AirCyber Rapport

Date d'export: 03-07-2026
Entreprise: Integris Composites S.A.S.
Pas encore validé
Version: 1.9

Sommaire

1. Présentation générale de l'entreprise 4

2. Niveau de maturité général au 03-07-2026 7

2.1 Définition des niveaux 7

2.2 Estimation des niveaux de l'entreprise 7

3. Appréciation générale ADVENS 9

4. Niveau de maturité bronze par domaine de securité 13

4.1 Niveau de risque global du niveau bronze 13

4.2 Recommandations pour atteindre un niveau de maturité 100% Bronze 16

5. Niveau de maturité silver par domaine de securité 18

5.1 Niveau de risque global du niveau silver 18

5.2 Recommandations pour atteindre un niveau de maturité 100% Silver 20

6. Niveau de maturité gold par domaine de securité 25

6.1 Niveau de risque global du niveau gold 25

6.2 Recommandations pour atteindre un niveau de maturité 100% Gold 27

7. Catalogue Aircyber 32

8. Annexes 33

8.1 Niveau bronze 33

8.2 Niveau silver 37

8.3 Niveau gold 41

1. Présentation générale de l'entreprise

Nom	Integris Composites S.A.S.
Activité	Développement et fabrication de protections balistiques en matériaux composites pour personnes, véhicules et aéronefs. Dans l'aéronautique, elle équipe avions et hélicos.
Connexion AirSupply	N/A
Clients	OEM Airbus Helicopter, OEM DGA, OEM Leonardo, OEM Rockwell-Collins France, OEM Safran, OEM Thales, OEM Safran Aircraft & Engines, OEM Daher, OEM Latecoere
Site analysé	Integris Composites S.A.S.-38270
Autres sites	Integris Composites A/S (Danemark); Integris CompositesLtd. (UK); Integris Composites B.V. (NL)
Chiffre d’affaire	46,00

Données Informatiques

Utilisateurs	N/A
Nombre de PC	N/A
Budget Informatique (%)	N/A
% du budget informatique dédié à la cybersécurité	15.0

Département informatique

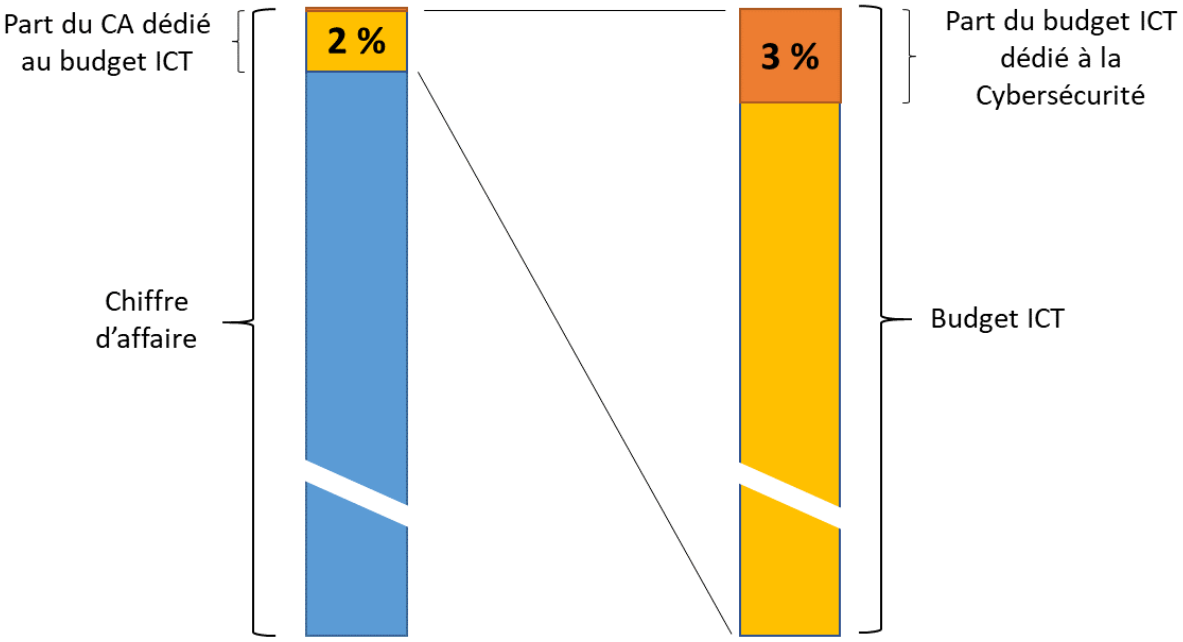
Équipe informatique	inconnu
Équipe sécurité	inconnu

Budget

L’analyse réalisée et mise à jour par BoostAeroSpace au regard du déploiement d'AirCyber a permis d’estimer un budget informatique et Cybersécurité minimum permettant d'augmenter et d'atteindre les objectifs de la filière (AirCyber Gold) ainsi qu'un budget Cybersécurité pour maintenir ce niveau.

- **Pour augmenter le niveau de cybersécurité de l'entreprise**, le budget de cybersécurité est généralement de 10 à 20 % du budget informatique, (0,2 à 0,4 % du chiffre d'affaires en considérant un budget informatique fixé à 2% du chiffre d'affaires). Ce calcul est applicable à partir d'un Chiffre d'Affaires de 25 Millions d'€, **toute entreprise avec un Chiffre d'Affaires inférieur à 25M€ devrait appliquer ce seuil de 50K€ par an** jusqu'à atteindre le niveau Gold.

- **Pour maintenir le niveau Gold**, une entreprise devrait consacrer 3% de son budget informatique à la Cybersécurité (0.06% du Chiffre d'Affaires en considérant un budget informatique fixé à 2% du Chiffre d'Affaires). Comme pour le budget d'augmentation, le budget de maintien est associé à **un minimum de 15K€ pour une entreprise dont le chiffre d'affaires est inférieur à 25 millions d'euros**. Cette estimation a été établie pour un fonctionnement nominal et ne prend pas en compte d’éventuels investissements nécessaires à la mise en place de nouveaux éléments de sécurité informatique.



Dans le cadre de l’évaluation d’AirCyber, BoostAeroSpace a comparé (lorsqu’ils étaient communiqués) les budgets ICT et Cybersécurité de l’entreprise évaluée avec cette estimation afin de permettre à l’entité de situer son niveau d’investissement.

Aucune information sur le budget Cybersécurité n’a été communiqué par l’entreprise, il n’est donc pas possible de comparer ce dernier avec l’état de l’art

2. Niveau de maturité général au 03-07-2026

2.1 Définition des niveaux

Les différents niveaux de maturité (Bronze, Silver et Gold) ont été définis sur les bases des recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information ("guide d'hygiène[1]") et des bonnes pratiques déployées par les industriels fondateurs de BoostAeroSpace.

Ces 3 niveaux sont formellement répartis de cette manière:

- **BRONZE**: Règles d'hygiène informatiques de bases de l'ANSSI "niveau standard". Déploiement simple des solutions (52 exigences).
- **SILVER**: Règles d'hygiène informatiques de bases de l'ANSSI "niveau avancé". Automatisation, industrialisation des solutions mises en place (48 exigences).
- **GOLD**: Mesures au même niveau de protection que les fondateurs de BoostAeroSpace (Détection des attaques et fuite d'information, Centralisation des solutions, suivi actif, maintiens et contrôle des solutions à distance par une équipe centrale spécialisée (27 exigences).

Pour chaque niveau, une liste d'exigences a été dressée. Le résultat indique le % d'exigences atteintes par niveau, ainsi le score de chaque niveau est sur 100%. Les exigences des niveaux supérieurs sont généralement des exigences antérieures en plus automatisées/centralisées, c'est pourquoi certaines exigences Silver ou Gold peuvent être validées alors que l'ensemble de celles du niveau inférieur ne sont pas encore validées.

L'objectif du projet BoostAeroSpace AirCyber est d'aider l'ensemble des Fournisseurs industriels à atteindre le Niveau Gold sur les 4 prochaines années, via, dans un premier temps cet état des lieux du niveau actuel puis via des recommandations et un ensemble de solutions et services référencés (voir programme complet pour plus de détails www.boostaerospace.com/aircyber).

Un premier catalogue de solutions référencées ainsi que l'ensemble des critères d'évaluation des niveaux avec les solutions et recommandations associées ont normalement été délivrées avec ce présent document, BoostAeroSpace invite l'industriel à s'en inspirer pour atteindre le niveau Gold.

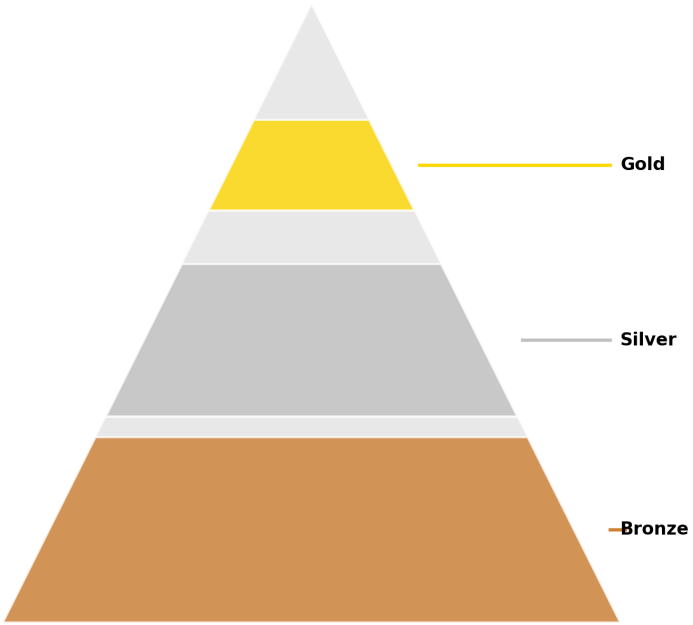
(1) https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique

2.2 Estimation des niveaux de l'entreprise

Ce rapport ayant été rédigé à partir d'une liste finie d'éléments recueillis de manière ponctuelle d'autres risques et d'autres forces peuvent exister dans l'entreprise analysée.

Malgré le fait que ce rapport a été rédigé avec la meilleur volonté possible, les personnes et entreprises impliquées dans la rédaction de ce rapport se doivent d'exclure leur responsabilité sur des faiblesses ou des non conformités au référentiel qui n'auraient pas été identifiées. Les résultats de ce rapport ne libèrent en aucun cas l'entreprise analysée de ses obligations de cybersécurité contractuelles avec ses clients (par exemple, dans le cas d'Airbus de la conformité avec l'A1015), d'obligations légales et de réduire les risques cyber que l'entreprise fait courir à ses clients dans la limite de leurs res-ponsabilités. Dans tous les cas, l'entreprise reste en totalité responsable des mesures cyber qu'elle choisit d'appliquer et de la réduction du risque associé. Les auteurs déclinent toute responsabilité concernant l'utilisation correcte ou incorrecte des informations con-tenues dans ce rapport.

