



Intégration de la cybersécurité dans la Supply Chain

Retour d'expérience du secteur aéronautique

Stéphanie BUSCAYRET (LATECOERE)

État des lieux

- © « La sécurité d'une chaîne qui n'est que celle du maillon le plus faible » trouve un écho naturel dans la Supply Chain aéronautique
- © Pour un donneur d'ordres, plus de 1 800 fournisseurs interconnectés au SI, 22 300 utilisateurs dans 30 pays... Un schéma d'entreprise étendue (EE) à l'échelle mondiale
- © La « digitalisation » des processus de production et des produits augmente la surface d'exposition de manière exponentielle



Toujours les mêmes questions :

Qui accède à quelles données, comment et pour quelles raisons ?





- © Quelle donnée est confiée au tiers ?
 - ✓ Classification des données (par le métier)
- © Dans quelles conditions puis-je externaliser ?
 - ✓ Analyse de risques – contexte (conjointe SI / métier)
 - ✓ Portefeuille fournisseurs qualifiés (SI / achats)
- © Le tiers présente-t-il les garanties appropriées?
 - ✓ Exigences SSI adaptatives dans le contrat (SI / juridique)
 - ✓ Cascade des exigences du client vers les fournisseurs
- © Anticiper la sortie du contrat
 - ✓ Clause de réversibilité – exercice annuel si possible (ensemble)
 - ✓ Anticipation du besoin de continuité de service

La sécurité de l'information, 1^{er} domaine sacrifié

- si la pression des acheteurs est trop forte sur les coûts
- si l'intérêt pour le fournisseur lui-même n'est pas compris



Nos fournisseurs sont des partenaires pour 5, 10 ou même 40 ans !

(Ça tombe bien, créer la confiance prend du temps...)

© Accompagner tout au long de la relation



© Le Plan d'Assurance Sécurité pour élaborer un processus commun

- Porteur de l'analyse du besoin de sécurité (partagé)
- Annexe au contrat (engagement des parties)
- Support du pilotage de la prestation / KPI SSI simples dans les mains du métier
- En évolution permanente (adaptabilité au contexte)

© Animer la relation sur le sujet de la cybersécurité

Co-construire la sécurité dans l'écosystème



- © L'enjeu : garantir le bon niveau de sécurité dans le temps
 - Créer la confiance (facteur humain)
 - Entretenir la dynamique (face à l'évolution de la menace)
 - Accompagner la montée en compétences (pérennité)

- © La seule stratégie possible : jouer collectif pour améliorer la résilience de la chaîne toute entière

AirCyber

La réponse du secteur aéronautique aux enjeux de cybersécurité de la Supply Chain

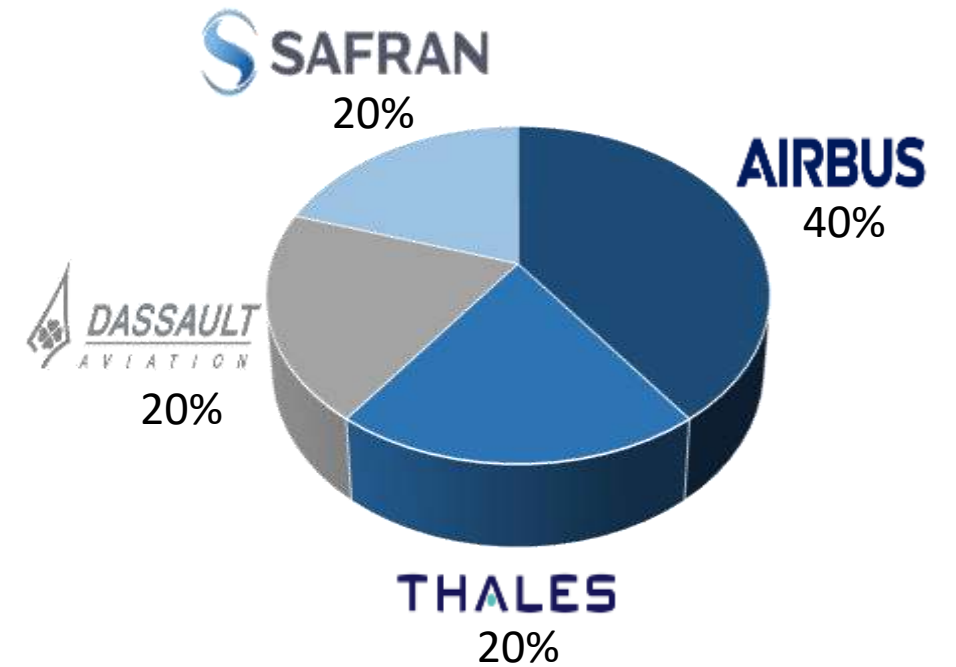
Romain BOTTAN (BoostAeroSpace)



