DIFFUSION RESTREINTE
Référence : EBIOS-RM-BET-ST-2026-V1.0

ANALYSE DE RISQUES EBIOS RISK MANAGER

BIOÉNERGIE TECH

Zone classifiée « Confidencial » — Projet SpainTurbine

Contrat Armée espagnole — 120 micro-turbines / mois pour drones militaires

Champ	Valeur
Émetteur	Responsable de la Sécurité des Systèmes d'Information (RSSI)
Validation	Direction Générale — M. Laurent Dubois, Directeur Général
Méthode	EBIOS Risk Manager (ANSSI, version 1.5, 2018) – ISO/IEC 27005:2022
Référentiel d'appui	PSSI-BET-ST-2026-V1.0 — DAT BET-ST-2026
Date d'émission	20 mai 2026
Classification	Diffusion restreinte — Diffusion interne BET + autorité de sécurité espagnole
Cycle de revue	Annuelle, ou à tout changement structurel majeur

Avertissement et classification

Le présent rapport constitue l'analyse de risques EBIOS Risk Manager du système d'information de la zone classifiée « Confidencial » de BIOÉNERGIE TECH dédié au projet SpainTurbine. Il est classifié « Diffusion restreinte » et diffusé exclusivement au Comité de Direction de BIOÉNERGIE TECH, au RSSI, à l'administrateur du système d'information, ainsi qu'aux personnels nominativement habilités sur le projet SpainTurbine. Toute reproduction, transmission à un tiers non habilité ou sortie du périmètre de l'entreprise est strictement interdite et expose son auteur aux sanctions disciplinaires et pénales prévues par la loi française (articles 413-9 et suivants du Code pénal) et par les engagements contractuels pris envers l'Armée espagnole.

Sommaire

Le présent rapport est structuré conformément aux cinq ateliers de la méthode EBIOS Risk Manager publiée par l'ANSSI. Il s'articule autour de la séquence suivante : Atelier 1 — Cadrage et socle de sécurité ; Atelier 2 — Sources de risques et objectifs visés ; Atelier 3 — Scénarios stratégiques et cyberbiographie de l'attaque ; Atelier 4 — Scénarios opérationnels; Atelier 5 — Traitement des risques (plan d'action, mesures techniques, physiques et organisationnelles, indicateurs de suivi, risques résiduels). Une conclusion synthétique reprend les enseignements majeurs et les jalons de mise en œuvre.

Introduction et synthèse exécutive

Contexte de l'étude

BIOÉNERGIE TECH, PME industrielle de quarante-neuf collaborateurs implantée à Chambéry, a signé en mai 2026 un contrat avec SpainTurbine portant sur la fourniture mensuelle de cent vingt micro-turbines destinées aux drones militaires de l'Armée espagnole, pour un montant annuel de 1,2 M€. Ce contrat soumet l'entreprise au régime de protection des informations classifiées « Confidencial » au sens de l'Instruction Générale Interministérielle n° 1300 et de son équivalent espagnol. Une zone classifiée dédiée a été déployée à Chambéry, isolée physiquement et logiquement du SI corporate, et hébergeant un SI cloisonné « air-gappé » conforme aux exigences contractuelles et aux recommandations de l'ANSSI.

Périmètre et méthode

L'étude couvre l'ensemble des actifs, processus et personnels de la zone classifiée : trois postes utilisateurs HP Elite 800 G9, un poste de mise à jour relié à un pare-feu Cisco Secure Firewall 1120, un poste de chiffrement, une station blanche S3Box Hogo, un switch Cisco Catalyst 9200, deux serveurs Dell PowerEdge R470 (principal + redondance) hébergeant sept VM (PKI, AD, ELK, Partage, Vidéo, Admin, Sauvegarde), des lecteurs biométriques HID Signo 25B, une caméra Axis M4216-V, un lecteur LTO-8 HPE StoreEver Ultrium 30750 et son coffre Fichet-Bauche Carena. Cinq personnels sont nominativement habilités : trois employés projet, un administrateur système-sécurité, et le Directeur Général M. Laurent Dubois. L'étude est conduite selon la méthode EBIOS Risk Manager v1.5 de l'ANSSI et s'appuie sur le DAT et la PSSI internes.

Principaux enseignements

L'analyse identifie deux scénarios à risque très élevé (cotés 12/16) : la compromission du SI cloisonné par introduction d'un implant via le flux de mise à jour (air-gap bypass) et le vol physique d'une cartouche LTO-8 par un personnel habilité sous coercition. Deux scénarios complémentaires de gravité élevée à modérée sont également retenus : le ransomware via la supply chain de la station blanche et l'espionnage économique indirect. Le plan de traitement combine trente-trois mesures (quinze techniques, huit physiques, dix organisationnelles), structurées en trois vagues sur douze mois pour un budget estimé à 180 000 € HT, permettant de ramener les risques résiduels au niveau « modéré » à « faible ».

Atelier 1 — Cadrage et socle de sécurité

1.1 Objectifs et finalité de l'atelier

Conformément à la méthode EBIOS Risk Manager publiée par l'ANSSI (version 1.5, 2018), l'atelier 1 a pour finalité de circonscrire l'étude, de définir les missions et valeurs métier portées par le système d'information cible, d'identifier les biens essentiels à protéger et les actifs supports qui les concrétisent, puis d'objectiver la criticité de chacun selon les critères de Disponibilité, d'Intégrité et de Confidentialité (D.I.C.). Il s'achève par l'identification des événements redoutés associés et par la qualification du socle de sécurité existant et de ses écarts.

La présente étude porte sur la zone classifiée « Confidencial » de BIOÉNERGIE TECH, dédiée au projet SpainTurbine (Armée espagnole). Le périmètre considéré est celui du Dossier d'Architecture Technique (DAT) BET-ST-2026 et de la Politique de Sécurité des Systèmes d'Information PSSI-BET-ST-2026-V1.0. L'étude ne traite pas du système d'information « corporate » de BIOÉNERGIE TECH, lequel relève d'une PSSI distincte.

1.2 Cadre stratégique et enjeux métier

BIOÉNERGIE TECH est une PME industrielle de quarante-neuf collaborateurs implantée à Chambéry, spécialisée dans la conception et la fabrication de cellules et modules de batteries innovantes ainsi que de turbines mini-hydrauliques. La signature, en mai 2026, du contrat SpainTurbine portant sur la fourniture de cent vingt micro-turbines mensuelles destinées à des drones militaires de l'Armée espagnole, pour un montant annuel d'un million deux cent mille euros, place de facto l'entreprise dans la chaîne d'approvisionnement de la défense et l'expose au régime de protection des informations classifiées « Confidencial » tel que défini par l'Instruction Générale Interministérielle n° 1300 et son équivalent espagnol.

Les enjeux structurants se déclinent selon quatre axes interdépendants : un enjeu contractuel et financier (maintien du contrat SpainTurbine et préservation du chiffre d'affaires associé) ; un enjeu réputationnel et stratégique (capacité de l'entreprise à se positionner durablement sur le marché de la défense européenne) ; un enjeu de souveraineté et de protection du secret de la défense nationale française et espagnole ; et enfin un enjeu humain et social, le contrat constituant un levier majeur de pérennité pour les quarante-neuf salariés.

1.3 Périmètre métier et technique

Le périmètre étudié, qualifié de « zone classifiée » dans la documentation interne, est physiquement et logiquement isolé du SI « corporate ». Il se compose de trois sous-réseaux indépendants décrits ci-après.

Sous-réseau	Cloisonnement	Composants principaux	Connexion externe
Réseau interne (production classifiée)	Totalement isolé (air-gap intégral)	Switch Cisco Catalyst 9200 ; serveurs Dell PowerEdge R470 (principal + redondance) hébergeant 7 VM : PKI, Partage de fichiers, Sauvegarde, SIEM ELK, Serveur Vidéo, Serveur	Aucune

Sous-réseau	Cloisonnement	Composants principaux	Connexion externe
		d'administration de rebond et Active Directory ; 3 postes utilisateurs HP Elite 800 G9 ; lecteurs biométriques HID Signo 25B et caméra Axis M4216-V dans le SAS.	
Réseau de chiffrement	Totalement isolé	1 poste HP Elite 800 G9 dédié au (dé)chiffrement des supports amovibles ; station blanche S3Box Hogo pour la décontamination antivirale.	Aucune
Réseau de mise à jour	Isolé du réseau interne — connecté à Internet de façon restreinte	1 poste HP Elite 800 G9 dédié relié au pare-feu Cisco Secure Firewall 1120 ; flux sortants strictement allowlistés vers les serveurs Microsoft Update.	HTTPS vers serveurs Microsoft Update uniquement ; transit des correctifs vers le réseau interne exclusivement par clé USB après passage en station blanche.
Stockage physique hors-ligne	Cloisonné de tout réseau	Coffre-fort Fichet-Bauche Carena 120 L hébergeant les bandes LTO-8 (sauvegardes à froid), le coffre à six compartiments cloisonnés pour les clés de chiffrement et la YubiKey de recouvrement.	Aucune

1.4 Missions métier

Quatre missions métier structurent l'activité de la zone classifiée. Elles constituent le référentiel permettant d'apprécier la criticité des biens essentiels qui en assurent la réalisation.

Code	Mission métier	Description opérationnelle
M1	Production technique des micro-turbines SpainTurbine	Conception détaillée (CAO/CAM), simulation, prototypage virtuel, génération des dossiers de fabrication et des plans de définition transmis à la chaîne de production des cent vingt micro-turbines mensuelles destinées aux drones militaires de l'Armée espagnole.
M2	Gestion documentaire classifiée « Confidencial »	Réception, qualification, stockage, partage interne et restitution des spécifications, plans, comptes rendus de tests et correspondances classifiées « Confidencial » au sens de l'IGI 1300 et de son équivalent espagnol.
M3	Exploitation et maintien en condition de sécurité du SI cloisonné	Administration de l'Active Directory, de la PKI interne, du SIEM ELK, des sauvegardes LTO-8, des correctifs de sécurité, de la station blanche et du contrôle d'accès physique ; tenue des registres et des journaux opposables.