	Bronze	Silver	Gold
Niveau de conformité	**90%** **4 actions à traiter**	**74%** **12 actions à traiter**	**44%** **15 actions à traiter**



3. Appréciation générale ADVENS

Nota:
Cette évaluation ne peut être prise pour une certification légitime ni remplacer les labels actuels ou l'évaluation faite par les fondateurs de BAS pour leurs fournisseurs/

Situation actuelle

Integris Composites possède un niveau de sécurité élevé au regard du référentiel AirCyber.
Integris Composites est un acteur industriel spécialisé dans la conception et la fabrication de solutions de protection balistique, couvrant des usages variés tels que les équipements de protection individuelle (plaques pour gilets pare-balles), les véhicules, les aéronefs et les plateformes navales. Le groupe opère dans un contexte international structuré, avec des entités en Europe, en Asie et en Amérique du Nord, et un centre de R&D partagé principalement entre la France et le Danemark, où sont hébergées des solutions critiques de simulation. En France, la branche aéronautique constitue une spécificité différenciante, intégrant des activités de test avec des infrastructures dédiées.
Afin de répondre aux demandes de marché de plus en plus importantes, le marché demande que Integris Composites soit conforme avec le programme AirCyber et établisse un plan d’action pour atteindre un niveau convenable de sécurité des systèmes d’informations.
L’entreprise évolue dans un environnement fortement contraint par les exigences de la Défense, notamment via le dispositif DiagCyber de la DGA, et inscrit ses investissements cybersécurité dans une logique de conformité et de co-financement public. Elle s’appuie sur une certification ISO 9001 ainsi que sur le référentiel Cyber Essentials+ pour structurer sa démarche de sécurité et répondre aux attentes de ses partenaires stratégiques.
La gouvernance cybersécurité repose sur une organisation distribuée, avec un RSSI en France appuyé par un homologue au Danemark et un responsable applicatif basé à Amsterdam. La dimension de l’équipe IT implique une priorisation des chantiers et une coordination étroite avec le groupe. Des décisions structurantes sont pilotées au niveau danois, notamment pour les infrastructures, les outils de sécurité et le SOC, induisant des enjeux d’alignement et d’harmonisation des pratiques entre entités.
Le système d’information est fortement interconnecté à l’échelle internationale via des liaisons VPN reliant les différents sites (Danemark, France, États-Unis, Singapour, Royaume-Uni, Pays-Bas). L’Active Directory est commun entre la France et le Danemark, avec une prédominance des technologies Microsoft, notamment pour les environnements collaboratifs (O365) et l’ERP. Les infrastructures critiques, dont certaines applications de conception issues de l’éditeur Dassault, sont majoritairement hébergées on-premise, en particulier pour les activités sensibles. En

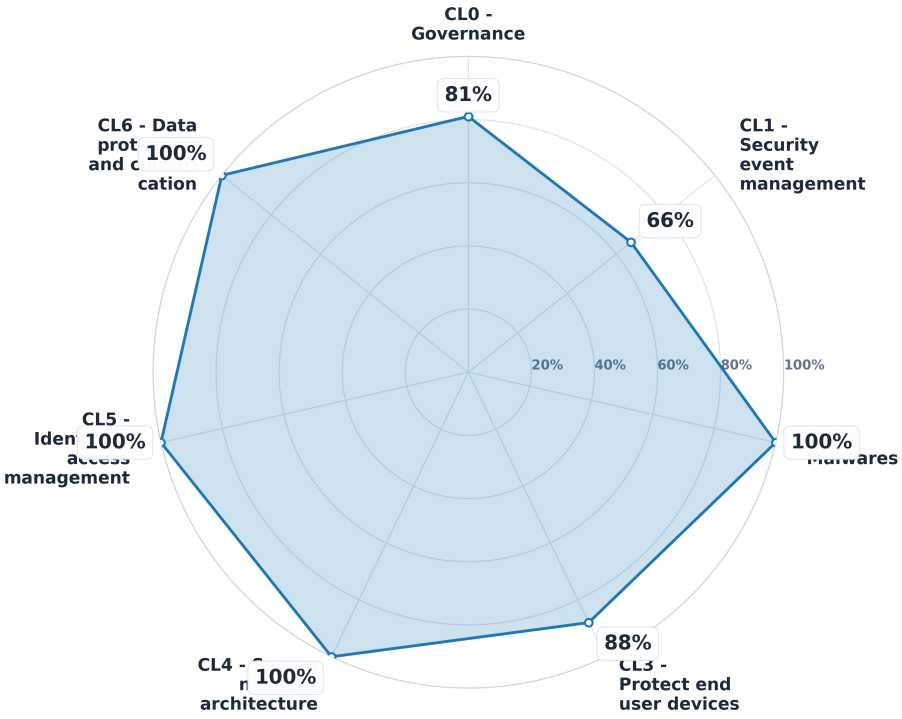
France, l’architecture reste partiellement segmentée, avec des projets en cours pour structurer des VLAN distincts selon les usages, tandis que le Danemark présente une maturité plus avancée sur ces aspects. Le parc comprend environ deux cents utilisateurs et une trentaine d’applications, avec une croissance continue liée aux activités industrielles et aux projets transverses.
Les environnements industriels et bureaux d’études sont étroitement liés, notamment via des flux de données techniques nécessaires à la production. Les postes de conception et de développement coexistent sur les mêmes réseaux, avec des mécanismes de cloisonnement logique par répertoires sécurisés. L’entreprise exploite plusieurs serveurs locaux pour des usages spécifiques (paie, gestion documentaire, collecte de données de production), complétés par des infrastructures centralisées au Danemark. La gestion des accès physiques repose sur des dispositifs de badge et de contrôle d’intrusion, avec des projets d’amélioration en cours, notamment pour répondre aux exigences de sécurité des environnements sensibles et classifiés. La présence d’un officier de sécurité et de zones sécurisées dédiées aux informations sensibles illustre la prise en compte des contraintes liées aux activités Défense.
La posture de cybersécurité s’appuie sur plusieurs mesures structurantes : généralisation du MFA pour l’ensemble des applications, déploiement d’outils EDR et SOC, journalisation centralisée partielle, et stratégie de sauvegarde multi-niveaux incluant réplication, externalisation et tests réguliers de PRA. Des tests de reprise sont réalisés de manière semestrielle afin de valider la résilience des systèmes critiques. En parallèle, des audits réguliers (pentests internes et externes) viennent renforcer l’identification des vulnérabilités.
Enfin, l’entreprise a engagé plusieurs initiatives pour renforcer sa maturité : programmes de sensibilisation obligatoires à l’arrivée des collaborateurs, campagnes de phishing, formalisation d’une PSSI et de procédures associées, ainsi que déploiement de solutions de classification et de gestion documentaire. Des projets structurants sont en cours ou planifiés, tels que la modernisation de la gestion des actifs, l’extension de la segmentation réseau, et le renforcement des dispositifs de supervision et de journalisation afin d’atteindre un niveau de cybersécurité cohérent avec les exigences de ses clients et partenaires industriels.
De ce fait, il est important, compte tenu du contexte de l’entreprise, de sa taille et de son activité industrielle spécifique, de définir au mieux les besoins de sécurité afin de cadrer une approche de gestion des risques cohérente et efficiente.
Parmi les mesures de sécurité mises en œuvre, nous pouvons citer :
• Les journaux des composants sont analysés en temps réel ;
• Un SOC est contractualisé ;
• Les postes de travail et leurs périphériques des utilisateurs sont surveillés via l'EDR ;
• Les connexions aux équipements sensibles utilisent une authentification forte ;
• Les dispositifs de détection d'attaque cyber sont régulièrement mis à jour ;
• Lorsqu'un incident survient dans la production, une investigation est réalisée afin d'identifier si cet incident pourrait être causé par un élément malveillant ;

• L'organisation est certifiée en matière de cybersécurité ;
• Lors d'une embauche, les employés suivent une sensibilisation à la cybersécurité.
Malgré tout, des écarts significatifs sont à mentionner avec le référentiel AirCyber. Nous devons mettre en avant un certain manque de dispositifs de sécurité et de suivi des bonnes pratiques aggravant les risques d'intrusion, d'altération et de vols des données.
Gouvernance :
• La conformité des filiales de l'entreprise n'est pas régulièrement vérifiée avec des visites sur site ;
• Aucune analyse de risques cyber sur les activités de l'entreprise n'est réalisée, empêchant une révision annuelle du niveau de risque de l'entreprise ;
• Aucun service de CERT n'est contractualisé ;
• Aucune solution informatisée pour la gestion du risque permettant de manière plus ou moins automatisée de remonter le niveau de risque cyber et de le traiter n'est déployée.
Gestion des événements de sécurité :
• Le puit de log, ne permet pas de centraliser et de conserver, au moins un an, les journaux des composants critiques (Accès internet, pare-feu, accès ERP, ...) ;
• Les journaux des authentifications des administrateurs sur les serveurs, équipements d'infrastructure et postes de travail, ne sont pas conservés un an ;
• Aucune procédure décrivant l'enregistrement et la configuration des journaux des composants critiques (accès internet, pare-feu, accès à l'ERP, etc.) n'est formalisée ;
• Aucun test annuel d'une procédure de gestion de problème de sécurité permettant d'être assuré de pouvoir réagir rapidement et d'impliquer les bonnes personnes internes ou externes.
Malware :
• Aucune sondes réseau afin de détecter les activités malicieuses ou anormales n'est déployée ;
• Aucune solution de navigation sécurisée pour la consultation des sites internet non-professionnels n'est déployée.
Protection des terminaux des utilisateurs :
• Absence d'un cloisonnement entre l'environnement de production industriel et les autres environnements ;
• Aucune personne ou un département qualifié dédié à la conception, l'exploitation, et la surveillance des équipements ICS n'est nommé ;
• Aucune procédure pour gérer le cycle de vie des ICS n'est formalisée.
Architecture réseau sécurisée :
• Aucune solution de détection et de surveillance des nouveaux équipements sur le réseau interne n'est déployée ;
• Les connexions non autorisées au réseau ne sont pas automatiquement bloquées ;
• Aucun réseau dédié et cloisonné pour l'administration des ICS ;
• Aucun réseau wifi de production dédié et isolé du réseau principal.
Gestion des identités et des accès :
• Aucun cloisonnement du réseau à travers par exemple des VLAN d'administration.

Classification des données et prévention des fuites de données :
• Aucune plateforme d'échange de fichiers sécurisée entre les sous-traitants et fournisseurs n’est déployée ;
• Aucun processus de protection des données pouvant inclure une solution de détection de fuite de données confidentielles, les rôles et responsabilités des employés vis-à-vis de ces données n’est formalisé ;
• Aucune solution de classification automatique des données de l'entreprise n’est mise en place ;
• La documentation relative à la conception, aux composants et à l'exploitation des ICS n’est pas stockée au niveau de sécurité approprié.
Ces manques font courir un risque cybersécurité moyen à l’entreprise. Il apparait donc nécessaire de mettre en place les actions détaillées ci-dessous.
De ce fait, un certain nombre de projets est déjà identifié et planifié cette année :
• Cloisonner entièrement le réseau à travers par exemple des VLAN d'administration ;
• Utiliser systématiquement une plateforme d'échange de fichiers sécurisée entre les sous-traitants et fournisseurs.

4. Niveau de maturité bronze par domaine de securité

Pour le premier niveau de maturité (Bronze), le graphique ci-dessous représente le % d'exigences validées, classées par domaines de sécurité.



4.1 Niveau de risque global du niveau bronze

L'entreprise a un niveau de maturité estimé à 90 % du niveau bronze, ce qui signifie que la majorité des mesures de base ont été prises (48 sur 52). L'effort à mettre en place pour atteindre le niveau bronze complet (4 requis manquants) est raisonnable. Le niveau de risque est considéré comme : bas.