BoostAeroSpace

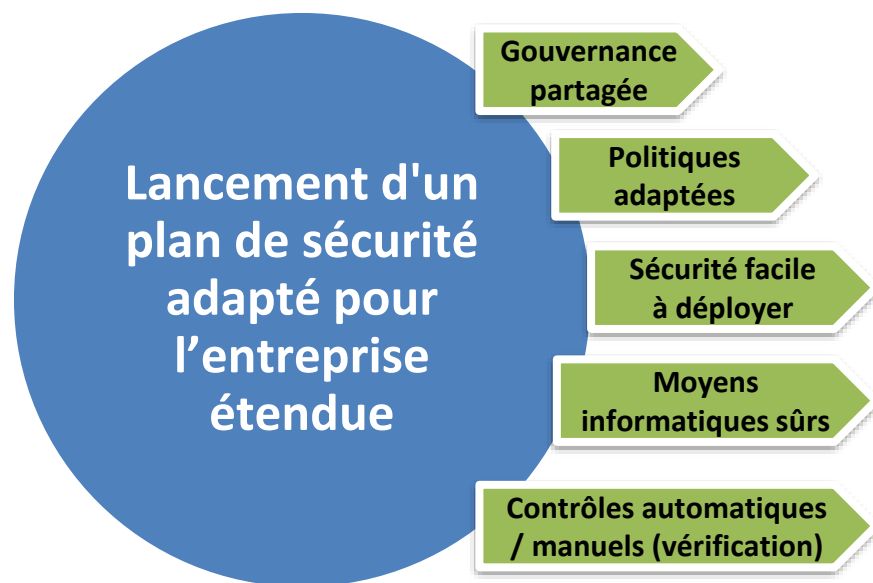
© 4 donneurs d'ordre du secteur Aerospace ont décidé de mettre leurs efforts en commun afin de mieux maîtriser leur Supply Chain, notamment en termes de sécurité

- → **Moyen** : Création d'une structure commune à ces 4 donneurs d'ordres : BoostAeroSpace
- **1 Mission** : Mettre en œuvre les outils collaboratifs, sous forme d'une plateforme numérique, afin d'améliorer la compétitivité et la sécurité de la Supply Chain aérospatiale internationale
- **5 Services** : AirSupply, AirConnect, AirDesign, AirCollab, AirCyber



Objectifs et résultats du projet AirCyber

© Augmenter la sécurité informatique et industrielle et la gestion de crise de la Supply Chain



(Résultat brainstorming sur la sécurité Supply Chain avec les experts des donneurs d'ordres)



© Réduire le coût de la Cybersécurité

- Rédiger des politiques et des règles de sécurité pour tous
- Réduire les investissements via la mutualisation
- Réduire le risque d'"incident"

© Accroître les performances en matière de Cybersécurité

- Partager les connaissances des experts
- Déployer des solutions performantes
- Effectuer des évaluations concrètes
- Couvrir TOUTES les entreprises



© "Services d'évaluation continue de maturité AirCyber"



© Intervention sur site d'aide au questionnaire, rapport de sécurité détaillé, renouvelé tous les 4 ans.
Outil de mise à jour / Dashboard des niveaux

© "Boîte à outils AirCyber" :



© Adaptation des documentations cybersécurité (études, configurations, sensibilisation) issues des donneurs d'ordres



© Catalogue dynamique des services et de solutions cyber reconnues dans la filière (proposé)



© Plan global de sensibilisation et de collaboration cybersécurité (forums, événements, etc.)



© Solution de surveillance & détection d'attaques entièrement compatible avec les OEMs et interconnectée avec les bases de données cybersécurité internationales

Niveaux de Maturité

Aider les fournisseurs à atteindre le niveau de maturité "or" en identifiant les solutions avec les fournisseurs et en les aidant à sécuriser leur IT.

Aider les fournisseurs pour la première étape d'évaluation.



Niveau Or

Contrôles de sécurité automatiques et tableau de bord en temps réel du niveau de sécurité.

Tous les domaines de sécurité sécurisés avec des cyber-solutions validées.

Aero – niveau des OEMS

Niveau Argent

Audit technique effectué, mesures correctives déployées.

Solutions déployées (utilisation sécurisée d'Internet, chiffrement des données, détection d'attaques, sécurité des PC / smartphone / serveur (hardening), authentification forte)

ANSSI "Hygiène" "avancés"

Niveau Bronze

Solutions de sécurité minimales déployées (gestion des correctifs, Antivirus, pare-feu, sensibilisation et formation des utilisateurs, anti-spam, chiffrement des disques).

ANSSI "Hygiène" "élémentaires"

Évaluation du niveau

Création et communication des documentations sécurité des fournisseurs.

Auto-évaluation par les fournisseurs de leur niveau (questionnaire + visite)

Roadmap projet AirCyber