Code	Mission métier	Description opérationnelle
M4	Contrôle physique et logique d'accès à la zone classifiée	Contrôle nominatif des entrées et sorties au moyen du double facteur badge + biométrie HID Signo 25B, supervision vidéo Axis M4216-V du SAS, gestion des YubiKey, des consignes de visite et des registres d'accès.

1.5 Biens essentiels (valeurs métier)

Les biens essentiels représentent les informations et processus qui justifient à eux seuls la mise en œuvre de la présente étude. Toute mesure de sécurité prescrite dans la suite du rapport devra pouvoir être rattachée à la protection d'au moins l'un de ces biens essentiels.

Code	Bien essentiel	Nature	Mission(s) rattachée(s)
VE1	Données techniques de conception des micro-turbines (fichiers CAO/CAM, dossiers de définition, paramètres de procédés, simulations, jumeaux numériques)	Information	M1, M2
VE2	Données contractuelles et opérationnelles SpainTurbine (correspondance, comptes rendus, livrables, certifications, exigences de l'autorité de sécurité espagnole)	Information	M2
VE3	Secrets cryptographiques et données d'authentification (certificats PKI, clés privées AD, clés de chiffrement LTO matérielles, secrets YubiKey)	Information	M3, M4
VE4	Journaux d'événements horodatés et indexés dans la pile ELK (Active Directory, Windows, pare-feu Cisco, station blanche, lecteurs biométriques, caméra)	Information	M3, M4
VE5	Sauvegardes hors-ligne LTO-8 (cartouches IBM Ultrium 8 chiffrées matériellement par le lecteur HPE StoreEver Ultrium 30750)	Information	M2, M3
VE6	Processus d'administration et d'exploitation du SI cloisonné (procédures, scripts, configurations Cisco et Dell de référence)	Processus	M3
VE7	Processus de contrôle d'accès physique au SAS et au local sécurité	Processus	M4

1.6 Échelle de criticité D.I.C.

L'évaluation est conduite selon une échelle à quatre niveaux conforme au guide ANSSI EBIOS RM. Chaque critère est apprécié indépendamment, puis le niveau global du bien essentiel est défini par la valeur maximale de ses trois composantes.

Niveau	Libellé	Critère D — Disponibilité	Critère I — Intégrité	Critère C — Confidentialité
1	Mineur	Indisponibilité tolérable sans impact métier (> 5 jours).	Altération limitée, détectable et corrigible dans la journée.	Divulgation acceptable à un cercle élargi de salariés.
2	Significatif	Indisponibilité tolérée jusqu'à 48 h, impact opérationnel limité.	Altération corrigible en quelques heures sans répercussion contractuelle.	Divulgation limitée à l'écosystème non habilité défense.
3	Majeur	Indisponibilité > 24 h entraînant manquement contractuel partiel.	Altération non immédiatement détectable, recours nécessaire à des sauvegardes.	Divulgation à un tiers non habilité ; impact contractuel et image notable.
4	Critique	Indisponibilité > 4 h provoquant rupture de la chaîne SpainTurbine, mise en cause de la sécurité nationale française et/ou espagnole.	Altération non détectable conduisant à la livraison d'un produit non conforme, sabotage différé type Stuxnet.	Divulgation à une puissance étrangère, à un concurrent stratégique ou au grand public ; atteinte au secret de la défense nationale.

1.7 Évaluation D.I.C. des biens essentiels

Bien essentiel	D	I	C	Justification synthétique
VE1 — Données techniques micro-turbines	3	4	4	C=4 : exfiltration vers une puissance étrangère = atteinte au secret défense. I=4 : altération CAO non détectable = drones défectueux livrés. D=3 : indisponibilité bloque la conception mais pas immédiatement la production déjà transmise.
VE2 — Données contractuelles SpainTurbine	2	4	4	C=4 : exposition publique des liens entre BIOÉNERGIE TECH et l'Armée espagnole. I=4 : altération de livrables = manquement contractuel. D=2 : reconstitution possible auprès du client.
VE3 — Secrets cryptographiques et authentification	4	4	4	Compromission d'un seul facteur = effondrement de toute la chaîne de confiance (chiffrement LTO, accès AD, accès physique).
VE4 — Journaux ELK	3	4	3	I=4 : sans intégrité, aucune imputabilité possible. C=3 : les logs contiennent des données d'usage. D=3 : indisponibilité dégrade la capacité de détection.

Bien essentiel	D	I	C	Justification synthétique
VE5 — Sauvegardes LTO-8	4	4	4	D=4 : sans LTO, pas de PRA. I=4 : sauvegarde altérée = restauration empoisonnée. C=4 : une bande exfiltrée contient des semaines de production classifiée.
VE6 — Processus d'administration	3	4	3	I=4 : un script altéré peut désactiver toute la sécurité. D=3 et C=3 : les procédures sont reconstituables mais leur exposition facilite la cartographie d'une attaque.
VE7 — Processus de contrôle d'accès physique	3	4	3	I=4 : un contournement non détecté ouvre la zone à un adversaire.

Conclusion de l'évaluation : la quasi-totalité des biens essentiels présente un niveau global D.I.C. égal à 4 (« Critique »). Cette observation confirme la sensibilité homogène du périmètre étudié et justifie le choix d'une doctrine de sécurité « défense en profondeur » et « zéro confiance », telle qu'elle est déjà formalisée dans la PSSI de niveau 1 de BIOÉNERGIE TECH.

1.8 Cartographie des actifs supports

Les actifs supports sont les éléments matériels, logiciels, humains, organisationnels ou immatériels qui permettent la réalisation des missions et l'existence des biens essentiels. Ils constituent la cible concrète des attaques. Leur identification est une étape préalable indispensable à l'élaboration des scénarios opérationnels conduits à l'atelier 4.

Code	Actif support	Catégorie	Biens essentiels portés
AS01	Serveurs Dell PowerEdge R470 (principal + redondance)	Matériel	VE1, VE2, VE3, VE4, VE5, VE6
AS02	Postes utilisateurs HP Elite 800 G9 (×3)	Matériel	VE1, VE2
AS03	Switch Cisco Catalyst 9200 (cœur de réseau)	Matériel / Logique	VE1, VE2, VE3, VE4
AS04	Pare-feu Cisco Secure Firewall 1120 (réseau MAJ)	Matériel / Logique	VE6
AS05	VM Active Directory	Logiciel	VE3, VE4, VE7
AS06	VM PKI interne	Logiciel	VE3
AS07	VM SIEM ELK (Elasticsearch / Logstash / Kibana)	Logiciel	VE4
AS08	VM Serveur de partage de fichiers (SMB v3)	Logiciel	VE1, VE2
AS09	VM Serveur vidéo (RTSP/H.264)	Logiciel	VE7
AS10	VM Serveur d'administration de rebond	Logiciel	VE6

Code	Actif support	Catégorie	Biens essentiels portés
AS11	VM Sauvegarde	Logiciel	VE5
AS12	Poste de mise à jour HP Elite 800 G9 (Internet restreint)	Matériel	VE6
AS13	Poste de chiffrement / déchiffrement HP Elite 800 G9	Matériel	VE3, VE5
AS14	Station blanche S3Box Hogo	Matériel	VE6
AS15	Lecteur HPE StoreEver LTO-8 Ultrium 30750	Matériel	VE5
AS16	Cartouches IBM LTO-8 Ultrium 8 (×15)	Support amovible	VE5
AS17	Coffre-fort Fichet-Bauche Carena 120 L	Sécurité physique	VE5, VE3
AS18	Coffre à six compartiments cloisonnés (clés de chiffrement)	Sécurité physique	VE3
AS19	Lecteurs biométriques HID Signo 25B (×2) — SAS et local sécurité	Sécurité physique	VE7
AS20	Caméra IP Axis M4216-V (SAS)	Sécurité physique	VE7
AS21	YubiKey C NFC FIDO2 (×5, dont 1 de recouvrement)	Authentifiant	VE3
AS22	Badges nominatifs (×5 employés projet)	Authentifiant	VE7
AS23	Câblage Ethernet Cat6a + verrous RJ45 et verrous USB	Matériel passif	VE1, VE3
AS24	Personnels habilités : 3 employés projet, 1 administrateur, 1 Directeur Général (M. Laurent Dubois)	Humain	Toutes valeurs métier
AS25	Tiers intervenants : fournisseur télécom, sous-traitant station blanche, organisme d'audit, agents de ménage non habilités	Humain	VE7
AS26	Local sécurité (salle serveur, SAS, alimentation onduleurs, climatisation)	Environnement physique	Toutes valeurs métier
AS27	Procédures et chartes opposables (PSSI, PO-IAM, PO-SAUV-LTO, PO-STATION-BLANCHE)	Organisationnel	Toutes valeurs métier

1.9 Événements redoutés

Les événements redoutés (ER) sont les conséquences indésirables sur les biens essentiels que la sécurité vise à éviter. Ils sont exprimés du point de vue métier et constituent les cibles que les scénarios stratégiques et opérationnels chercheront à matérialiser.

Code	Événement redouté	Bien(s) essentiel(s)	Critère D.I.C. impacté	Impact métier maximal anticipé
ER1	Exfiltration de tout ou partie des plans CAO/CAM des micro-turbines vers une puissance étrangère ou un concurrent	VE1	C=4	Atteinte au secret de la défense nationale, perte du contrat SpainTurbine, mise en cause pénale de la Direction (art. 413-9 CP), risque de redressement judiciaire.
ER2	Altération non détectée des fichiers de définition CAO/CAM de micro-turbines (sabotage différé)	VE1, VE5, VE6	I=4	Livraison de drones défectueux, accidents en zone de combat, mise en cause pénale et contractuelle, dommages corporels possibles.
ER3	Indisponibilité prolongée du SI cloisonné dépassant le RTO contractuel (rupture de la production assistée)	VE1, VE2, VE3, VE4	D=4	Retard de livraison des cent vingt turbines mensuelles, pénalités contractuelles, mobilisation du PCA.
ER4	Compromission des secrets d'authentification (PKI, AD, clés LTO, YubiKey)	VE3	C=4 et I=4	Effondrement de la chaîne de confiance, attaque de type « Golden Ticket » Kerberos, perte de l'imputabilité.
ER5	Vol, substitution ou destruction d'une cartouche LTO-8 contenant la sauvegarde hebdomadaire	VE5	C=4 et D=4	Exfiltration d'un instantané complet du projet ; ou impossibilité de restaurer en cas de sinistre.
ER6	Modification non autorisée du périmètre d'habilitation (création de compte fantôme, élévation de privilèges)	VE3, VE4, VE7	I=4 et C=4	Persistance silencieuse d'un attaquant, contournement durable des contrôles d'accès.
ER7	Divulgation par voie d'imprudence d'informations classifiées (clé USB perdue, photo, e-mail erroné)	VE1, VE2	C=4	Atteinte au secret défense, sanction disciplinaire et pénale, notification réglementaire ANSSI et autorité espagnole.
ER8	Compromission durable du SI par un implant introduit via le flux de mise à jour (air-gap bypass)	VE1 à VE6	C=4 et I=4	Espionnage permanent, exfiltration discrète, sabotage différé.