L'entreprise a un niveau de maturité estimé à 92% du niveau bronze, ce qui signifie que la majorité des mesures de base ont été prises (47 sur 51). L'effort à mettre en place pour atteindre le niveau bronze complet (4 requis manquants) est raisonnable. Le niveau de risque est considéré comme : bas

Récapitulatif de l'état des mesures de sécurité observées associées au niveau minimum (Bronze)

Mis en place

1.1 - Les accès aux bâtiments, bureaux et installations informatiques sont contrôlé et limité aux personnes approuvées.
1.2 - L'enceinte des salles serveurs et locaux techniques est surveillée et protégée.
1.4 - Les visiteurs sont accompagnés en permanence dans les locaux.
2.1.1 - Un schéma réseau complet de votre système d'information est maintenu.
2.2 - La liste du parc informatique est mise à jour régulièrement.
2.3 - Un service affecté à la gestion du système informatique est en place.
2.4 - Un référent en sécurité des systèmes d’information est présent.
2.4.1 - Une politique de sécurité de l'information et des directives associées sont en place et communiquées à l'ensemble des utilisateurs et des responsables projet.
2.5 - L'ensemble des postes de travail (serveurs, PC portable, PC de bureau) est sécurisé d'une manière homogène.
2.6 - Un anti-virus est implémenté sur l'ensemble du parc.
2.8.1 - Les smartphones d'entreprise ont une politique de sécurité dédiée.
2.9.4 - Le serveur AD est durcis.
2.10 - Une politique de sauvegarde automatique des composants critiques est définie et appliquée avec une procédure de restauration testée.
2.11 - Des règles concernant le comportement des utilisateurs vis-à-vis des périphériques qu'ils pourraient brancher sur leurs ordinateurs sont définies (interdire de brancher une clé usb trouvée par hasard, faire un scan antivirus des clés des partenaires, ne pas brancher n'importe quel accessoire sur son pc…).
3.1.1 - Les antécédents des employés sont vérifiés avant leur embauche quand nécessaire en fonction de leur rôle prévu au sein de l'entreprise.
3.1.2 - Lorsque des contraintes de sécurité ont été identifiées, les antécédents et l'adéquation du profil des nouveaux embauchés sont vérifiés.
3.2 - Aucun compte utilisateur ne dispose de droit administrateur.
3.3 - L'entreprise dispose d'un inventaire exhaustif des comptes d'administration.
3.5 - Les utilisateurs sont sensibilisés aux bonnes pratiques de la sécurité informatique.
3.6 - Les utilisateurs ont à leur disposition des moyens de sécurité informatique liés aux déplacements sur leur PC portable.
4.1 - Une procédure d'entrée et de départ concernant les utilisateurs et administrateurs est en place.
4.2 - L'installation des logiciels sur ordinateur ne peut se faire que par le biais d'un compte admin nécessitant une authentification différente ou via une demande au support informatique utilisateurs.
4.3 - Les mots de passe stockés sur les systèmes sont protégés (chiffrement).
4.4 - Une politique de gestion des mots de passe est définie.
4.4.1 - Les mots de passe et identifiants par défaut du parc informatique sont modifiés
4.5 - Les composants (excepté les équipements réseaux) du parc informatique sont régulièrement mis à jour.

4.6 - La fin de la maintenance des logiciels et systèmes est anticipée.
4.6.1 - L'ensemble des versions des logiciels installés sur le parc informatique est vérifié.
4.9 - L'entreprise a en place un processus d'escalade et d'alerte des incidents de sécurité.
4.10 - Des flux d'actualité des nouvelles failles cyber sont suivis.
5.2 - Des équipements de sécurité sont utilisés pour protéger et cloisonner le réseau interne.
5.2.1 - Des firewall sont utilisés sur les postes clients.
5.2.2 - La configuration des firewall est contrôlée.
5.3 - Des règles de sécurité permettant l'interdiction ou l'avertissement de protocoles utilisées non chiffrés sont en place.
5.8 - Tous les équipements connectés au système d'information de l'entreprise ont fait l'objet d'une procédure formelle et préalable d'approbation.
5.11 - L'accès Wifi "visiteur" est isolé du reste du réseau de l'Entreprise.
5.13 - Une solution permettant le filtrage des e-mails est en place.
5.17 - Un VPN est utilisé pour l'accès à distance.
6.1 - Les données importantes sont sauvegardées régulièrement.
6.4 - Les disques durs des ordinateurs portables et smartphones sont chiffrés automatiquement.
6.6 - Des audits de sécurité réguliers sont réalisés.
6.8 - Un moyen de chiffrement des données sensibles envoyées à l'extérieur de l'entreprise est à disposition.
6.9 - Une politique de classification des données en fonction de leur usage (public, confidentiel entreprise, confidentiel…) est en place ainsi que des règles de protection des données sont définies.
6.10 - Les données de l'entreprise sont associées à des responsables identifiés.
7.1.1 - Une cartographie du système industriel contenant les éléments les plus sensibles est formalisée et mise à jour.
7.6 - Un programme de sensibilisation aux bonnes pratiques de sécurité des ICS est réalisé
7.7 - La charte d'utilisation est signée par les utilisateurs des systèmes contrôle d'automatisation industrielle
Ext24 - Des processus de décommissionnement sont en place avant la mise au rebut des actifs.

A améliorer

1.7 - Réaliser régulièrement des visites pour vérifier la sécurité physique et informatique des différents sites géographiques.
2.9.3 - Formaliser une procédure décrivant l'enregistrement et la configuration des journaux des composants critiques (accès internet, pare-feu, accès à l'ERP, etc.).
7.0 - Cloisonner l'environnement de production industriel avec les autres environnements.

9.8 - Réaliser une analyse de risques cyber sur les activités de l'entreprise.
Ext53 - Créer un réseau wifi de production dédié et isolé du réseau principal.

4.2 Recommandations pour atteindre un niveau de maturité 100% Bronze

Sont listés ci-dessous les prérequis restants à valider pour atteindre le niveau BRONZE. Ils sont classés par criticité:

- High: à traiter sous 6 mois.
- Medium: à traiter sous 1 an.
- Low: à traiter sous 1 an et demi.

High bronze (6 mois après validation du MA)

Issue: 1.7

Rule: [CL0.7-B] Verify compliance of entities, subsites

Notice:

Aircyber: S'assurer que les politiques de sécurité ainsi que les processus déployés soit appliqués dans les entités ou sous-entités.

Issue: 7.0

Rule: [CL3.1-B] ICS network segregation

Notice:

AirCyber: La séparation du réseau informatique utilisé par les systèmes industriels est critique à plusieurs titres, ne serait-ce que par la valeur des biens à protéger et par la difficulté à maintenir à jour et donc sécurisés les équipements industriels.
Il est par conséquent nécessaire d'effectuer une première séparation simple des réseaux informatiques bureautique et industriels, de sorte que la communication entre ces deux réseaux soit rendue impossible, ou alors extrêmement restreinte à une liste d'équipements bien identifiés. L'objectif immédiat est d'éviter qu'un poste de travail bureautique, infecté, puisse infecter à son tour les machines du réseau industriel.
La configuration sur des réseaux logiques différents est une première étape, l'utilisation de réseaux logiques VLAN est également une bonne première solution.
L'évolution vers la mise en place d'équipements dédiés de ségrégation réseau de type firewall, la mise en place de passerelles Internet dédiées et sécurisées pour la maintenance à distance occasionnellement autorisée est également une bonne pratique.

Medium bronze (1 an après validation du MA)

Issue: 2.9.3

Rule: [CL1-B] inventory log sources on ICT sensitive systems

Notice:

AirCyber : Etablir un processus pour répertorier les journaux (logs) générés par les systèmes et les équipements informatiques critiques (par ex, les pare-feux, les points d'accès internet, les serveurs applicatifs), et pour les archiver pendant un an.

ANSSI : "Disposer de journaux pertinents est nécessaire afin de pouvoir détecter d’éventuels dysfonctionnements et tentatives d’accès illicites aux composants du système d’information. Les évènements critiques pour la sécurité doivent être journalisés et gardés pendant au moins un an (ou plus en fonction des obligations légales du secteur d’activités).
Précisions TPE/PME: Il existe de nombreux produits/solutions proposant des solutions de management des logs adaptées au contraintes des TPE et PME.

Low bronze (1 an et demi après validation du MA)

Issue: 9.8

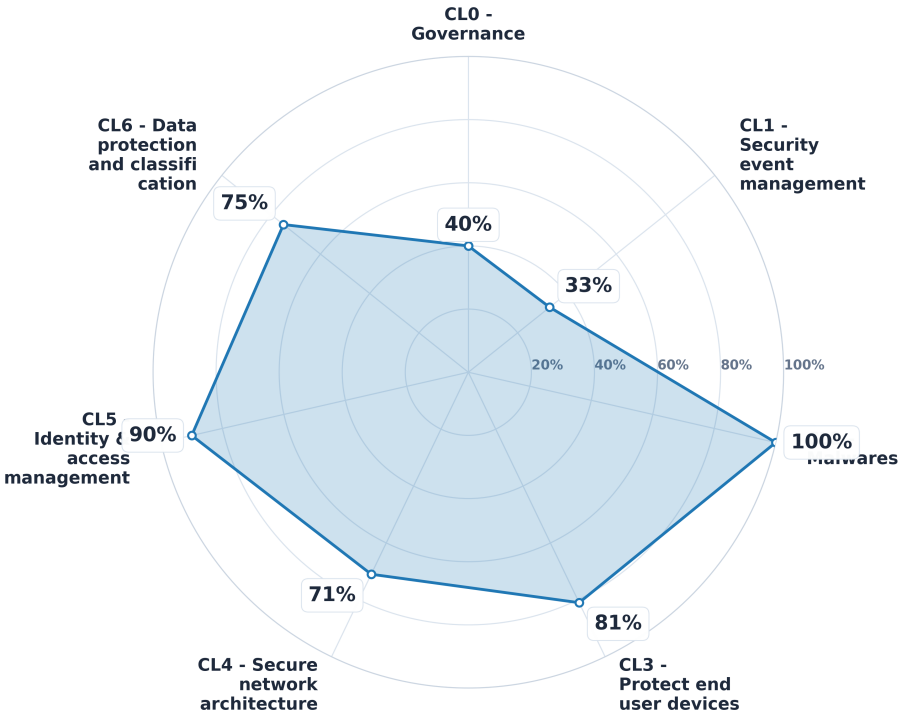
Rule: [CL0.6-B] Setup a risk analysis

Notice:

AirCyber: S'aider d'un expert en cybersécurité pour effectuer une analyse de risque de son système d'information, avec une méthode adaptée à la taille de son entreprise. Il est également crucial de bien identifier les risques résiduels une fois les mesures de sécurité implémentées.
ANSSI: "La démarche recommandée consiste, dans les grandes lignes, à définir le contexte, apprécier les risques et les traiter. L’évaluation de ces risques s’opère généralement selon deux axes : leur probabilité d’apparition et leur gravité. S’ensuit l’élaboration d’un plan de traitement du risque à faire valider par une autorité désignée à plus haut niveau. La méthode EBIOS référencée par l’ANSSI est recommandée. Elle permet d’exprimer les besoins de sécurité, d’identifier les objectifs de sécurité et de déterminer les exigences de sécurité."

