandations de l'ANSSI ?

Académie de formation et de cybersécurité

Programme de formation comprenant des modules d'apprentissage en ligne et des sessions de formation en présentiel couvrant la cybersécurité et la sécurité/protection des données

La Cybersecurity Academy comprend des écoles spécialisées dans les domaines du SI/IT et de la sécurité des produits et solutions, permettant aux équipes et partenaires de Thales de maîtriser l'évolution des défis en matière de cybersécurité grâce à une formation et une certification de pointe.

Chaque collège propose des compétences spécialisées et des parcours d'apprentissage adaptés, en parfaite adéquation avec la stratégie globale du Groupe.

Dans le cadre de l'engagement du Groupe d'être une entreprise apprenante, Thales définit et priorise les compétences essentielles en cybersécurité et met en œuvre une feuille de route triennale en constante amélioration, fondée sur quatre piliers clés : gouvernance et alignement stratégique, formation et certification, communauté et collaboration, et Performance & Cyber Culture. Cette approche structurée garantit le développement durable et l'excellence des capacités de cybersécurité à travers Thales.

Incident de cybersécurité

Une instruction de groupe définit le cadre pour la préparation et la gestion des crises cybernétiques : des exercices de crise sont régulièrement organisés et 5 modules de formation en ligne sont disponibles pour tous les employés du groupe.

Thales supervise le suivi de ses produits, solutions et/ou clients par l'intermédiaire de ses centres d'opérations de sécurité (SOC). Le traitement des incidents est effectué sous l'autorité du CERT. Chez Thales, l'engagement du Groupe envers ses partenaires et clients est de répondre à leurs demandes d'information par le biais d'un point de contact unique, garantissant ainsi la conformité avec les réglementations internationales et locales.

- Le PSIRT est centralement structuré pour coordonner les PSIRT organisés par GBU et par pays, selon nos activités.
- Le CERT et les PSIRTs s'appuient sur une fonction centrale de Cyber Threat Intelligence (CTI) qui fournit une connaissance technique approfondie des menaces pertinentes pour les secteurs industriels desservis par Thales, ainsi que des développements géopolitiques actuels.

Pour plus de détails, veuillez consulter la Computer Emergency Response Team sur le site web de Thales.

Focus : Sécurité des données et cybersécurité | Sécurité des produits du Groupe

Engagement en matière de sécurité des produits

Thales intègre la cybersécurité en tant qu'exigence de conception, de développement, de déploiement et d'exploitation pour ses produits, solutions et services. L'objectif est de protéger les clients du Groupe, leurs opérations et infrastructures critiques contre les risques cyber, tout au long de leur cycle de vie, y compris après livraison (vulnérabilités, correctifs, conseils, mises à jour). Cette ambition s'inscrit dans la stratégie de cybersécurité du Groupe et le positionnement de marque et de marché de Thales, qui reposent sur la CONFIANCE. Dans ce contexte, une gouvernance centrale de la cybersécurité a été créée.

Organisation

Au sein de la Direction de la Cybersécurité du Groupe (GCD), le Responsable de la Sécurité des Produits du Groupe (GPSO) est chargé de définir et piloter la gouvernance de la cybersécurité des produits & solutions Thales..

Il assure une sécurité de bout en bout tout au long du cycle de vie du projet et du produit – de l'offre au déclassement – en établissant des directives, règles et politiques communes, en soutenant leur déploiement et en promouvant les pratiques de sécurité des produits en interne et en externe.

Toutes ces missions sont rendues possible par :

1. En s'appuyant sur le réseau des CPSC (Chefs de la sécurité des produits), CSA (Autorités de cybersécurité), COL (Chefs d'opérations cybernétiques) et Cyber HoD (Chef de discipline cybersécurité) de Thales, tel que décrit dans le document Gouvernance de la cybersécurité pour les solutions du groupe.

En suivant un cadre de sécurité des produits basé sur trois piliers (gouvernance, cycle de vie du développement de solution de bout en bout, cyberassurance) répartis en dix sous-activités qui constituent la « sécurité des produits par Thales ».

3. Fournir un plan directeur dédié sur 3/5 ans (CERBERUS) destiné à alimenter le cadre de sécurité des produits.

Le **Bureau de Sécurité des Produits du Groupe** a été construit sur la base d'un cadre à 3 piliers, **divisé en 10 domaines d'action**

+

Le cadre est alimenté par un **plan directeur défini tous les 5 ans** appelé CERBERUS qui combine la **stratégie de Thales, les tendances mondiales et plusieurs réglementations applicables**

- **C = Cybersécurité** (protection des produits contres les menaces numériques)
- **E = Efficacité** (sur l'ensemble du cycle de vie des solutions)
- **R = Risques** (évaluation des risques et des vulnérabilités pour identifier les mesures d'amélioration)
- **B = Plan directeur** ("Blueprint", définition d'une feuille de route claire pour les PS)
- **E = Education** (prise en compte des aspects humains et du développement des talents)
- **R = Reprise** (garantie d'une reprise rapide et efficace aux incidents et crises de sécurité)
- **U = Unité** (promotion de la collaboration entre tous les départements avec une vision partagée)
- **S = Services** (promouvoir Thales Cyber Services pour lutter contre l'effet de silo)