1.10 Socle de sécurité existant et écarts

Le socle de sécurité existant est décrit en détail par la PSSI-BET-ST-2026-V1.0 et par le DAT. Il s'appuie sur les guides ANSSI : « Maîtrise de l'accès Internet », « Recommandations relatives à l'administration sécurisée des systèmes d'information », « Recommandations de sécurité Active Directory », « Recommandations pour la mise en œuvre d'une politique de cloisonnement », « Recommandations sur

la journalisation » (NT-022) et « Guide d'hygiène informatique ». La synthèse ci-dessous met en regard les mesures déployées et les écarts résiduels identifiés.

Domaine de sécurité	Mesures existantes	Écarts ou points d'attention résiduels
Cloisonnement	Air-gap intégral du réseau interne, pare-feu Cisco 1120 sur le réseau MAJ, VLAN distincts par fonction, verrous physiques sur ports RJ45 et USB, station blanche obligatoire pour tout support amovible.	Aucun cloisonnement formel inter-VM sur le même hyperviseur Dell ; un escalade depuis la VM Partage de fichiers peut atteindre la VM AD si l'hyperviseur est vulnérable. Aucun contrôle physique de sortie type fouille corporelle.
Authentification et IAM	MFA badge + YubiKey FIDO2 pour les postes ; ajout d'un facteur biométrique HID Signo 25B pour le SAS et le local sécurité ; comptes nominatifs à privilèges, Kerberos AES-256, LDAPS, revue trimestrielle des comptes, désactivation à 60 jours.	Absence explicite de modèle de tiering Microsoft (Tier 0 / 1 / 2) ; pas de PAW (Privileged Access Workstation) dédié à l'administration ; YubiKey de recouvrement stockée dans le même coffre que les clés LTO (concentration des secrets).
Journalisation et détection	Centralisation ELK de tous les journaux, conservation 36 mois (12 en ligne + 24 sur LTO), tableaux Kibana RSSI, synchronisation NTP mensuelle vérifiée.	absence de règles de détection comportementale (UEBA) ; aucun honeypot interne ; alertes Kibana revues hebdomadairement (couverture nocturne et weekend non précisée).
Sauvegardes	LTO-8 complètes hebdomadaires, incrémentales quotidiennes, chiffrement matériel HPE Ultrium, dépôt en coffre Fichet-Bauche Carena, quatre cartouches dans une zone sécurisée dans le premier site..	Pas de scellés numérotés et infalsifiables sur les bandes ; pas de hash de référence calculé en fin de sauvegarde et stocké hors bande ; test de restauration complet annuel (rythme insuffisant face à des sauvegardes empoisonnées).
Sécurité physique	Lecteurs biométriques HID Signo 25B (×2), caméra Axis M4216-V dans le SAS, coffre Fichet-Bauche, coffre à six compartiments pour clés de chiffrement, badges nominatifs.	Caméra unique limitée au SAS ; angle mort sur la zone du coffre LTO et de la salle serveur ; pas de détection métal en sortie ; pas de scellés numérotés sur les cartouches LTO ; coffre à clés et coffre LTO dans le même périmètre physique.
Gestion des supports amovibles	Station blanche S3Box Hogo obligatoire ; verrous physiques sur ports USB ; PC dédié au chiffrement/déchiffrement des supports.	S3Box Hogo n'analyse que les signatures connues ; absence de bac à sable comportemental (sandbox dynamique) ; pas de DLP en sortie ; pas de hash de référence des supports légitimes.
Gestion des tiers et coactivité	Badge journalier nominatif, accompagnement par un employé projet, clause miroir PSSI, droit d'audit, notification d'incident sous 24 h.	Voisinage industriel sensible (CHEMICALIA à 40 m, métallurgie 80–100 m, voie ferrée 200 m) accroît le risque de coactivité non maîtrisée ; coordonnées des sous-traitants conservées au format numérique exposé au SI corporate.

Domaine de sécurité	Mesures existantes	Écarts ou points d'attention résiduels
Continuité et résilience	PCA / PRA, exercices semestriels tabletop, exercice annuel scénarisé, RETEX systématique.	Le périmètre des exercices ne couvre pas explicitement le scénario insider sous coercition ; pas de plan de communication de crise envers l'autorité espagnole formalisé.

Les écarts identifiés alimentent directement le plan d'action de l'atelier 5. Ils ne remettent pas en cause le caractère significatif du socle déployé, mais ils traduisent les marges de progression que BIOÉNERGIE TECH doit instruire pour porter durablement le niveau de sécurité au standard requis par la classification « Confidencial ».

Atelier 2 — Sources de risques et objectifs visés

2.1 Finalité de l'atelier

L'atelier 2 d'EBIOS Risk Manager identifie, qualifie et hiérarchise les sources de risques (SR) susceptibles de cibler le système d'information étudié, puis met en regard chaque source avec les objectifs visés (OV) qu'elle est en mesure de poursuivre. Le couple SR/OV constitue la brique élémentaire à partir de laquelle seront construits, à l'atelier 3, les scénarios stratégiques. Conformément au guide ANSSI EBIOS RM, la pertinence d'un couple SR/OV est cotée selon deux axes : la motivation et les ressources de la source d'une part, l'activité observée sur la cible (ou un secteur similaire) d'autre part.

2.2 Cartographie des sources de risques

Au regard du caractère défense du projet SpainTurbine, de la typologie « Confidencial » des données manipulées et de la position de BIOÉNERGIE TECH dans la supply chain de l'Armée espagnole, cinq sources de risques ont été retenues, couvrant un spectre allant de l'attaquant étatique structuré à l'incident humain non malveillant.

Code	Source de risque (SR)	Motivation principale	Ressources et capacités	Activité observée sur le secteur
SR1	Service de renseignement étatique étranger (type APT structuré : APT28 « Fancy Bear », APT29 « Cozy Bear », Lazarus, Storm-2372)	Acquisition de renseignement militaire et industriel, contre-influence, cartographie de la supply chain défense, sabotage différé en cas de tension géopolitique.	Extrêmes : équipes dédiées, 0-day, signatures de code volées, opérations « OT/IT », exploitation des chaînes logistiques (SolarWinds, 3CX, MOVEit), capacité d'opérations physiques (HUMINT).	Très forte : campagnes documentées contre l'industrie de défense européenne (ENISA Threat Landscape 2024–2026, CERT-FR 2024-AVI-0421, rapports MIVILUDES espagnols).
SR2	Initié malveillant (employé projet, administrateur, sous-traitant) — recruté, retourné, corrompu ou sous contrainte	Gain financier direct, idéologie, chantage familial (kompromat), idéalisme ou aigreur personnelle, retournement par un service étranger.	Élevées de facto : accès physique légitime, connaissance précise des procédures internes, capacité à contourner les contrôles techniques.	Référence Carnegie Mellon CERT Insider Threat Center : 23 % des incidents IP defense dus à des initiés ; affaire Dassault-Atos 2021 et Thales 2023.
SR3	Cybercriminel opportuniste organisé (groupe ransomware-as-a-service	Gain financier par rançon, double extorsion (chiffrement +	Moyennes à élevées : kits offerts en RaaS, brokers d'accès initial, infrastructures C2	Croissante : campagnes contre les sous-traitants de la défense (SGS,

Code	Source de risque (SR)	Motivation principale	Ressources et capacités	Activité observée sur le secteur
	, type LockBit, BlackCat/ALPHV, Akira)	fuite), revente sur dark web des données stratégiques.	distribuées, mais capacité de pénétration d'un air-gap limitée.	Veolia, KP Snacks, ASCO Industries 2019).
SR4	Concurrent industriel (espionnage économique) — fabricants asiatiques ou est-européens de drones tactiques	Captation d'avantage commercial (design des micro-turbines), discréditation du fournisseur français, raccourcir le délai R&D propre.	Moyennes : recours à des prestataires (intelligence économique douteuse), ingénierie sociale, recrutement d'anciens salariés, achat de données sur marchés noirs.	Documentée : rapports DGSI sur l'ingérence économique 2022–2025, dossiers Safran et Naval Group.
SR5	Hacktiviste ou mouvement anti-armement	Visibilité médiatique, dénonciation idéologique de la militarisation européenne ou de la vente d'armes à l'étranger.	Faibles à moyennes : OSINT, defacement web, fuite organisée, doxing des dirigeants.	Modérée mais constante : groupes type Anonymous, Distributed Denial of Secrets, fuites Wikileaks et plus récemment OperationDefense ; relayée par presse engagée.
SR6	Erreur humaine non malveillante (« divulgation accidentelle »)	Aucune intention malveillante — fatigue, méconnaissance, urgence opérationnelle, contournement de procédure perçue comme contraignante.	Faibles techniquement mais conséquences potentiellement majeures (clé USB perdue, courriel erroné, photo d'écran).	Permanente : statistiques ANSSI 2024 indiquent que 60 % des fuites de données restent d'origine humaine non intentionnelle.

2.3 Évaluation de la pertinence des sources de risques

L'évaluation s'appuie sur une grille à trois axes — motivation, ressources, activité observée — chacun coté de 1 (faible) à 4 (très fort). Une source dont la somme dépasse 8 et dont chaque axe vaut au moins 2 est retenue pour la suite de l'étude. Les sources écartées sont conservées en suivi de veille mais ne donnent pas lieu à scénario stratégique dédié.