5. Niveau de maturité silver par domaine de securité

Pour le premier niveau de maturité (Silver), le graphique ci-dessous représente le % d’exigences validées, classées par domaines de sécurité.



5.1 Niveau de risque global du niveau silver

L'entreprise a un niveau de maturité estimé à 74 % du niveau silver, ce qui signifie que plus de la moitié des mesures de base ont été prises (35 sur 47). L'effort à mettre en place pour atteindre le niveau silver complet (12 requis manquants) est conséquent. Le niveau de risque est considéré comme : moyen.

L'entreprise a un niveau de maturité estimé à 72% du niveau silver, ce qui signifie que plus de la moitié des mesures de base ont été prises (34 sur 47). L’effort à mettre en place pour atteindre le niveau silver complet (13 requis manquants) est conséquent. Le niveau de risque est considéré comme : moyen

Récapitulatif de l'état des mesures de sécurité observées associées au niveau minimum (Silver)

Mis en place

1.3 - L'enceinte des locaux est surveillée et protégée.
1.5 - Un onduleur est en place.
1.6 - Une politique de bureau propre est en place.
2.1 - L'entreprise dispose d'un inventaire complet de son parc informatique.
2.5.1 - L'ensemble des smartphones est sécurisé d'une manière homogène.
2.7 - Un anti-virus est implémenté sur l'ensemble du parc informatique permettant de détecter et supprimer les programmes malveillants sur signature.
2.8 - Les smartphones d'entreprise sont gérés par l'équipe informatique.
2.8.2 - Une solution de MDM est en place.
2.9.5 - La configuration de la journalisation de l'active directory est en place.
3.1 - Chaque employé dispose d'un identifiant informatique nominatif.
3.3.1 - La sécurité des comptes administrateurs est contrôlée.
3.4 - Les équipes opérationnelles sont formés à la sécurité des systèmes d'information.
4.2.1 - Les comptes utilisateurs sont gérés de façon centralisée et sécurisée.
4.6.2 - Une liste des logiciels autorisés et interdits est formalisée.
4.7 - Une veille est en place sur les alertes des éditeurs et des avis de sécurité de l'ANSSI.
4.8.1 - L'entreprise a mis en place un SIEM.
4.9.1 - Des solutions sur les postes de travail et serveurs de type IDS et IPS sont déployés.
5.1 - Les serveurs les plus sensibles du parc informatique sont identifiés du service informatique.
5.4 - L'authentification forte pour la connexion aux e-mails d'entreprise depuis internet est en place.
5.5.1 - L'entreprise utilise des fonctionnalités SSO.
5.6.1 - Des protections sont en place sur les postes de travail permettant d'éviter que les utilisateurs puissent ouvrir des réseaux internet sans sécurité.
5.7 - Des protections sont en place vis à vis des menaces relatives à l'utilisation de supports amovibles.
5.8.1 - L'entreprise a un contrôle total sur l’environnement professionnel des applications d'entreprise / données sur les appareils mobiles.
5.9 - Les accès à internet sont filtrés par un serveur mandataire (proxy).
5.10 - Une surveillance du trafic Internet est en place.
5.10.1 - Toutes les connexions entre les différents sites de la société sont chiffrés et filtrés.
5.12 - L'accès Wifi est sécurisé avec une séparation des usages.
5.13.1 - Les utilisateurs ont la possibilité de chiffrer facilement le contenu des E-mails.
5.14 - Les interconnexions réseau avec les sous-traitants et fournisseurs sont sécurisés.
6.2 - Les sauvegardes sont protégées.

6.6.2 - Les règles des Firewalls sont revues régulièrement.
6.7.1 - Des tests d'intrusion du site web sont réalisés.
7.1.2 - Les sauvegardes des OS des système d'information industriel les plus sensibles sont réalisées. (Sauvegarde de la configuration de la machine, du code source, des données, etc.)
7.3 - Le processus de gestion des crises comprenant l'environnement industriel est formalisé (reprise d'activité de la production après un crash système).

A améliorer

2.9 - Mettre en place un puit de log, permettant de centraliser, de conserver (au moins un an) et de configurer les journaux des composants critiques (Accès internet, pare-feu, accès ERP, ...).
2.9.2 - Activer et garder pendant un an les journaux des authentifications des administrateurs sur les serveurs, équipements d'infrastructure et postes de travail.
4.8.5 - Bloquer automatiquement les connexions non autorisées au réseau.
5.6 - Cloisonner entièrement le réseau à travers par exemple des VLAN d'administration.
5.14.1 - Utiliser systématiquement une plateforme d'échange de fichiers sécurisée entre les sous-traitants et fournisseurs.
5.15 - Déployer des dispositifs permettant d'autoriser la connexion au réseau qu'aux appareils identifiés et gérés par le système d'information.
6.6.1 - Vérifier la conformité des filiales de l'entreprise régulièrement.
7.4 - Stocker avec niveau de sécurité approprié la documentation relative à la conception, aux composants et à l'exploitation des ICS.
7.8 - Formaliser et mettre en place des procédures pour gérer le cycle de vie des ICS.
7.10 - Définir une architecture ainsi que des règles de gestion spécifiques aux ICS.
7.11 - Réaliser des audits de conformité technique de sécurité annuellement sur les processus de changements des solutions dédiées de l'IACS.
9.8.1 - Réviser annuellement le niveau de risque cyber de l'entreprise.

5.2 Recommandations pour atteindre un niveau de maturité 100% Silver

Sont listés ci-dessous les prérequis restants à valider pour atteindre le niveau SILVER. Ils sont classés par criticité:

- High: à traiter sous 6 mois après le niveau Bronze.
- Medium: à traiter sous 1 an après le niveau Bronze.
- Low: à traiter sous 1 an et demi après le niveau Bronze.

High silver (6 mois après le niveau Bronze)

Issue: 5.6

Rule: [CL5-S] Dedicated and compartmentalized network for information system administration

Notice:

AirCyber : déployer une politique de comptes admin temporaire afin de sécuriser au maximum le réseau. Faire un audit de configuration avec un intérêt particulier sur la gestion de l'identité et les accès à haut privilèges.
ANSSI: "Un cloisonnement physique des réseaux dèsque cela est possible est recommandé."

Issue: 7.10

Rule: [CL3-S] ICS : Secure industrial network & devices access from company network

Notice:

AirCyber: Le réseau informatique "industriel" est une des parties les plus sensibles pour une entreprise. Il faut donc veiller à particulièrement protéger ce réseau. Pour ce faire, il doit être ségrégué du reste du réseau informatique de l'entreprise (pare-feu...). De plus les droits informatiques de ce réseau doivent être limité aux stricts besoins ainsi que les accès à internet.

Issue: 7.11

Rule: [CL0.2-S] Industrial IT : Audit the change processes, and dedicated IACS solutions

Notice:

AirCyber: Effectuer des tests d'étanchéité du système, à travers l'utilisation des outils de test ou d'une prestation de pentest.

Issue: 7.4

Rule: [CL6-S] ICS : documentation for design, components and operation

Notice:

AirCyber: Le réseau informatique "industriel" est une des parties les plus sensibles d'une entreprise industrielle, et doit de ce fait bénéficier d'une attention particulière

et d'une politique de sécurité dédiée. La description détaillée du réseau industriel doit être documentée et mise à jour régulièrement, au minimum à chaque ajout d'un nouveau composant. Le réseau industriel doit être au maximum séparé du réseau bureautique et mettre en place des mécanismes d'isolation des différents équipements qui le composent (VLAN, Sous Réseaux, Firewalls), et l'accès à Internet vers ou depuis les éléments du réseau industriel doit être restreint au maximum. Les éléments d'un réseau industriel doivent être vus comme des sources potentielles d'infection du réseau (risque lié à la connexion / mise à jour par le vendeur de l'élément) autant qu'être une cible difficile à sécuriser par configuration qu'il faut protéger au maximum, parfois en ajoutant un équipement en coupure réseau devant ce dernier (risque lié à l'impossibilité de modifier la configuration sécurité de l'équipement industriel).
ANSSI: Les systèmes industriels utilisent aujourd’hui abondamment les technologies de l’information alors qu’ils n’ont pas été conçus pour faire face aux menaces qu’elles introduisent. De nombreuses bonnes pratiques sont similaires à celles de l’informatique de gestion, mais leur mise en œuvre est à adapter aux contraintes du domaine industriel. Contrôle d’accès physique aux équipements et aux bus de terrain, Cloisonnement des réseaux, Gestion des médias amovibles, Gestion des comptes (accès logique, authentification), Durcissement des configurations, Gestion des journaux d’événements et d’alarmes, Gestion des configurations, Sauvegardes / restaurations, Documentation, Protection antivirale, Mise à jour des correctifs (planification), Protection des automates, Stations d’ingénierie, postes de développement.

Issue: 7.8

Rule: [CL3-S] ICS : specific patch management

Notice:

AirCyber: Le réseau informatique "industriel" est une des parties les plus sensibles pour une entreprise. Il faut donc veiller à particulièrement protéger ce réseau. Pour ce faire, la mise en place d'une politique rigoureuse de mise à jour des systèmes est nécessaire.

Issue: 9.8.1

Rule: [CL0.6-S] Risk management process (reviewed yearly)

Notice:

AirCyber Advanced : Une fois une analyse de risque réalisée sur le système d'information de l'entreprise, le niveau supérieur consiste à mettre à jour et revoir de façon périodique (au moins annuel) cette analyse.

Medium Silver (1 an après le niveau Bronze)

Issue: 4.8.5

Rule: [CL4-S] Detect / block unauthorized connection to network

Notice:

ANSSI: "Des mesures techniques telles que l’authentification des postes sur le réseau peuvent être déployées (par exemple à l’aide du standard 802.1X ou d’un équivalent)."

Issue: 5.14.1

Rule: [CL6-S] Secure exchange platform access with suppliers and subcontractors to exchange sensitive data

Notice:

ANSSI: "Pour des besoins opérationnels, une entité peut être amenée à établir une interconnexion réseau dédiée avec un fournisseur ou un client. Il convient d’établir un tunnel site à site, de préférence IPsec, en respectant les préconisations de l’ANSSI. Le partenaire étant considéré par défaut comme non sûr, il est indispensable d’effectuer un filtrage IP à l’aide d’un pare-feu au plus près de l’entrée des flux sur le réseau de l’entité. La matrice des flux (entrants et sortants) devra être réduite au juste besoin opérationnel, maintenue dans le temps et la configuration des équipements devra y être conforme. "Précisions TPE/PME: certaines solutions anti-virus offrent ce genre de fonctionnalités qui, selon l'envergure du SI de l'entreprise, peuvent être suffisantes.

Issue: 6.6.1

Rule: [CL0.6-S] Verify compliance of entities

Notice:

ANSSI: " Il est important de vérifier régulièrement la conformité de l'entreprise afin qu'elle réponde aux règles de sécurité informatique définies par l'entreprise. Cela peut être vérifié par des audits de conformité."

Low silver (1 an et demi après le niveau Bronze)

Issue: 2.9

Rule: [CL1-S] Centralized secure log collection system from the different ICT sensitive sources

Notice:

AirCyber : Afin d'avoir une vue d'ensemble sur les logs, mettre en place un outil centralisant les logs et permettant de les analyser est nécessaire.
Précisions TPE/PME: Il existe de nombreux produits/solutions proposant des solutions de management des logs adaptées au contraintes des TPE et PME.
ANSSI: "Une centralisation des journaux sur un dispositif dédié pourra être envisagée. Cela permet de faciliter la recherche automatisée d'événements suspects, d'archiver les journaux sur une longue durée et d'empêcher un attaquant d'effacer d'éventuelles traces de son passage sur les équipements qu'il a compromis."

Issue: 2.9.2

Rule: [CL1-S] logs check for admin accounts usage

Notice:

AirCyber : Collecter les logs des comptes admins sur les serveurs.
ANSSI: "Les mécanismes d'audit des événements concernant les comptes d'administration doivent être mis en œuvre. En particulier, les journaux suivants doivent être activés: ouvertures/fermetures de session; verrouillage des comptes; gestion des comptes; gestion des groupes de sécurité."

Issue: 5.15

Rule: [CL4-S] Detect any new device connected to the network.

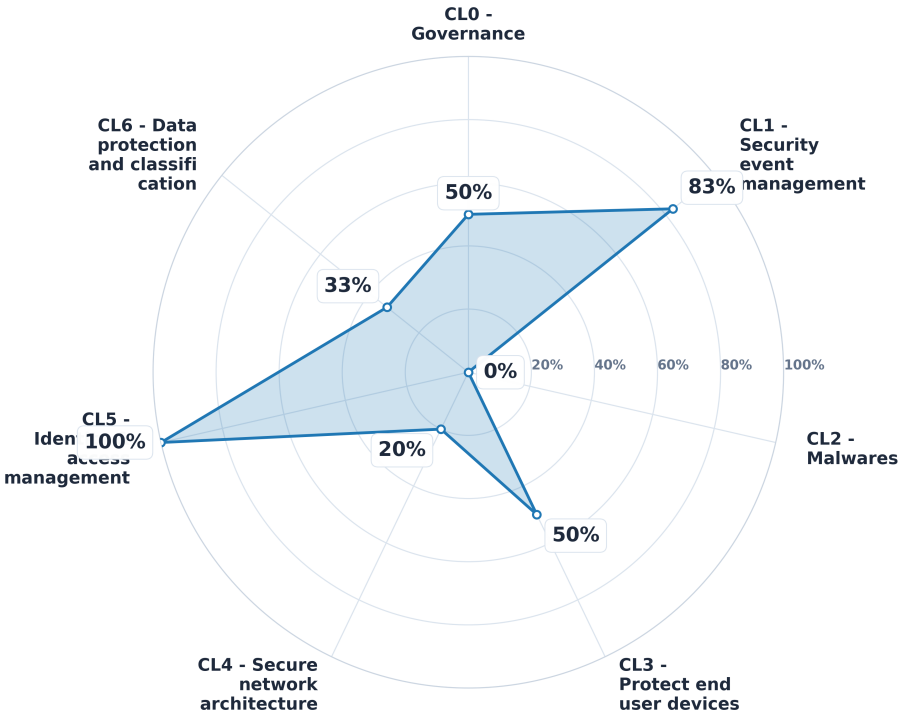
Notice:

AirCyber: De la même manière qu'il est important de détecter les nouvelles connexions sur le réseau, les entreprises devraient aujourd'hui être en mesure de détecter les connexions de tout nouvel appareil ou dispositif afin de se prémunir des actions malveillantes.

---

6. Niveau de maturité gold par domaine de securité

Pour le premier niveau de maturité (Gold), le graphique ci-dessous représente le % d’exigences validées, classées par domaines de sécurité.



6.1 Niveau de risque global du niveau gold

L'entreprise a un niveau de maturité estimé à 44 % du niveau gold, ce qui signifie que moins de la moitié des mesures de base ont été prises (12 sur 27). L'effort à mettre en place pour atteindre le niveau gold complet (15 requis manquants) est important mais atteignable. Le niveau de risque est considéré comme : moyen.

L'entreprise a un niveau de maturité estimé à 44% du niveau gold, ce qui signifie que moins de la moitié des mesures de base ont été prises (12 sur 27). L’effort à mettre en place pour atteindre le niveau gold complet (15 requis manquants) est important mais atteignable. Le niveau de risque est considéré comme : moyen

Récapitulatif de l'état des mesures de sécurité observées associées au niveau minimum (Gold)

Mis en place

2.9.1 - Les journaux des composants sont analysés en temps réel.
3.5.1 - Lors d'une embauche, les employés suivent une sensibilisation à la cybersécurité.
4.8 - Un SOC est contractualisé.
4.8.2 - Les postes de travail et leurs périphériques des utilisateurs sont surveillés via l'EDR.
4.8.3 - L'entreprise a en place un outil d'alerte permettant d'exécuter un arrêt automatique lors d'un cas d'incident majeur.
5.5 - Les connexions aux équipements sensibles utilisent une authentification forte.
6.3 - L'entreprise utilise une solution de stockage cloud.
6.7 - Des tests d'intrusion (pentest) réguliers sur le SI sont réalisés.
6.7.2 - Les dispositifs de détection d'attaque cyber sont régulièrement mis à jour.
7.12 - Un processus de surveillance des menaces et des vulnérabilités sur les composants ICS est formalisé et suivi.
7.13 - Un service SOC ou équivalent est contractualisé ou mis en place. Il permet de surveiller de manière active le réseau et ainsi détecter les incidents de sécurité des équipements industriel.
7.14 - Lorsqu'un incident survient dans la production, une investigation est réalisée afin d'identifier si cet incident pourrait être causé par un élément malveillant
Ext29 - L'organisation est certifiée en matière de cybersécurité.

A améliorer

2.1.2 - Automatiser la cartographie réseau.
2.1.3 - Déployer une solution de détection et de surveillance des nouveaux équipements sur le réseau interne.
4.8.4 - Contractualiser ou mettre en place un centre de supervision du réseau permettant la détection des incidents de sécurité (NOC, Network Operations Center).
4.8.6 - Déployer et superviser des sondes réseau afin de détecter les activités malicieuses ou anormales.
4.11 – Contractualiser un service de CERT.
5.10.2 - Déployer une solution de navigation sécurisée pour la consultation des sites internet non-professionnels.
6.5 - Formaliser et déployer un processus de protection des données pouvant inclure une solution de détection de fuite de données confidentielles, les rôles et responsabilités des employés vis-à-vis de ces données.
6.9.1 - Mettre en place une solution de classification automatique des données de l'entreprise.
6.9.2 - Utiliser une solution de prévention de fuite de données.
7.1.3 - Tester régulièrement les sauvegardes des équipements industriels.
7.2 - Mettre à jour régulièrement la documentation, la nomenclature et les schémas des équipements ICS.

7.5 - Nommer une personne ou un département qualifié dédié à la conception, l'exploitation, et la surveillance des équipements ICS.
7.9 - Utiliser un réseau dédié et cloisonné pour l'administration des ICS.
9.7.1 - Formaliser et tester au moins annuellement une procédure de gestion de problème de sécurité permettant d'être assuré de pouvoir réagir rapidement et d'impliquer les bonnes personnes internes ou externes.
9.8.2 - Déployer une solution informatisée pour la gestion du risque permettant de manière plus ou moins automatisée de remonter le niveau de risque cyber et de le traiter.

6.2 Recommandations pour atteindre un niveau de maturité 100% Gold

Sont listés ci-dessous les prérequis restants à valider pour atteindre le niveau GOLD. Ils sont classés par criticité:

- High: à traiter sous 6 mois après le niveau Silver.
- Medium: à traiter sous 1 an après le niveau Silver.
- Low: à traiter sous 1 an et demi après le niveau Silver.

High gold (6 mois après le niveau Silver)

Issue: 2.1.3

Rule: [CL4-G] Automatic HW inventory tool centralized and new device detection.

Notice:

Aircyber Advanced : L'inventaire matériel centralisé du parc informatique doit permettre de détecter tout nouvel équipement grâce à une observation du réseau et de notifier régulièrement des événements sécurité liés à ces détections.

Issue: 4.11

Rule: [CL0.6-G] Automatic vulnerability detection plus threat intelligence regarding cyber threat, attacks and vulnerabilities from all sources

Notice:

AirCyber: il est nécessaire pour bien surveiller le niveau de menace cybersécurité de souscrire à des services de veille sécurité appelés CERT. Ces services offrent une veille sur la sécurité de l'entreprise, souvent également une veille sur les attaques qui pourraient survenir en écoutant les forums illégaux, ainsi que de manière plus basique des alertes sécurités adaptées à l'entreprise, son secteur industriel et aux équipements informatiques qu'elle à déployée.

Issue: 5.10.2

Rule: [CL2-G] secure internet access to non- categorized websites or personal

Notice:

ANSSI : Des mécanismes complémentaires sur le serveur mandataire pourront être activés selon les besoins de l'entité : analyse antivirus du contenu, filtrage par catégories d'URLs, etc. Le maintien en condition de sécurité des équipements de la passerelle est essentiel, il fera donc l'objet de procédures à respecter. Suivant le nombre de collaborateurs et le besoin de disponibilité, ces équipements pourront être redondés. Par ailleurs, pour les terminaux utilisateurs, les résolutions DNS en direct de noms de domaines publics seront par défaut désactivées, celles-ci étant déléguées au serveur mandataire. Enfin, il est fortement recommandé que les postes nomades établissent au préalable une connexion sécurisée au système d'information de l'entité pour naviguer de manière sécurisée sur le Web à travers la passerelle.

Issue: 6.5

Rule: [CL6-G] data lost prevention solutions with central management of data confidentiality solutions

Notice:

AirCyber : Le vol de données est aujourd'hui une réelle arme pour les attaquants. il convient donc de se prémunir en déployant des solutions qui surveillent et analysent tout comportement anormal afin, au cas échéant, de bloquer par exemple un vol de données. Ces solutions sont intimement reliées à la classification des données. Précisions TPE/PME: certaines solutions anti-virus offrent ce genre de fonctionnalités qui, selon l'envergure du SI de l'entreprise, peuvent être suffisantes.

Issue: 6.9.1

Rule: [CL6-G] Data tagging and data labelling

Notice:

AirCyber: Lorsque la classification des données est mise en place en entreprise il est nécessaire de fournir aux utilisateurs les moyens informatique pour les aider à marquer les documents, et ceci avec des solutions les plus automatisées possible afin de réduire la contrainte coté utilisateur.

Issue: 6.9.2

Rule: [CL6-G] Automatic encryption of data classified as confidential when sent outside company (e-mail, USB key…)

Notice:

AirCyber: Associée à la classification effective des données (marquage qu'une donnée est confidentielle par exemple), la mise en place d'outils permettant d'interdir à des données confidentielles de sortir du système d'information sans une protection adéquate est une très bonne mesure pour réduire le risque de fuite de données sensibles en entreprise.

Issue: 7.2

Rule: [CL4-G] ICS : mapping of the company network

Notice:

AirCyber: les mêmes règles de cartographie réseau et d'identification des serveurs critiques doivent être appliqués au réseau industriel.
ANSSI: "Créer et maintenir à jour un schéma simplifié du réseau (ou cartographie) représentant les différentes zones IP et le plan d’adressage associé, les équipements de routage et de sécurité (pare-feu, relais applicatifs, etc.) et les interconnexions avec l’extérieur (Internet, réseaux privés, etc.) et les partenaires. Ce schéma doit également permettre de localiser les serveurs détenteurs d’informations sensibles de l’entité."