Source	Motivation	Ressources	Activité observée	Score	Pertinence retenue ?
SR1 — APT étatique	4	4	4	12	**Oui — priorité 1**
SR2 — Initié sous coercition ou corruption	3	4	3	10	**Oui — priorité 1**
SR3 — Cybercriminel ransomware	3	3	3	9	**Oui — priorité 2**
SR4 — Concurrent industriel	3	3	3	9	**Oui — priorité 2**
SR5 — Hacktiviste	2	2	2	6	Suivi de veille uniquement
SR6 — Erreur humaine	1	1	4	6	Suivi opérationnel (PSSI § 6)

2.4 Objectifs visés (OV) par source de risque

Pour chaque source retenue, les objectifs visés sont déclinés en cohérence avec la nature de la cible et les biens essentiels identifiés à l'atelier 1. Chaque OV est rattaché à un ou plusieurs événements redoutés (ER).

Couple	Source de risque	Objectif visé (OV)	Événement(s) redouté(s) corrélé(s)
SR1.OV1	SR1 — APT étatique	Exfiltrer les plans CAO/CAM des micro-turbines au profit d'une puissance étrangère.	ER1, ER8
SR1.OV2	SR1 — APT étatique	Implanter durablement un implant dans le SI cloisonné en vue d'un sabotage différé ou d'une exfiltration continue.	ER2, ER4, ER8
SR1.OV3	SR1 — APT étatique	Cartographier la supply chain défense BIOÉNERGIE TECH ↔ SpainTurbine ↔ Armée espagnole pour préparer une attaque connexe.	ER1, ER7
SR2.OV1	SR2 — Initié	Exfiltrer directement des données techniques ou contractuelles via clé USB, photographie ou dictée.	ER1, ER7
SR2.OV2	SR2 — Initié	Introduire ou faire introduire un implant logiciel via un support amovible préparé hors site.	ER2, ER4, ER6, ER8
SR2.OV3	SR2 — Initié	Voler ou substituer une cartouche LTO-8 lors de la rotation hebdomadaire.	ER5
SR3.OV1	SR3 — Cybercriminel	Chiffrer le SI cloisonné et exiger une rançon ; double extorsion par menace de fuite.	ER3, ER5

Couple	Source de risque	Objectif visé (OV)	Événement(s) redouté(s) corrélé(s)
SR4.OV1	SR4 — Concurrent	Acquérir les spécifications détaillées des micro-turbines pour réduire un cycle de R&D propre.	ER1
SR4.OV2	SR4 — Concurrent	Discréditer BIOÉNERGIE TECH auprès de SpainTurbine par fuite contrôlée mettant en cause sa sécurité.	ER1, ER7

2.5 Synthèse — couples SR/OV retenus pour les ateliers suivants

Au terme de l'atelier 2, neuf couples SR/OV ont été retenus comme pertinents et seront déclinés en scénarios stratégiques (atelier 3) puis opérationnels (atelier 4). Deux d'entre eux — SR1.OV2 (compromission via flux MAJ / clé USB) et SR2.OV3 (vol ou substitution LTO depuis le coffre) — feront l'objet d'une cinématique d'attaque opérationnelle détaillée, conformément à la commande de l'étude.

Atelier 3 — Scénarios stratégiques

3.1 Finalité de l'atelier

L'atelier 3 d'EBIOS Risk Manager élabore les scénarios stratégiques, c'est-à-dire les chemins d'attaque à haute granularité que peuvent emprunter les sources de risques pour atteindre leurs objectifs visés. Le scénario stratégique ne décrit pas le détail technique (réservé à l'atelier 4), mais identifie les parties prenantes de l'écosystème mobilisées, les modes opératoires de premier ordre et la séquence logique permettant de relier une SR à un OV. Chaque scénario stratégique est qualifié par une gravité (reprise de la criticité des biens essentiels impactés) et par une appréciation de la pertinence (combinaison de la motivation, des ressources et des opportunités d'exécution offertes par l'écosystème).

3.2 Cartographie de l'écosystème — parties prenantes

L'écosystème de BIOÉNERGIE TECH au titre du projet SpainTurbine comprend les parties prenantes ci-dessous. Pour chacune, l'évaluation porte sur trois critères classiques EBIOS RM : la dépendance (D), la pénétration (P) et la maturité de sécurité (M), notés de 1 (faible) à 4 (très fort). La gravité de la partie prenante est obtenue en multipliant D × P et en pondérant par l'inverse de M.

Partie prenante	Rôle dans l'écosystème	D — Dépendance	P — Pénétration	M — Maturité	Niveau de menace écosystème
Armée espagnole / Autorité de sécurité espagnole	Client final, prescripteur de la classification « Confidencial ».	3	2	4	Modéré — maturité élevée
SpainTurbine (entité commerciale)	Intermédiaire contractuel, point d'entrée des correspondances classifiées.	3	3	3	Modéré — vecteur d'ingénierie sociale
Microsoft Update (chaîne MAJ Windows)	Source unique des correctifs téléchargés par le PC de mise à jour.	4	3	3	Élevé — risque supply chain
HP (constructeur des HP Elite 800 G9)	Fournisseur matériel, intervention firmware potentielle.	2	2	3	Modéré — risque firmware / SMBIOS
Dell (serveurs PowerEdge R470)	Fournisseur matériel, support iDRAC.	2	2	3	Modéré
Cisco (Switch 9200 et Firewall 1120)	Fournisseur réseau, firmware, IOS-XE.	2	2	3	Modéré — risque type CVE Cisco IOS-XE 2023-20198
S3Box / Hogo (station blanche)	Sous-traitant matériel et logiciel, mise à jour de signatures.	4	3	2	Élevé — point unique de filtrage des supports

Partie prenante	Rôle dans l'écosystème	D — Dépendance	P — Pénétration	M — Maturité	Niveau de menace écosystème
HPE (lecteur LTO-8 StoreEver)	Fournisseur du lecteur de bandes, microcode.	2	2	3	Modéré
IBM (cartouches LTO-8)	Fournisseur du média de sauvegarde.	1	1	3	Faible
HID Global (lecteurs biométriques Signo 25B)	Fournisseur sécurité physique, firmware et serveur de gestion.	3	2	3	Modéré — point critique IAM physique
Yubico (YubiKey C NFC FIDO2)	Fournisseur de l'authentifiant fort.	3	1	4	Faible — haute maturité
Fournisseur télécom local	Accès périodique au site pour travaux exceptionnels.	2	3	2	Élevé — accès physique privilégié
Sous-traitant matériel station blanche	Accès périodique au site, maintenance de la S3Box.	3	3	2	Élevé
Organisme d'audit / certification	Accès supervisé périodique, traitement de documentation classifiée.	2	2	3	Modéré
ProClean Services Alpes (femme de ménage)	Accès aux locaux corporate hors zone classifiée mais coactivité possible.	1	3	1	Modéré — ingénierie sociale, vol opportuniste
Voisinage industriel (CHEMICALIA, métallurgie, voie ferrée)	Coactivité physique, risques de sinistre induit.	1	1	1	Faible mais non négligeable (impact disponibilité)

Les parties prenantes notées « Élevé » constituent des points d'entrée privilégiés pour les sources de risques de l'atelier 2. Le sous-traitant station blanche, le fournisseur télécom et la chaîne Microsoft Update concentrent à eux seuls trois vecteurs de supply chain compromise dans un SI pourtant air-gappé. L'évaluation confirme que la sécurité du périmètre repose moins sur le cloisonnement réseau que sur la maîtrise des passerelles humaines et logistiques.

3.3 Scénarios stratégiques retenus

Quatre scénarios stratégiques majeurs sont retenus. Pour chacun d'eux, la « cyberbiographie de l'attaque » décrit le cheminement de la source de risque, depuis sa motivation initiale jusqu'à la matérialisation de l'événement redouté. Ces scénarios couvrent les couples SR/OV de priorité 1 et 2 identifiés à l'atelier 2.

3.3.1 Scénario stratégique SS1 — APT étatique étranger : exfiltration via flux MAJ et clé USB

Couplage : SR1.OV1 / SR1.OV2. Gravité estimée : 4 — Critique. Pertinence : 3 — Forte.

Cyberbiographie. Un service de renseignement étranger ciblé sur le programme drone européen identifie BIOÉNERGIE TECH comme fournisseur stratégique de SpainTurbine via la presse spécialisée, les déclarations DGA-DGE et le registre du commerce. Une cellule HUMINT documente l'organigramme de la zone classifiée (5 habilités), tandis qu'une cellule technique prépare un implant capable de transiter par la station blanche. L'implant peut être véhiculé par une compromission de la chaîne logicielle (signature volée à un prestataire en amont de Microsoft Update, technique attestée dans les rapports CISA AA21-008A et MITRE T1195.002), ou par une compromission matérielle (firmware d'un composant HP). Une fois le SI cloisonné infecté, l'implant est doté d'un canal asynchrone : il stocke les données à exfiltrer sur la prochaine clé USB sortante, voire dans les paquets de mise à jour eux-mêmes lors du cycle inverse, garantissant à l'attaquant une exfiltration discrète sur plusieurs mois.

3.3.2 Scénario stratégique SS2 — Initié sous coercition : vol physique LTO et clés

Couplage : SR2.OV1 / SR2.OV3. Gravité estimée : 4 — Critique. Pertinence : 3 — Forte.

Cyberbiographie. Une source adverse — service étranger, concurrent ou réseau criminel — conduit un travail de profilage OSINT sur les cinq personnels habilités (LinkedIn, réseaux sociaux, presse locale chambérienne, annuaire ENSI). Elle identifie une vulnérabilité humaine — dette de jeu, conjoint étranger, enfant malade, mécontentement professionnel — et approche directement la cible la plus à même de produire un résultat : l'administrateur système, qui dispose simultanément des privilèges Active Directory, des accès au coffre Fichet-Bauche, du droit de manipuler les LTO et du coffre à six compartiments où sont stockées les clés de chiffrement. L'initié, sous coercition, exfiltre une cartouche LTO complète lors d'une rotation hebdomadaire en la substituant par une cartouche identique vidée. Il fournit en parallèle une copie des clés de chiffrement extraites du coffre à six compartiments. La donnée classifiée est ainsi sortie du site sous une forme exploitable hors ligne, sans qu'aucun flux réseau ne soit observable par le SIEM ELK.

3.3.3 Scénario stratégique SS3 — Cybercriminel ransomware via supply chain station blanche

Couplage : SR3.OV1. Gravité estimée : 4 — Critique. Pertinence : 2 — Modérée (l'air-gap limite fortement la propagation des kits ransomware grand public).

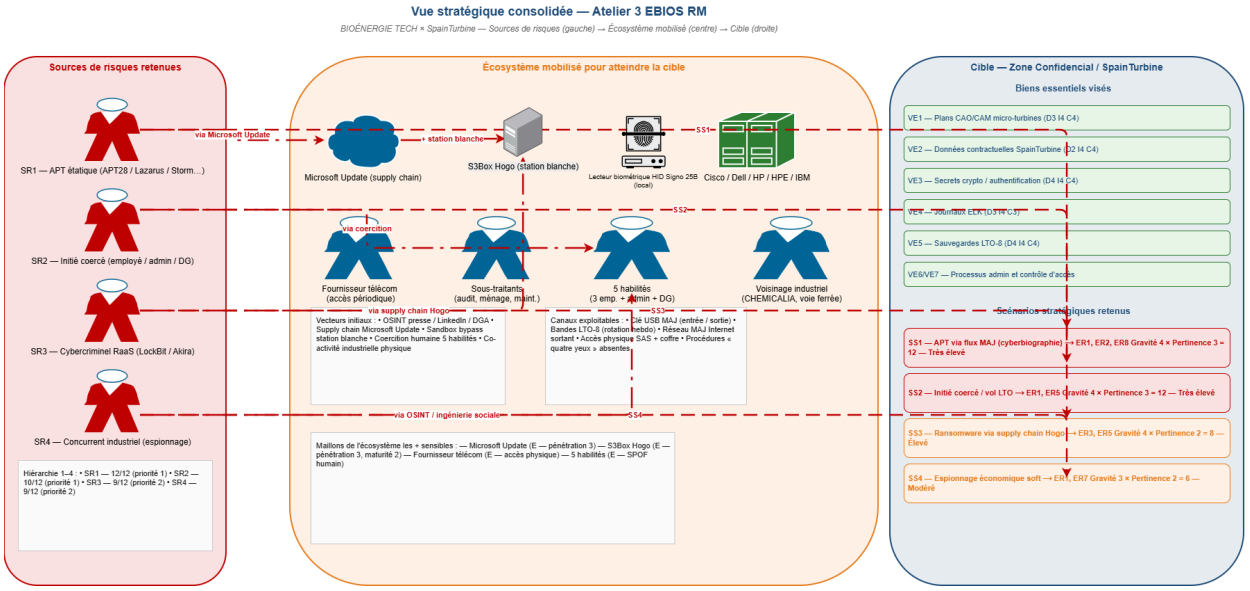
Cyberbiographie. Un groupe RaaS opportuniste, ne ciblant pas spécifiquement BIOÉNERGIE TECH, compromet en amont la chaîne logicielle du sous-traitant station blanche S3Box / Hogo (mise à jour de signatures distribuée à l'ensemble des clients). Lors de la prochaine mise à jour de signatures importée par le PC MAJ et passée en station blanche, le payload est injecté dans la station blanche elle-même puis dans le SI cloisonné via la première clé USB sortante de la station vers un poste utilisateur. L'attaquant pivote ensuite vers la VM Active Directory, exécute un déploiement de chiffrement via GPO,

atteint le serveur principal et son redondant, et présente une demande de rançon en double extorsion (chiffrement + menace de fuite des données classifiées « Confidencial »).

3.3.4 Scénario stratégique SS4 — Concurrent industriel : espionnage économique soft

Couplage : SR4.OV1 / SR4.OV2. Gravité estimée : 3 — Majeure. Pertinence : 2 — Modérée.

Cyberbiographie. Un concurrent étranger des fournisseurs de drones tactiques approche par voie indirecte un ancien salarié non habilité du projet (par exemple un ingénieur ayant participé à l'étude amont des micro-turbines) ou un sous-traitant audit. La technique privilégiée est l'ingénierie sociale ciblée (faux recruteur, fausse « opportunité d'expert » sur LinkedIn ou conférence technique) afin d'obtenir des informations partielles (architectures, formulations, paramètres de procédés) sans nécessairement pénétrer le SI cloisonné. Le risque complémentaire est celui d'une fuite contrôlée à la presse spécialisée mettant en cause la sécurité du fournisseur, afin d'amener SpainTurbine à dénoncer le contrat au profit du concurrent.



3.4 Évaluation de la gravité des scénarios stratégiques

Scénario stratégique	SR — OV associé	Biens essentiels impactés	Gravité (1–4)	Pertinence (1–4)	Niveau de risque agrégé
SS1 — APT étatique via flux MAJ	SR1.OV1, SR1.OV2	VE1, VE3, VE4, VE5, VE6	4	3	**12 — Très élevé**
SS2 — Initié coercitif / vol LTO	SR2.OV1, SR2.OV3	VE1, VE3, VE5	4	3	**12 — Très élevé**
SS3 — Ransomware via supply chain station blanche	SR3.OV1	VE1 à VE6	4	2	**8 — Élevé**
SS4 — Espionnage économique indirect	SR4.OV1, SR4.OV2	VE1, VE2	3	2	6 — Modéré

Les scénarios SS1 et SS2, classés « Très élevé », justifient le développement détaillé d'une cinématique d'attaque à l'atelier 4. SS3 et SS4 sont traités au plan d'action de l'atelier 5 par des mesures partagées avec les deux scénarios précédents (durcissement de la station blanche, programme insider threat, sensibilisation OSINT).

Atelier 4 — Scénarios opérationnels

4.1 Finalité et méthodologie

L'atelier 4 traduit les scénarios stratégiques retenus en cinématiques d'attaque opérationnelles. À ce niveau, l'étude se positionne du point de vue de l'attaquant et déroule chaque étape technique et physique : reconnaissance, accès initial, persistance, mouvement latéral, collecte, exfiltration et couverture. La granularité retenue est compatible avec la matrice MITRE ATT&CK pour les phases logiques et avec le référentiel ANSSI EBIOS RM pour les phases physiques. Chaque scénario opérationnel s'achève par l'identification des vulnérabilités exploitées et par une cotation de la vraisemblance selon l'échelle à quatre niveaux ANSSI.

4.1.1 Échelle de vraisemblance

Niveau	Libellé	Définition opérationnelle
V1	Minimal	L'attaque exige des ressources, une connaissance et des opportunités d'accès qui dépassent largement celles de la source de risque considérée.
V2	Significatif	L'attaque est techniquement faisable mais exige une coordination avancée et plusieurs prérequis.
V3	Fort	L'attaque est documentée dans des cas réels comparables ; les ressources requises sont à la portée de la source de risque.
V4	Maximal	L'attaque est attestée dans des incidents similaires ; aucun prérequis majeur n'est nécessaire au-delà de la motivation.

4.2 Scénario opérationnel SO1 — Air-gap bypass via flux de mise à jour et clé USB

Référence stratégique : SS1 (SR1.OV1 + SR1.OV2). Cible : exfiltration des plans CAO/CAM des micro-turbines et implantation d'un implant persistant. Hypothèse adverse : APT étatique étranger, ressources extrêmes, capacité d'opérations supply chain et cyber simultanées.

4.2.1 Phase 1 — Reconnaissance externe (préparation à long terme)

1. OSINT métier : exploitation des publications presse régionale (Le Dauphiné Libéré, L'Usine Nouvelle) annonçant le contrat SpainTurbine de 1,2 M€ et identifiant BIOÉNERGIE TECH comme sous-traitant défense.
2. OSINT humain : identification des cinq personnels habilités via LinkedIn, salons professionnels (Forum DGA Innovation, Eurosatory), conférences ENSI, articles « ils nous ont rejoints ».
3. OSINT technique : identification de l'écosystème fournisseur — HP Elite 800 G9, Cisco Catalyst 9200, Cisco Secure Firewall 1120, S3Box Hogo, Dell PowerEdge R470 — via offres d'emploi (« administrateur Cisco 9200 et Dell iDRAC »), via les marchés publics, via les rapports d'audit RGPD publiquement déposés à la CNIL.

4. Phase « passive footprinting » : observation du site Chambéry, des horaires de livraison, des sous-traitants (camion ProClean Services Alpes, ThermoVent Industrie, DataSys Rhône-Alpes), identification du créneau d'intervention de la station blanche.

4.2.2 Phase 2 — Préparation de la charge utile (kill chain MITRE ATT&CK Resource Development)

5. Développement d'un implant Windows en deux étapes : un dropper en mode utilisateur signé avec un certificat dérobé à un éditeur tiers (technique T1553.002), et un payload kernel-mode signé Microsoft (cas similaire à FiveSys, 2021, ou à FudModule, 2024).
6. Le payload est conçu pour : (i) détecter le contexte « air-gap », (ii) journaliser silencieusement les accès aux fichiers .step, .iges, .dwg, .dwf, .catpart, .pdf classifiés, (iii) collecter par incréments les données dans une zone chiffrée du registre Windows, (iv) attendre l'apparition d'un support amovible étiqueté « MAJ » et y déposer la collecte chiffrée par stéganographie dans un fichier .cab.
7. Compromission, en amont, d'un fournisseur tiers de Microsoft Update — soit par achat sur un broker d'accès initial, soit par compromission d'un signataire WSUS legitime — permettant d'injecter le payload dans un correctif KBxxxxxxx signé Microsoft.
8. Adaptation polymorphique du dropper de manière à éviter les signatures statiques de la station blanche S3Box Hogo : empaquetage Sektor7-like, chiffrement par clé dérivée du nom de la KB, hooking syscall AMSI bypass.