Issue: 7.5

Rule: [CL3-G] ICS : Set IT specific standard & governance

Notice:

AirCyber : "Le réseau informatique "industriel" est une des parties les plus sensibles pour une entreprise. Il faut donc veiller à particulièrement protéger ce réseau. Pour ce faire, la mise en place d'une gouvernance et de règles spécifiques est nécessaire.

Issue: 7.9

Rule: [CL4-G] ICS : dedicated and compartmentalized network for the administration

Notice:

AirCyber: Le réseau informatique "industriel" est une des parties les plus sensibles pour une entreprise. Il faut donc veiller à particulièrement protéger ce réseau. Pour ce faire, il doit être ségrégué du reste du réseau informatique de l'entreprise (pare-feu…). De plus les droits informatiques de ce réseau doivent être limité aux stricts

besoins. Le parc industriel doit avoir des moyens de protection dédiés à l'instar des moyens mis en place globalement sur le SI du fait de la spécificité des SI industriels (OS non maintenu, par exemple)

Issue: 9.7.1

Rule: [CL1-G] Escalation and alerting process with Security hotline

Notice:

AirCyber Advanced : En plus d'une procédure de gestion des évènements critiques, mettre en place un process centralisé d'alerting et de réaction en cas d'incident est un plus.

Issue: 9.8.2

Rule: [CL0.6-G] Continuous risk assessment with central tool generating KPI presented to management level

Notice:

AirCyber: Avoir un indicateur du niveau de risque de son entreprise mis à jour très régulièrement en fonction des différents évènements cybersécurité qui surviennent dans son système est primordial pour réagir face à des évènements cyber en appliquant les bonnes mesures de gestion de risque. Plusieurs outils de gestion de risque, ou certaines solutions de surveillance informatique apportent les briques nécessaires à alimenter des tableaux de bords permettant des prises de décisions qualifiées.

Medium gold (1 an après le niveau Silver)

Issue: 2.1.2

Rule: [CL4-G] Live / automatic update of the company network map

Notice:

AirCyber : Afin de garantir une sécurité de bout en bout du SI, il est important de disposer d'un outil qui met à jour en temps réel la cartographie du réseau de manière à pouvoir identifier les failles ou, le cas échéant, la porte d'entrée d'une potentielle cyber attaque.
Précisions TPE/PME: Certains anti virus proposent des fonctionnalités de ce type.

Issue: 7.1.3

Rule: [CL6-G] ICS : Setup distinct physical sites for backup storage

Notice:

AirCyber : Le fournisseur doit tester regulièrement la bonne restoration de sauvegarde.

Low gold (1 an et demi après le niveau Silver)

Issue: 4.8.4

Rule: [CL2-G] Central Network cyber incidents monitoring

Notice:

AirCyber Advance : Mettre en place des sondes sur le réseau permettant de détecter toute activité anormale et de remonter des alertes

---

Issue: 4.8.6

Rule: [CL2-G] Network traffic abnormal behavior monitoring

Notice:

AirCyber: Établir, mettre en œuvre, exploiter et surveiller des sondes de détection réseau communes pour détecter les activités malveillantes ou les utilisations anormales.

---

7. Catalogue Aircyber

En tant qu'adhérents au programme AirCyber vous avez accès au catalogue de solutions et services cyber. Inscrivez-vous ou créez un compte ici lien. Vous pourrez explorer les solutions cyber utilisées par les OEM et les fournisseurs industriels de l’industrie Aérospatiale, créer votre propre liste de produits et services cyber et référencer les solutions qui n'ont pas encore été ajoutées.

8. Annexes

8.1 Niveau bronze

Niveau	Domaine	Question	Réponse
Bronze	CL5 - Identity & access management	1.1 Les accès à vos bâtiments, bureaux et installations informatiques sont-ils contrôlés et limités (par exemple par l'utilisation de portes verrouillées, de lecteurs de cartes magnétiques, de dispositifs de prévention, de détection et d'intervention en cas de vol, etc.) ?	Oui
Bronze	CL5 - Identity & access management	1.2 L'enceinte de vos salles serveurs et locaux techniques est-elle sécurisée par une clôture, une barrière à l'entrée, une vidéosurveillance , et une alarme ?	Oui
Bronze	CL5 - Identity & access management	1.4 Les visiteurs sont-ils accompagnés en permanence dans vos locaux ?	Oui
Bronze	CL0 - Governance	1.7 Si vous avez plusieurs sites géographiques informatiques effectuez-vous des visites pour vérifier la sécurité physique et informatique régulièrement (min. 1 fois tous les 2 ans)	Non
►vincent.badinier@advens.fr		Aucune visite physique réellement réalisée sur le site du Danemark.	
Bronze	CL4 - Secure network architecture	2.1.1 Avez-vous un schéma réseaux complet de votre société ?	Oui
Bronze	CL6 - Data protection and classification	2.10 Définissez-vous et appliquez-vous une politique de sauvegarde automatique des composants critiques avec une procédure de restauration testée?	Oui
Bronze	CL3 - Protect end user devices	2.11 Avez-vous définit des règles concernant le comportement des utilisateurs vis-à-vis des périphériques qu'ils pourraient brancher sur leurs ordinateurs (interdire de brancher une clé usb trouvée par hasard, faire un scan antivirus des clés des partenaires, ne pas brancher n'importe quel accessoire sur son pc...)?	Oui
Bronze	CL4 - Secure network architecture	2.2 La liste de votre parc informatique est-il mis à jour régulièrement ? (serveurs, PC de bureau, PC portable, imprimantes, équipements réseaux, smartphones, etc.)	Oui
Bronze	CL0 - Governance	2.3 Existe-t-il une personne ou un département affecté à la gestion du système informatique ?	Oui
Bronze	CL0 - Governance	2.4 Avez-vous un référent en sécurité des systèmes d'information (RSSI ou équivalent) ?	Oui

Niveau	Domaine	Question	Réponse
Bronze	CL0 - Governance	2.4.1 Votre organisation a-t-elle mis en place une politique de sécurité de l'information et des directives associées ? Les communiquez-vous à l'ensemble des utilisateurs et des responsables projet ?	Oui
Bronze	CL3 - Protect end user devices	2.5 Utilisez-vous un outil pour vous assurer que l'ensemble de vos postes de travail (serveurs, PC portable, PC de bureau) sont sécurisés d'une manière homogène (politiques de sécurité identiques entre les postes, gestion des écarts, etc.)	Oui
Bronze	CL2 - Malwares	2.6 Avez-vous implémenté un outil de détection des programmes malveillants (antivirus) sur l'ensemble du parc informatique bureautique et sur les serveurs ?	Oui
Bronze	CL3 - Protect end user devices	2.8.1 Les smartphones d'entreprise ont-ils une politique de sécurité dédiée ?	Oui
Bronze	CL1 - Security event management	2.9.3 Utilisez-vous une procédure pour implémenter l'enregistrement des journaux des composants les plus importants comme les firewall, les accès internet ?	Non
Bronze	CL4 - Secure network architecture	2.9.4 Sécurisez-vous la configuration par défaut de votre serveur Active Directory (AD) et gardez-vous au moins pendant un an les logs avec les informations d'authentification sur l'AD? (Durcissement du système d'exploitation (restreindre les protocoles et services exécutés, interdire l'accès internet direct depuis le serveur, désactiver les comptes par défaut) et du paramétrage du service Active Directory (AD en lecture seule, validation des politiques, des règles de sécurité des postes de travail gérés via l'AD, restriction et sécurisation des mots de passe des comptes à privilèges...).	Oui
Bronze	CL0 - Governance	3.1.1 Effectuez-vous une vérification de la nationalité, des antécédents des employés avant leur embauche quand nécessaire (par exemple : demande casier judiciaire, prise de références), en fonction de leur rôle prévu au sein de l'entreprise (par exemple personnel sénior, personnel informatique, personnel d'entretien) ?	Oui
Bronze	CL0 - Governance	3.1.2 Lorsque des contraintes de sécurité ont été identifiées, habilitation requise par exemple, vérifiez-vous les antécédents et l'adéquation du profil des nouveaux embauchés (casier judiciaire/nationalité) ?	Oui
Bronze	CL5 - Identity & access management	3.2 Confirmez-vous que les comptes affectés aux utilisateurs pour accéder et utiliser le système d'information (ordinateur, serveur, cloud) ne disposent pas de droits administrateur (les administrateurs peuvent modifier les paramètres de sécurité, installer des logiciels et des périphériques et accéder à tous les fichiers de l'ordinateur) ?	Oui
Bronze	CL3 - Protect end user devices	3.3 Disposez-vous d'un inventaire exhaustif des comptes à privilèges (d'administration) et le maintenez-vous à jour ?	Oui

Niveau	Domaine	Question	Réponse
Bronze	CL0 - Governance	3.5 Sensibilisez-vous les utilisateurs aux règles, bons comportements à adopter et consignes de sécurité de l'information régissant l'activité quotidienne ?Ceci est-il confirmé par la signature d'une charte des systèmes d'information précisant les règles, et consignes cybersécurité qu'ils doivent respecter, ou un équivalent juridiquement opposable (comme annexe règlement intérieur, contrat de travail)?	Oui
Bronze	CL6 - Data protection and classification	3.6 Les utilisateurs ont-ils à leur disposition des moyens de sécurité informatique liés aux déplacements sur leur PC portable? (Filtre écran, câble de sécurité, VPN, chiffrement, surveillance,...)	Oui
Bronze	CL5 - Identity & access management	4.1 Existe-t-il une procédure d'entrée et de départ concernant les utilisateurs et administrateurs ?	Oui
Bronze	CL1 - Security event management	4.10 Avez-vous souscrit à un flux d'actualité vous informant des nouvelles failles cybersécurité et d'alertes cybersécurité comme ceux proposés par les CERT gouvernementaux (ANSSI FR, NIST US), les sites de veille sécurité internationaux ?	Oui
Bronze	CL5 - Identity & access management	4.2 Faut-il des droits d'administration nécessitant une authentification différente avec un compte admin ou un support informatique aux utilisateurs pour installer des logiciels sur leurs ordinateurs ?	Oui
Bronze	CL5 - Identity & access management	4.3 Protégez-vous les mots de passe stockés sur les systèmes (chiffrement) ?	Oui
Bronze	CL5 - Identity & access management	4.4 Existe-t-il une politique de gestion des mots de passe (fréquence de mise à jour, contraintes minimum de sécurité, caractères spéciaux, nombre de caractères, politique spécifique pour les profils administrateurs...) ?	Oui
Bronze	CL4 - Secure network architecture	4.4.1 Changez-vous les mots de passe et identifiants par défaut du parc informatique ?	Oui
Bronze	CL4 - Secure network architecture	4.5 Faites-vous régulièrement des mises à jour des composants (serveurs, PC de bureau, PC portable, imprimantes , équipements réseaux, smartphones, etc..) sur votre parc informatique ?	Oui
Bronze	CL4 - Secure network architecture	4.6 Anticipez-vous la fin de la maintenance des logiciels et systèmes ?	Oui
Bronze	CL3 - Protect end user devices	4.6.1 Afin d'éviter les failles potentielles (logiciel inconnu, non mis à jour...) vérifiez-vous les versions des logiciels installés sur votre parc informatique ?	Oui