4.2.3 Phase 3 — Accès initial et delivery

9. Téléchargement légitime du correctif piégé par le PC MAJ via le pare-feu Cisco Secure Firewall 1120 (flux F01 — HTTPS sortant vers le serveur Microsoft Update officiel ; l'allowlisting au sens du DAT ne distingue pas un payload Microsoft légitime d'un payload Microsoft compromis en amont).
10. Validation manuelle de l'opérateur : vérification du hash du paquet KB depuis le bulletin Microsoft Security ; le hash correspond, l'opérateur valide (signature et hash légitimes — la compromission est upstream).
11. Copie du paquet vers une clé USB dédiée (flux F02). L'administrateur respecte la procédure PO-STATION-BLANCHE et insère la clé sur la station blanche S3Box Hogo.
12. La station blanche analyse la clé USB. Les signatures connues sont inopérantes (payload empaqueté avec une clé dérivée). Aucune sandbox dynamique n'est instrumentée sur la S3Box dans la configuration de référence ; le payload n'est exécuté qu'au prochain redémarrage, postérieur à l'analyse. La clé est validée et marquée « clean ».
13. La clé USB est insérée sur le PC employé. Le payload se déclenche au montage via une vulnérabilité de parsing de fichier .lnk (équivalent CVE-2024-38112 ou successeur) ou via une politique GPO autorisant l'exécution de .msi signés Microsoft sur la chaîne MAJ.

4.2.4 Phase 4 — Exécution et persistance

14. Le dropper s'installe en service Windows masqué sous un nom légitime (svchost-like) avec déclenchement par tâche planifiée à horaire variable pour brouiller la détection.

15. Élévation de privilèges via une vulnérabilité Print Spooler dérivée (T1068) ou via une chaîne UAC bypass connue.
16. Persistance double : (i) modification d'une clé HKLM\…\Run, (ii) création d'un compte fantôme « svc-update-host » dans Active Directory par injection LDAP, masqué dans l'OU « Computers » et exempté des audits hebdomadaires.

4.2.5 Phase 5 — Mouvement latéral et privilège AD

17. Reconnaissance interne via BloodHound miniature embarqué : énumération SMB sur le serveur de partage de fichiers (F09/F10), énumération LDAP sur l'AD (F01).
18. Capture d'un ticket Kerberos via DCSync sur la VM Active Directory (préalable : le compte fantôme dispose des droits Replicating Directory Changes faute de durcissement Tier 0).
19. Forge d'un Golden Ticket (T1558.001) à partir du hash krbtgt. L'attaquant dispose désormais d'un accès durable et imperceptible au domaine.
20. Pivot vers la VM Sauvegarde via SMB ; lecture des inventaires LTO et identification des cartouches contenant la dernière complète.

4.2.6 Phase 6 — Collecte

21. Inventaire silencieux des fichiers CAO/CAM sur la VM Partage de fichiers : extensions .catpart, .catproduct, .step, .iges, .pdf signés, .docx classifiés.
22. Marquage des fichiers d'intérêt et collecte différée : seul un sous-ensemble (≈ 200 Mo) est exfiltré à chaque cycle pour ne pas dépasser la taille moyenne attendue d'un correctif Microsoft.
23. Chiffrement local de la collecte par AES-256 avec une clé dérivée d'une graine embarquée par l'opérateur adverse ; stockage dans un fichier .cab masqué dans le répertoire %TEMP%.

4.2.7 Phase 7 — Exfiltration (canal asynchrone air-gap)

24. Lors de la prochaine validation de correctif, l'opérateur insère une clé USB sortante (procédure normale F02 inversée). Le payload détecte le montage et écrit la collecte dans un fichier d'apparence légitime (.cab signé apparente).
25. La clé est analysée à nouveau par la station blanche, qui ne reconnaît pas comme malveillant un .cab signé Microsoft.
26. La clé est insérée sur le PC MAJ pour archivage (ou par réutilisation involontaire de la même clé). À la connexion Internet suivante, le payload présent sur le PC MAJ établit un canal C2 via DNS-over-HTTPS vers update.microsoft.com (ou un sous-domaine compromis en amont).
27. L'exfiltration s'étale sur plusieurs semaines pour rester sous les seuils volumétriques observables.

4.2.8 Phase 8 — Couverture et résilience

28. Suppression sélective des entrées d'audit Windows par utilisation d'un compte à privilèges Tier 0 légitime (le compte fantôme injecté).
29. Maintien d'au moins deux mécanismes de persistance hétérogènes pour résister à une éradication partielle.

30. Falsification ciblée des journaux ELK : insertion d'événements « bénins » destinés à diluer les tentatives d'authentification suspectes ; pas de tentative de suppression complète, susceptible de déclencher une alerte d'intégrité Kibana.

4.2.9 Vulnérabilités exploitées (cartographie)

Réf.	Vulnérabilité exploitée	Famille	Référence
V1.1	La station blanche S3Box Hogo repose principalement sur des signatures statiques ; absence de sandbox dynamique avec mesure comportementale.	Détection	ANSSI Guide stations blanches 2022
V1.2	La validation par hash ne protège pas d'une compromission upstream de la chaîne de signature.	Supply chain	MITRE T1195.002
V1.3	Le PC MAJ dispose d'une connexion sortante Internet non limitée à l'analyse de paquet profonde sortante.	Réseau	ANSSI NT-022
V1.5	L'Active Directory n'applique pas formellement le modèle Tier 0/1/2 ni les Privileged Access Workstations (PAW) ; un compte standard à privilèges peut DCSync.	IAM	ANSSI Guide AD 2022
V1.6	Absence de monitoring du krbtgt et des replications Directory Changes au-delà de la simple journalisation Kibana.	Détection	Microsoft Security Tech Center
V1.7	Pas de hash de référence des binaires Microsoft Update stockés hors bande pour comparaison.	Intégrité	ANSSI Hash-NT
V1.8	Pas de DLP en sortie sur les clés USB (volumétrie, signature, contenu).	Fuite	ANSSI DLP-NT 2024

4.2.10 Cotation de la vraisemblance SO1

Critère	Évaluation	Justification
Motivation adverse	4 — Très forte	Intérêt stratégique direct pour un service étatique : drones militaires européens en production active.
Capacités techniques requises	Très élevées	Compromission supply chain + bypass station blanche + post-exploitation AD.
Opportunités d'exécution	Modérées à élevées	Présence d'un canal MAJ avec sortie Internet, station blanche non sandboxée, MAJ téléchargées hebdomadairement.
Probabilité de détection précoce	Faible	Aucun EDR mentionné, aucun monitoring krbtgt avancé, télémétrie limitée aux signatures statiques.
Vraisemblance retenue	**V3 — Forte**	Compatibilité avec les modes opératoires APT documentés (SolarWinds 2020, 3CX 2023).

4.3 Scénario opérationnel SO2 — Initié sous coercition : vol de cartouche LTO et clés de chiffrement

Référence stratégique : SS2 (SR2.OV1 + SR2.OV3). Cible : exfiltrer une sauvegarde hebdomadaire complète du SI cloisonné en sortant physiquement une cartouche LTO-8 et les clés de chiffrement permettant son exploitation hors site. Hypothèse adverse : initié coerćé par un service ou un réseau adverse — cible privilégiée : l'administrateur système.

4.3.1 Phase 1 — Profilage et ciblage humain

31. Constitution d'un dossier OSINT sur les cinq personnels habilités : LinkedIn, presse locale (Le Dauphiné, France 3 Alpes), réseaux sociaux personnels, état civil reconstitué, dettes ou difficultés familiales identifiables.
32. Identification de la cible la plus rentable : l'administrateur système. Justification : porteur simultané du domaine Active Directory, des accès au coffre Fichet-Bauche Carena, du droit d'extraction d'une LTO et de la connaissance des clés stockées dans le coffre à six compartiments.
33. Identification d'un levier de coercition exploitable : par exemple un enfant à charge en clinique privée pour pathologie lourde, ou un conjoint étranger dont la situation administrative française est fragile, ou des dettes de jeu remontant à un fichier FICOBA.

4.3.2 Phase 2 — Approche et recrutement

34. Approche directe en milieu civil hors site : conférence professionnelle, salon Eurosatory, salon Milipol, ou par tiers « consultant en intelligence économique ».
35. Présentation de la coercition : combinaison kompromat (photos compromettantes fabriquées, chantage familial) + incitation financière (versement initial de 5 000 € à 10 000 €, prime à livraison de 50 000 € à 100 000 €).
36. Engagement : remise d'une cartouche LTO-8 hebdomadaire complète, accompagnée des clés de chiffrement permettant son exploitation hors ligne.

4.3.3 Phase 3 — Préparation matérielle de l'opération

37. Acquisition par l'adversaire d'une cartouche IBM LTO-8 vierge identique au modèle exploité (même référence, étiquetage personnalisé pré-imprimé pour assurer une substitution indétectable visuellement).
38. Formation de l'initié à la séquence de substitution et à la manipulation discrète : choix du moment (rotation hebdomadaire du vendredi soir hors heures ouvrées, lorsque le DG n'est pas sur site), simulation préalable hors site, gestion du stress.
39. Acquisition par l'adversaire d'un lecteur HPE StoreEver LTO-8 Ultrium 30750 (≈ 6 000 € HT, achetable d'occasion sans formalité particulière) pour exploitation hors ligne.

4.3.4 Phase 4 — Exécution physique sur site

40. Vendredi soir, fin de production : l'administrateur déclenche la sauvegarde complète hebdomadaire sur le lecteur HPE Ultrium 30750. La PSSI prévoit que les bandes soient déposées dans le coffre Fichet-Bauche Carena à l'issue de la sauvegarde.