Niveau	Domaine	Question	Réponse
Bronze	CL1 - Security event management	4.9 Existe-t-il des processus d'escalade et d'alerte des incidents de sécurité ?	Oui
Bronze	CL3 - Protect end user devices	5.11 Avez-vous un accès Wifi "visiteur" isolé du reste du réseau de l'Entreprise ? (Connexion spécifique, Wifi dédié ?)	Oui
Bronze	CL2 - Malwares	5.13 Existe-t-il un système de filtrage des E-mails ? (Anti-spam, suppression des fichiers joints suspects, etc...)	Oui
Bronze	CL5 - Identity & access management	5.17 Pour l'accès à distance à votre système d'information (utilisateurs nomades ou d'astreinte, sites distants, actions de maintenance préventives ou correctives) avez-vous systématiquement mis en place une solution de sécurité garantissant une identification et une authentification forte de l'utilisateur (VPN associé à de la MFA, identifiant/mot de passe personnels, uniques et incessibles, certificats, ...) ?	Oui
Bronze	CL4 - Secure network architecture	5.2 Utilisez-vous des équipements de sécurité pour protéger et cloisonner votre réseau interne. (Firewall, proxy, etc.) ?	Oui
Bronze	CL3 - Protect end user devices	5.2.1 Utilisez-vous un firewall sur les postes clients ? (PC portable, PC de bureau) ?	Oui
Bronze	CL3 - Protect end user devices	5.2.2 Contrôlez-vous la configuration des firewall au moins une fois par an ?	Oui
Bronze	CL4 - Secure network architecture	5.3 Avez-vous une architecture réseau privilégiant les communications sécurisées et n'autorisant que de manière exceptionnelle les communications non-sécurisées en les isolant du reste du réseau. Par exemple, encourager les communications chiffrées et interdire les protocoles non sécurisés (ex : configurer les pare-feu réseau et sur les postes de travail/serveurs pour interdire le protocole telnet-23 dans le réseau local, l'utilisation de partages Windows via Samba v1, l'authentification NTLMv1, etc.) ?	Oui
Bronze	CL4 - Secure network architecture	5.8 Tous les équipements (ordinateur, tablette, smartphone), connectés au système d'information de l'entreprise ont-ils fait l'objet d'une procédure formelle et préalable d'approbation ?	Oui
Bronze	CL6 - Data protection and classification	6.1 Les données importantes sont-elles sauvegardées régulièrement ?	Oui
Bronze	CL6 - Data protection and classification	6.10 Avez-vous défini que les données de votre entreprise devaient être associées à des responsables identifiés et leurs responsabilités (données des RH, données du bureau d'étude, etc.)	Oui

Niveau	Domaine	Question	Réponse
Bronze	CL6 - Data protection and classification	6.4 Chiffrez-vous les disques durs des ordinateurs, smartphones sans aucune interaction des utilisateurs (chiffrage automatique transparent) ?	Oui
Bronze	CL0 - Governance	6.6 Procédez-vous à des audits de sécurité réguliers (applicatif, réseau, processus), puis appliquez-vous les actions correctives associées ?	Oui
Bronze	CL6 - Data protection and classification	6.8 Avez-vous à disposition les moyens et outils nécessaires pour chiffrer les données sensibles envoyées à l'extérieur de l'entreprise ?	Oui
Bronze	CL6 - Data protection and classification	6.9 Définissez-vous une politique de classification des données en fonction de leur usage (public, confidentiel entreprise, confidentiel...) et des règles de protection à appliquer à ces données ?	Oui
Bronze	CL3 - Protect end user devices	7.0 Mettez-vous en place un cloisonnement entre l'environnement de production industriel et les autres environnements (qualification, pré-production, systèmes d'information entreprise, etc.) ?	Non
Bronze	CL6 - Data protection and classification	7.1.1 Avez-vous effectué une cartographie de votre système d'information industriel en identifiant les éléments le plus sensibles?	Oui
Bronze	CL0 - Governance	7.6 Existe-t-il un programme de sensibilisation ou de formation en matière de sécurité des ICS pour les employés et sous-traitants ?	Oui
Bronze	CL0 - Governance	7.7 Les utilisateurs, automaticiens et administrateurs des systèmes contrôle d'automatisation industrielle (IACS) ont-ils signés une charte d'utilisation et de bonnes pratiques cybersécurité ?	Oui
Bronze	CL0 - Governance	9.8 Avez-vous déjà effectué une analyse de risque cyber sur votre entreprise ?	Non

8.2 Niveau silver

Niveau	Domaine	Question	Réponse
Silver	CL5 - Identity & access management	1.3 L'enceinte de vos locaux est-elle sécurisée par des gardiens avec une surveillance de nuit, une barrière à l'entrée, une vidéosurveillance et une alarme ?	Oui
Silver	CL5 - Identity & access management	1.5 Utilisez-vous des onduleurs ou des batteries de secours (pour assurer l'alimentation en cas de coupure de courant) ?	Oui
Silver			Oui

Niveau	Domaine	Question	Réponse
	CL5 - Identity & access management	1.6 Avez-vous une politique de bureau (physique et verrouillage écran) propre pour les papiers et les supports de stockage amovibles sensibles ?	
Silver	CL4 - Secure network architecture	2.1 Avez-vous un inventaire complet et à jour de votre parc informatique ? (serveurs, PC de bureau, PC portable, imprimante , équipements réseaux, smartphones, etc..)Disposez-vous d'un inventaire précis et à jour des actifs (poste de travail, serveur...) entrant dans la production de vos clients ?	Oui
Silver	CL3 - Protect end user devices	2.5.1 Utilisez-vous un outil pour vous assurer que l'ensemble de vos smartphones sont sécurisés d'une manière homogène (politiques de sécurité identiques entre les postes, gestion des écarts, etc.)	Oui
Silver	CL2 - Malwares	2.7 Avez-vous implémenté un outil de suppression ou de mise en quarantaine des programmes malveillants basé sur la détection de comportement (EDR) sur l'ensemble du parc informatique ?	Oui
Silver	CL3 - Protect end user devices	2.8 Les smartphones d'entreprise sont-ils gérés par votre équipe informatique ? (par exemple : configuration des mots de passe et de la politique des anti-virus)	Oui
Silver	CL3 - Protect end user devices	2.8.2 Les smartphones d'entreprise sont-ils gérés de manière centrale avec un outil permettant de contrôler leur configuration, état de sécurité ?	Oui
Silver	CL1 - Security event management	2.9 Disposez-vous d'une solution centralisée pour activer, conserver (au moins un an) et configurer les journaux des composants les plus importants comme les firewalls ou les accès internet ?	Non
Silver	CL1 - Security event management	2.9.2 Activez-vous, gardez-vous au moins pendant un an et configurez-vous les journaux des authentifications des administrateurs sur les équipements réseaux, serveurs et ordinateurs?	Non
Silver	CL4 - Secure network architecture	2.9.5 Avez-vous terminé la sécurisation de votre serveur active directory (en appliquant l'ensemble des bonnes pratiques ou accepté les risques résiduels des mesures non déployées) et en permettant la génération d'alertes détaillées en cas d'incident sécurité (configuration des journaux détaillés, surveillance des journaux) ?	Oui
Silver	CL5 - Identity & access management	3.1 Chaque employé dispose-t-il d'un identifiant informatique nominatif sur les environnements IT ou de production ?	Oui
Silver	CL5 - Identity & access management	3.3.1 Si vous utilisez des comptes d'administrateurs sur les machines, avez-vous une solution en place pour contrôler leur sécurité (sécurité du mot de passe, blocage du compte, changement à distance, etc.)?	Oui

Niveau	Domaine	Question	Réponse
Silver	CL0 - Governance	3.4 Formez-vous les équipes opérationnelles, (administrateurs réseau, sécurité et système, chefs de projet, développeurs, RSSI) à la sécurité des systèmes d'information ?	Oui
Silver	CL5 - Identity & access management	4.2.1 Avez-vous une gestion centralisée et sécurisée des comptes des utilisateurs capable de détecter des comportements anormaux (vol d'identifiants, utilisation sur des serveurs non standard, tentative de découverte du mot de passe...)?	Oui
Silver	CL3 - Protect end user devices	4.6.2 Avez-vous la liste des logiciels autorisés et interdits ?	Oui
Silver	CL0 - Governance	4.7 Suivez-vous au moins de manière hebdomadaire une procédure de gestion des alertes et avis de sécurité de CERT (Computer Emergency Response Team) et des éditeurs de logiciels ?	Oui
Silver	CL1 - Security event management	4.8.1 Centralisez-vous au travers d'outils de collecte SIEM (Security Information Event Management) les incidents et évènements de sécurité ?	Oui
Silver	CL4 - Secure network architecture	4.8.5 Bloquez-vous les connexions non autorisées à votre réseau ?	Non
Silver	CL3 - Protect end user devices	4.9.1 Avez-vous mis en place des solutions sur les PC et les Serveurs permettant de détecter des comportements anormaux, les bloquer ou alerter (IDS/IPS) ?	Oui
►vincent.badinier@advens.fr		EDR et XDR déployés permettant de remplir les fonctions IDS et IPS.	
►vincent.badinier@advens.fr		Aucune sonde IDS/IPS déployée.	
Silver	CL4 - Secure network architecture	5.1 Connaissez-vous les serveurs les plus sensibles de votre parc ?	Oui
Silver	CL2 - Malwares	5.10 Existe-t-il une surveillance du trafic Internet avec des alertes mais aussi des indicateurs (KPI) sur l'utilisation des données de l'entreprise sur Internet ?	Oui
Silver	CL6 - Data protection and classification	5.10.1 Chiffrez-vous vos connexions entre vos différents sites de votre société et vos partenaires ?	Oui
Silver	CL3 - Protect end user devices	5.12 Avez-vous un accès Wifi sécurisé avec une séparation des usages ? (personnel , industriel, professionnelle , visiteur, etc.)	Oui
Silver	CL6 - Data protection and classification	5.13.1 Offrez-vous aux utilisateurs la possibilité de chiffrer facilement le contenu des E-mails ?	Oui