41. L'administrateur est seul dans le local sécurité — la procédure « quatre yeux » de la PSSI § 4.1.2 n'est obligatoire que pour des actions logiques irréversibles ; aucune procédure n'impose un double contrôle physique pour le dépôt en coffre.
42. Ouverture du coffre Fichet-Bauche Carena ; la caméra Axis M4216-V couvre le SAS d'entrée mais pas l'intérieur du local sécurité ni l'angle du coffre. La séquence n'est pas filmée.
43. Substitution de la cartouche LTO de la semaine N par la cartouche vierge préparée hors site. La cartouche dérobée porte les sauvegardes complètes de la semaine.
44. Ouverture du coffre à six compartiments : extraction d'une copie des clés de chiffrement matériel LTO de la semaine (la PSSI permet à un administrateur de manipuler sa clé). Photographie discrète à l'aide d'un objet personnel autorisé sur site.
45. Fermeture des coffres et journalisation conforme dans ELK (mouvement de bande enregistré au registre, mais sans contrôle d'intégrité du contenu).
46. Sortie du SAS via les lecteurs biométriques HID Signo 25B et la caméra Axis : la cartouche LTO-8 mesure 102 × 105 × 22 mm pour 250 g, dissimulable dans une serviette ou un manteau d'hiver ; aucune procédure de fouille ni de détection métal n'est en place à la sortie.

4.3.5 Phase 5 — Exploitation hors site

47. Remise du jeu cartouche + clés au commanditaire en lieu neutre (parking, salon, drop physique).
48. Lecture sur le lecteur HPE Ultrium 30750 acquis par l'adversaire ; déchiffrement matériel à l'aide des clés extraites du coffre à six compartiments.
49. Exfiltration vers l'infrastructure adverse : indexation des fichiers CAO/CAM, des courriers SpainTurbine, des configurations Cisco et Dell de référence.

4.3.6 Phase 6 — Couverture et tenue dans la durée

50. La cartouche substituée est étiquetée pour passer un éventuel contrôle de prise en main. La détection éventuelle n'interviendra qu'à l'occasion du prochain test de restauration partielle (mensuel) — donc dans un délai allant de 0 à 30 jours.
51. L'initié peut renouveler l'opération sur plusieurs semaines tant que la procédure de double contrôle physique reste absente. Une fois la défection identifiée, l'attaquant dispose déjà d'un instantané complet du projet.
52. L'initié peut, en complément, retarder un test de restauration au prétexte d'une indisponibilité matérielle, en exploitant son rôle d'administrateur.

4.3.7 Vulnérabilités exploitées (cartographie)

Réf.	Vulnérabilité exploitée	Famille	Référence
V2.1	Absence de procédure formelle « quatre yeux » sur tout accès au coffre Fichet-Bauche et au coffre à six compartiments.	Organisationnel	ANSSI Guide PSSI § Quatre yeux
V2.2	Cartouches LTO non scellées par scellés numérotés infalsifiables ; absence de hash de référence stocké hors bande.	Sécurité physique	ANSSI Sauvegardes 2023

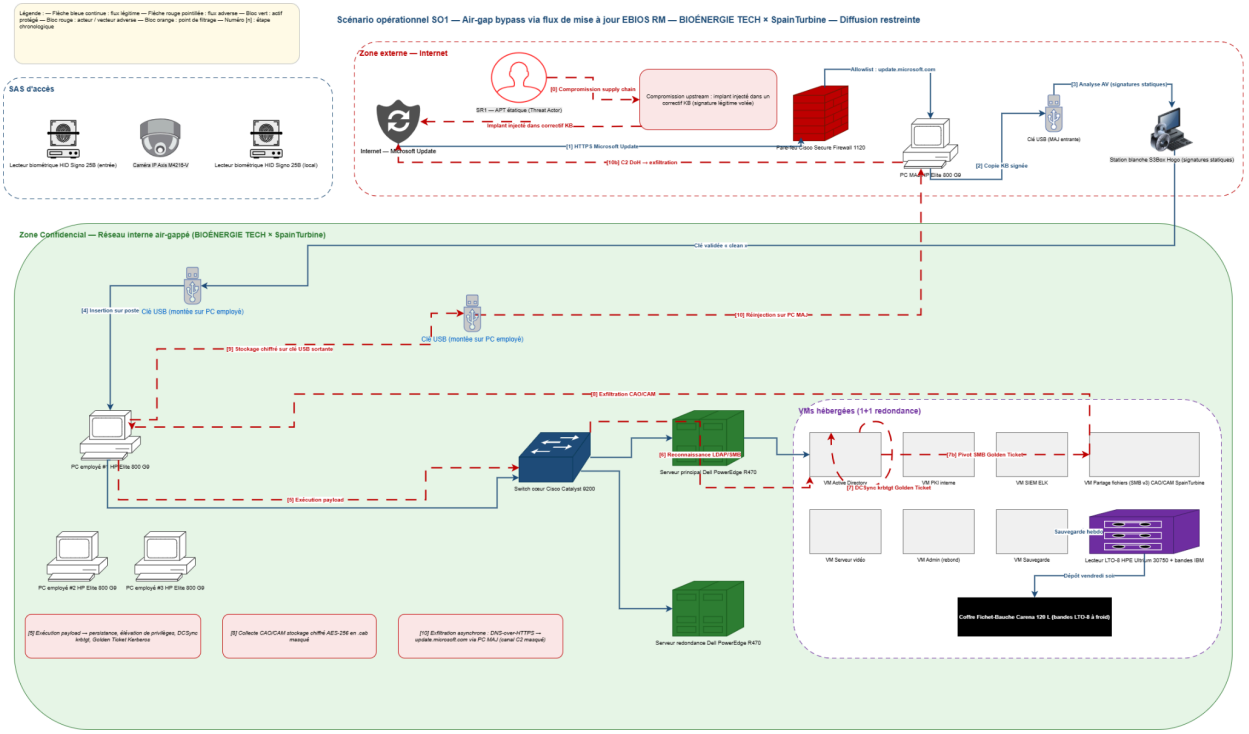
Réf.	Vulnérabilité exploitée	Famille	Référence
V2.3	Vidéosurveillance limitée au SAS d'entrée ; angle mort sur l'intérieur du local sécurité, sur le coffre LTO et sur le coffre à six compartiments.	Sécurité physique	ANSSI Vidéoprotection 2021
V2.4	Co-localisation des secrets : les clés de chiffrement matériel LTO sont stockées dans le même périmètre physique que les LTO qu'elles protègent.	Cryptographie	ANSSI Recommandations clés-NT
V2.5	Aucun contrôle de sortie corporelle : pas de fouille aléatoire, pas de détection métal sur les badges/sorties.	Sécurité physique	Doctrine défense MILSEC4
V2.6	Concentration extrême des privilèges sur l'administrateur unique (SPOF humain) ; pas de séparation des rôles (SoD) entre administration système et gestion des sauvegardes.	Gouvernance	ISO 27002:2022 § 5.3
V2.7	Programme insider threat limité : absence de vetting psychologique périodique, absence de procédure d'alerte interne (whistleblowing) éprouvée.	Humain	CERT Carnegie Mellon Insider Guide v6
V2.8	Test de restauration complet annuel et partiel mensuel : fenêtre de détection trop longue pour révéler une substitution hebdomadaire.	Détection	ANSSI Sauvegardes 2023

4.3.8 Cotation de la vraisemblance SO2

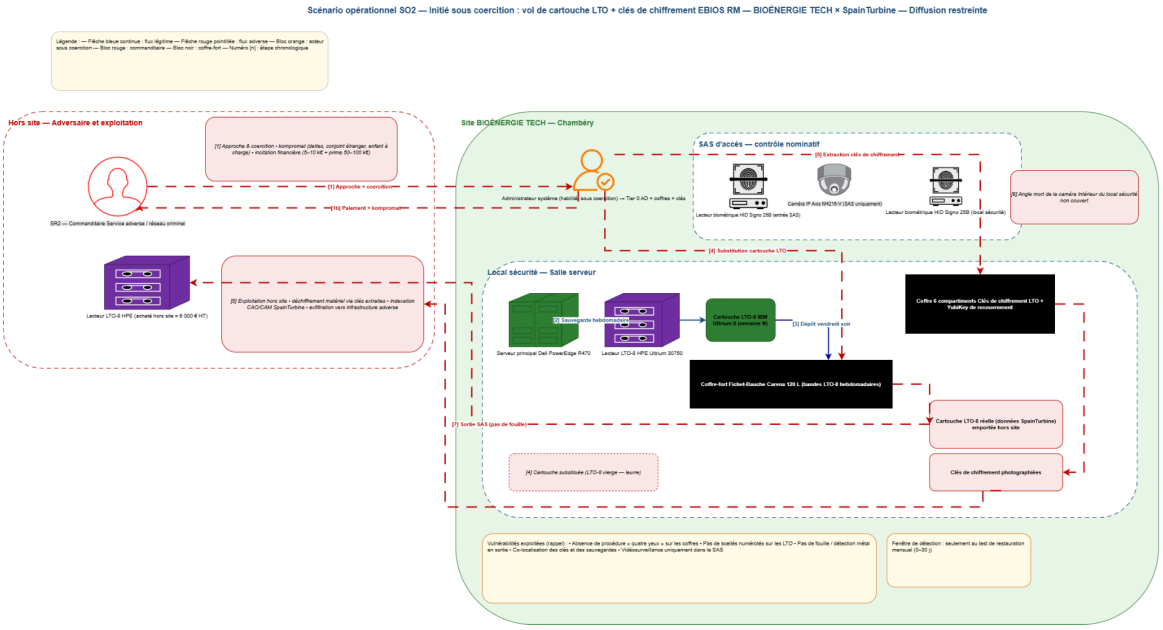
Critère	Évaluation	Justification
Motivation adverse	3 à 4	Intérêt stratégique direct ; le coût d'une opération humaine est largement inférieur à celui d'une opération supply chain technique.
Faisabilité technique	Très élevée	Aucune dépendance à un 0-day ou à un implant ; opération essentiellement humaine et physique.
Opportunités d'exécution	Élevées	Rotation hebdomadaire prévisible, pas de quatre yeux, vidéosurveillance partielle, pas de fouille.
Probabilité de détection précoce	Faible	Détection possible uniquement au test de restauration mensuel.
Vraisemblance retenue	**V3 — Forte**	Cas comparables en industrie défense (Dassault 2018, Naval Group, dossiers DGSI).