Niveau	Domaine	Question	Réponse
Silver	CL4 - Secure network architecture	5.14 Sécurisez-vous les interconnexions réseau avec vos sous-traitants et fournisseurs ?	Oui
Silver	CL6 - Data protection and classification	5.14.1 Offrez-vous une plateforme d'échange sécurisé pour vos sous-traitants et fournisseurs ?	Non
►vincent.badinier@advens.fr		Projet de déploiement ooDrive non finalisé.	
Silver	CL4 - Secure network architecture	5.15 N'autorisez-vous la connexion au réseau qu'aux appareils identifiés et gérés par le système d'information ?	Non
Silver	CL5 - Identity & access management	5.4 Utilisez-vous une authentification forte pour la connexion à vos mails entreprise depuis Internet (double authentification avec téléphone et / ou blocage des comptes contre les essais de mots de passe, changement de mot de passe régulier, mot de passe complexe) ?	Oui
Silver	CL5 - Identity & access management	5.5.1 Utilisez-vous des fonctionnalités SSO (single sign on) pour les applications http ou E-SSO avec un gestionnaire de mots de passe automatisé ?	Oui
Silver	CL5 - Identity & access management	5.6 Utilisez-vous un réseau dédié, cloisonné (internet, poste utilisateur) et sécurisé par des mécanismes de ruptures protocolaires (machines de rebond, bastion d'administration, proxyfication, etc.) pour l'administration du système d'information ?	Non
Silver	CL5 - Identity & access management	5.6.1 Avez-vous une protection sur les postes de travail pour éviter que les utilisateurs puissent ouvrir des réseaux internet sans sécurité en branchant par exemple un modem / clé usb 3G, smartphone et en même temps avoir ces même ordinateurs connectés au réseau de l'entreprise ?	Oui
Silver	CL3 - Protect end user devices	5.7 Vous protégez-vous des menaces relatives à l'utilisation de supports amovibles ?	Oui
Silver	CL6 - Data protection and classification	5.7.1 Chiffrez-vous les données sensibles sur des supports amovibles sans aucune action requise de la part des utilisateurs (chiffrement automatique transparent) ?	Oui
Silver	CL3 - Protect end user devices	5.8.1 Avez-vous un contrôle total sur l'environnement professionnel des applications d'entreprise / données sur les appareils mobiles? (Etanchéité des environnements personnel et professionnel)	Oui
Silver	CL2 - Malwares	5.9 Les accès à internet sont-ils filtrés par un serveur mandataire (proxy) ?	Oui
Silver		6.2 Vos sauvegardes sont-elles protégées dans un local sécurisé ?	Oui

Niveau	Domaine	Question	Réponse
	CL6 - Data protection and classification		
Silver	CL0 - Governance	6.6.1 Vérifiez-vous la conformité des filiales de votre entreprise ?	Non
►vincent.badinier@advens.fr		Pas de suivi pro-actif de la conformité des filiales.	
Silver	CL4 - Secure network architecture	6.6.2 Effectuez-vous régulièrement des vérifications des règles de vos Firewalls ?	Oui
Silver	CL3 - Protect end user devices	6.7.1 Procédez-vous à des tests d'intrusion (pentest) des sites web de votre société, puis appliquez-vous les actions correctives associées ?	Oui
Silver	CL6 - Data protection and classification	7.1.2 Effectuez-vous des sauvegardes des éléments les plus sensibles de vos systèmes d'information industriel (configuration, code source et données)?	Oui
Silver	CL3 - Protect end user devices	7.10 Existe-t-il une architecture et des règles de gestion spécifiquement définies ?	Non
Silver	CL0 - Governance	7.11 Les processus de changement, les solutions dédiées de l'IACS font-ils l'objet d'un audit de conformité technique sécurité annuel ?	Non
Silver	CL6 - Data protection and classification	7.3 Existe-t-il un processus documenté de gestion des crises ? (comme par exemple, la reprise d'activité après un crash système)	Oui
Silver	CL6 - Data protection and classification	7.4 La documentation relative à la conception, aux composants et à l'exploitation des ICS est-elle stockée avec un niveau de sécurité approprié ?	Je ne sais pas
Silver	CL3 - Protect end user devices	7.8 Des procédures sont-elles en place pour gérer le cycle de vie des ICS ?	Je ne sais pas
Silver	CL0 - Governance	9.8.1 Révisez-vous annuellement le niveau de risque cyber de votre entreprise en révisant les analyses de risques de votre entreprise ?	Non

8.3 Niveau gold

Niveau	Domaine	Question	Réponse
Gold	CL4 - Secure network architecture	2.1.2 Votre cartographie réseaux et protocoles autorisés est-elle disponible et automatiquement mise à jour ?	Non

Niveau	Domaine	Question	Réponse
Gold	CL4 - Secure network architecture	2.1.3 Avez-vous mis en place une solution de détection et de surveillance (type NAC, surveillance DHCP) de la connexion de nouveaux équipements (type PC, serveur, imprimante, box) sur votre réseau interne ?	Non
Gold	CL1 - Security event management	2.9.1 Analysez-vous les journaux des composants (serveurs, PC de bureau, PC portable, imprimante , équipements réseaux, smartphones, ...) les plus importants (exemple : supervision/investigation temps réel, SOC, etc.) ?	Oui
Gold	CL0 - Governance	3.5.1 Mettez-vous en place des formations systématique en cybersécurité pour l'ensemble des employés, et contractants, adaptées ou customisées en fonction de leur rôle dans l'entreprise et effectuez-vous le suivi de participation à ces formations?	Oui
Gold	CL0 - Governance	4.11 Avez-vous mis en place ou contracté des services d'alertes sécurité professionnels et customisés pour votre entreprise, son secteur d'activité, les équipements informatiques que vous avez déployés etc. ? ("CERT" professionnels ou sectoriels, services de Threat Intelligence) ?	Non
Gold	CL1 - Security event management	4.8 Existe-t-il un centre d'opération de sécurité SOC (Security OperationCenter) permettant la détection et la supervision de la sécurité du système d'information ?	Oui
Gold	CL3 - Protect end user devices	4.8.2 Supervisez-vous les périphériques des utilisateurs comme par exemple : PC fixe, PC portable, smartphone, clé USB, etc... ?	Oui
Gold	CL1 - Security event management	4.8.3 Existe-t-il un outil d'alerte permettant d'exécuter un arrêt automatique ou une isolation de certain éléments du parc en cas d'incident majeur ?	Oui
Gold	CL2 - Malwares	4.8.4 Existe-t-il un centre de supervision de votre réseau permettant la détection des incidents de sécurité (NOC (Network Operations Center))?	Non
►vincent.badinier@advens.fr		Le firewall ne fait pas fonction de NOC.	
Gold	CL2 - Malwares	4.8.6 Avez-vous déployé et supervisez-vous des sondes réseau pour détecter des activités malicieuses ou anormales?	Non
►vincent.badinier@advens.fr		Pas de sonde réseau déployée.	
Gold	CL2 - Malwares	5.10.2 Si vous avez autorisé la navigation vers des sites internet non-professionnel, avez-vous déployé une solution de navigation sécurisée pour ces sites l'isolant du réseau informatique standard?	Non
Gold	CL5 - Identity & access management	5.5 Utilisez-vous une authentification forte et surveillez-vous (alertes en cas d'échec) la connexion aux équipements sensibles comme par exemple : l'administration des	Oui

Niveau	Domaine	Question	Réponse
		équipements IT, l'administration des services cloud et sites internet ?	
Gold	CL6 - Data protection and classification	6.3 Utilisez-vous un système de stockage et de sauvegarde des données piloté en central, comme un Cloud (AWS, O365 Sharepoint, OneDrive, google drive,...) ?	Oui
Gold	CL6 - Data protection and classification	6.5 Mettez-vous en place des solutions de gestion de protection des données de l'entreprise (détection de fuite des données confidentielles, rôles et responsabilités ...) ?	Non
Gold	CL0 - Governance	6.7 Procédez-vous à des tests d'intrusion (pentest) réguliers sur votre SI et de vos filiales, puis appliquez-vous les actions correctives associées ?	Oui
Gold	CL1 - Security event management	6.7.2 Vérifiez-vous et mettez-vous à jour régulièrement vos dispositifs de détection d'attaque cyber ? (Via par exemple la mise à jour des règles de supervision sécurité suite aux pentests effectués sur vos systèmes, ou une gestion de projet sécurité)	Oui
Gold	CL6 - Data protection and classification	6.9.1 Avez-vous mis en place une solution de classification automatique des données de votre entreprise, ou d'aide à la prise de décision de protection d'une données qui serait classifiée sensible?	Non
Gold	CL6 - Data protection and classification	6.9.2 Avez-vous une solution permettant d'interdire l'envoi de données confidentielles non protégées ou de procéder à leur chiffrement systématique avant qu'elles soient enregistrées ou envoyées en dehors de votre système d'information ?	Non
Gold	CL6 - Data protection and classification	7.1.3 Est-ce que les sauvegardes de vos systèmes d'information sont régulièrement testées?	Non
Gold	CL6 - Data protection and classification	7.12 Les composants de l'ICS font ils l'objet d'un processus de surveillance des menaces et des vulnérabilités ?	Oui
Gold	CL4 - Secure network architecture	7.13 Existe-t-il un centre de supervision sécurité (SOC, NOC (Network Operations Center), backup status...) de votre réseau permettant la détection des incidents de sécurité, problème de backup, et/ou surveillance active de l'Informatique industrielle (IACS) ?	Oui
Gold	CL1 - Security event management	7.14 Lorsqu'un incident survient dans la production, investiguez-vous pour identifier si cet incident pourrait être causé par un élément malveillant ?	Oui
Gold	CL4 - Secure network architecture	7.2 documentation, la nomenclature et les schémas des équipements ICS sont-ils tenus à jour ?	Non
Gold			Non

Niveau	Domaine	Question	Réponse
	CL3 - Protect end user devices	7.5 Existe-t-il une personne qualifiée ou un département dédié à la conception, l'exploitation, et la surveillance des équipements de l'ICS ?	
Gold	CL4 - Secure network architecture	7.9 Utilisez-vous un réseau dédié et cloisonné pour l'administration des ICS ?	Non
Gold	CL1 - Security event management	9.7.1 Avez-vous mis en place, documenté et testé au moins annuellement un procédure de gestion de problèmes sécurité vous permettant d'être assuré de pouvoir réagir rapidement et d'impliquer les bonnes personnes internes ou externes?	Non
Gold	CL0 - Governance	9.8.2 Avez-vous une solution informatisée pour la gestion du risque vous permettant de manière plus ou moins automatisée de remonter le niveau de risque cyber et de le traiter ?	Non
►vincent.badinier@advens.fr		Absence d'analyse de risque.	

8.4 Questions Générales

Niveau	Domaine	Question	Réponse
N/A		8.1 Avez-vous des exigences précises de vos clients en matière de gestion de la sécurité des SI ? (par exemple : appels d'offres, clauses dans les contrats)	Oui
N/A		8.4 Avez-vous pour votre part mis en place des exigences particulières en termes de cyber sécurité vis-à-vis de vos propres fournisseurs ?	Non
N/A		9.1 Connaissez-vous bien l'ensemble des risques liés à la Cyber sécurité ? (Infogérances, Perte de données, image de l'entreprise, cyber-espionnage, risque légal...)	Oui
N/A		9.10 Vos différents contrats d'assurance vous couvrent-ils en cas de perte d'activité liée à un problème de sécurité informatique ?	Oui
N/A		9.2 Existe-t-il un budget spécifique lié à la gestion informatique dans l'entreprise ? (Matériel / suivi / maintenance / sécurité ?)	Oui
N/A		9.6 Aujourd'hui, pensez-vous être suffisamment protégé contre les risques liés à l'informatique et à l'internet ?	Non
N/A		9.7 Avez-vous, à votre connaissance, déjà été victime d'une cyber attaque ?	Non
N/A		9.9 Disposez-vous d'un contrat d'assurance lié au risque informatique ? (Matériel et cyberattaque ?)	Oui

BRONZE

AirCyber self-declared maturity

Has been delivered to:

Integris Composites S.A.S.

MEMBER SINCE 11-03-2026
Analyzed site: Integris Composites S.A.S.-38270 France

Meeting the following requirements:

BRONZE	SILVER	GOLD
92%	74%	44%

Generated on 03-07-2026.This certificate has been automatically generated based on the AirCyber questionnaire’s answers provided. No AirCyber cyber security expert has validated the stated maturity level.
Aircyber standard v1.9