4.4 Schéma des attaques qui ont été retenues

4.4.2 Modèle Draw.io du scénario SO1 (air-gap bypass via MAJ)



4.4.3 Modèle Draw.io du scénario SO2 (vol LTO par initié coercé)



Atelier 5 — Traitement des risques

5.1 Finalité et stratégie générale de traitement

L'atelier 5 d'EBIOS Risk Manager arrête, pour chaque scénario stratégique et opérationnel retenu, une stratégie de traitement et un plan d'action concret. Quatre stratégies sont mobilisables conformément à l'ISO/IEC 27005 et au guide ANSSI EBIOS RM : éviter le risque (en supprimant l'activité ou l'actif support à l'origine de la menace), réduire le risque (par mesures techniques, organisationnelles et physiques), transférer le risque (assurance cyber, contractualisation) ou accepter le risque résiduel (documenté, daté, validé par la Direction Générale).

Compte tenu de la classification « Confidencial » des données, de la sensibilité défense du projet SpainTurbine et de l'engagement contractuel pris envers l'autorité espagnole, la doctrine retenue par BIOÉNERGIE TECH est majoritairement la réduction du risque. L'évitement est mobilisé pour les scénarios à très forte gravité dont le coût d'une mesure de réduction excéderait le bénéfice attendu (par exemple : suppression pure et simple du flux Internet sortant pour le PC MAJ s'il est démontré que les WSUS hors ligne couvrent le besoin). Le transfert est mobilisé sous la forme d'une police d'assurance cyber dont la franchise et le plafond restent à arbitrer. L'acceptation est réservée à des risques résiduels nominatifs validés par décision formelle du Directeur Général après visa du RSSI.

5.2 Échelle de priorité des mesures

Priorité	Délai cible de mise en œuvre	Catégorie EBIOS RM	Validation requise
P1 — Critique	≤ 3 mois après publication de l'étude	Mesures couvrant les scénarios cotés ≥ 10 (SS1, SS2)	Directeur Général + RSSI
P2 — Élevée	≤ 6 mois	Mesures couvrant les scénarios cotés 7 à 9 (SS3, SS4)	RSSI + Administrateur
P3 — Renforcement	≤ 12 mois	Mesures de durcissement préventif et amélioration continue	RSSI
P4 — Veille	Suivi permanent	Mesures non encore implémentables sans investissement majeur	RSSI + Direction Financière

5.3 Plan d'action — Mesures techniques logiques

Réf.	Mesure de sécurité	Risque(s) traité(s)	Référentiel ANSSI / ISO	Priorité	Responsable	Indicateur de suivi
MT-01	Mise en œuvre du modèle de tiering Microsoft Tier 0 / 1 / 2 sur l'Active Directory : isolement des comptes Administrateur du domaine sur Tier 0, blocage des authentifications interactives sur Tier 0 depuis des postes non PAW, refus NTLM, GPO « Authentication Silo ».	SO1 — V1.5, V1.6	ANSSI Guide AD 2022 § 3.2	P1	Administrateur + RSSI	100 % comptes Tier 0 dans silo dédié
MT-02	Déploiement de PAW (Privileged Access Workstations) dédiées à l'administration AD, sans navigation Internet ni messagerie, durcies selon STIG Microsoft et hors zone utilisateur.	SO1 — V1.5	ANSSI NT-014 ; Microsoft PAW	P1	Administrateur	Nombre de PAW déployées (cible : 2)
MT-03	Installation d'un EDR comportemental (type ESET PROTECT Enterprise / SentinelOne / Microsoft Defender for Endpoint en mode air-gap) sur l'ensemble des postes, serveurs et VM, avec règles de détection comportementale et alimentation des journaux dans ELK.	SO1 — V1.4 ; SO3 (ransomware)	ANSSI EDR-NT-2023	P1	Administrateur	Couverture EDR ≥ 100 % des actifs IT
MT-04	Whitelisting applicatif strict via Windows Defender Application Control (WDAC) ou AppLocker en mode « Audit » puis « Enforce » sur tous les postes et serveurs de la zone classifiée. Seuls les binaires signés validés sont exécutables.	SO1 — V1.2, V1.4	ANSSI Guide WDAC 2023	P1	Administrateur	Nombre d'exceptions documentées ≤ 5
MT-05	Renforcement de la station blanche S3Box Hogo : adjonction d'une sandbox dynamique offline (analyse comportementale 90 s par fichier), multi-moteurs antivirus (≥ 4), détection YARA, calcul de hash et vérification contre une base de hash légitimes Microsoft Update.	SO1 — V1.1 ; SO3 — supply chain	ANSSI Guide stations blanches 2022	P1	Administrateur + Sous-traitant Hogo	% supports analysés en sandbox dynamique = 100 %
MT-06	Mise en place d'un DLP USB couplé à WDAC : (i) chiffrement obligatoire BitLocker To Go sur toute clé USB ; (ii) journalisation horodatée du contenu (liste, taille, hash) à chaque montage et	SO1 — V1.8 ; SO2 — V2.5	ANSSI USB-NT 2024	P1	Administrateur	% clés USB enrôlées AD = 100 %

Réf.	Mesure de sécurité	Risque(s) traité(s)	Référentiel ANSSI / ISO	Priorité	Responsable	Indicateur de suivi
	démontage ; (iii) blocage de toute clé non enrôlée nominativement.					
MT-07	Activation et durcissement du monitoring krbtgt : surveillance des replications Directory Changes, alertes Kibana sur DCSync, rotation semi-annuelle du mot de passe krbtgt (deux fois en deux semaines).	SO1 — V1.5, V1.6	ANSSI Guide AD 2022 § 4.4	P1	Administrateur	Délai entre rotations krbtgt ≤ 180 j
MT-08	Calcul, à l'issue de chaque sauvegarde LTO, d'un hash SHA-256 du contenu de la bande, signé par la PKI interne et stocké hors bande dans le coffre à six compartiments. Vérification systématique avant tout test de restauration.	SO2 — V2.2, V2.8 ; ER2	ANSSI Sauvegardes 2023 § 5.4	P1	Administrateur	% bandes ayant un hash signé = 100 %
MT-09	Test de restauration partielle hebdomadaire (au lieu de mensuelle) sur la VM Sauvegarde redondante, avec vérification du hash de bande et comparaison aux fichiers d'origine.	SO2 — V2.8 ; ER2	ANSSI Sauvegardes 2023 § 6	P1	Administrateur	Fréquence des tests ≥ 1/sem ; taux de succès ≥ 99 %
MT-10	Désactivation du téléchargement Internet automatique sur le PC MAJ ; alimentation des correctifs Microsoft Update via un dépôt WSUS hors ligne synchronisé manuellement par l'administrateur tous les jeudis matin.	SO1 — V1.2, V1.3	ANSSI MAJ-NT 2023	P2	Administrateur	Nombre de téléchargements directs / mois = 0
MT-11	Mise en place de règles de détection UEBA dans ELK : anomalie d'horaire d'authentification, mouvements de fichiers atypiques (> 100 fichiers en 5 min), accès simultanés depuis plusieurs adresses MAC, créations de comptes hors heures ouvrées.	SO1 — V1.4 ; SO2 — V2.7	ANSSI NT-022 § 3	P2	RSSI + Administrateur	Nombre de règles UEBA actives ≥ 20
MT-12	Hardening Cisco Catalyst 9200 et Secure Firewall 1120 : désactivation des services inutiles, contrôle TACACS+ ou RADIUS dédié, mise à jour IOS-XE corrigeant CVE-2023-20198 et CVE-2023-20273, configuration safeguard sous gabarit ANSSI.	SO1 — V1.3 ; SO3	ANSSI Guide Cisco 2022	P2	Administrateur	Score CIS Benchmark ≥ 90 %

Réf.	Mesure de sécurité	Risque(s) traité(s)	Référentiel ANSSI / ISO	Priorité	Responsable	Indicateur de suivi
MT-13	Cloisonnement formel des VM : VLAN distincts, ACL inter-VM bloquantes par défaut, désactivation du clipboard et du drag-and-drop hyperviseur, mise à jour de l'hyperviseur Dell suivant le calendrier MISRA-CVE.	SO1 — escalade VM	ANSSI Cloisonnement-NT 2024	P2	Administrateur	Nombre de flux inter-VM non documentés = 0
MT-14	Activation systématique de la signature des événements ELK (mécanisme « audit log signing » Elasticsearch) et alerte Kibana à la moindre tentative de modification rétroactive.	SO1 — phase couverture	ANSSI NT-022 § 5	P2	Administrateur	100 % logs signés
MT-15	Mise en place de honey-tokens dans l'Active Directory et la VM Partage de fichiers : comptes leurres jamais utilisés, fichiers leurres à noms attractifs ; toute interaction génère une alerte Kibana critique.	SO1, SO2 — détection précoce	MITRE D3FEND DEC-0042	P3	Administrateur	Nombre de honey-tokens ≥ 10 ; alertes annuelles tracées

5.4 Plan d'action — Mesures physiques

Réf.	Mesure de sécurité	Risque(s) traité(s)	Référentiel ANSSI / ISO	Priorité	Responsable	Indicateur de suivi
MP-01	Renforcement de la vidéosurveillance : ajout de deux caméras IP supplémentaires (modèle Axis P3265-LV ou équivalent) couvrant l'intérieur du local sécurité, l'angle du coffre Fichet-Bauche et le coffre à six compartiments. Enregistrement 90 jours sur VM Vidéo dédiée.	SO2 — V2.3	ANSSI Vidéoprotection 2021 § 4	P1	Administrateur + RSSI	Couverture vidéo zones sensibles ≥ 95 %
MP-02	Procédure « quatre yeux » obligatoire pour toute ouverture du coffre Fichet-Bauche Carena et du coffre à six compartiments : présence simultanée et enregistrée de l'administrateur et du Directeur Général (ou d'un suppléant désigné par décision formelle).	SO2 — V2.1, V2.4, V2.6	ANSSI PSSI-NT § Quatre yeux ; ISO 27002 § 5.3	P1	Direction Générale	0 ouverture en mode mono-opérateur
MP-03	Apposition sur chaque cartouche LTO-8 d'un scellé numéroté infalsifiable (modèle Tyden-Brammall ou équivalent défense) ; consignation du	SO2 — V2.2	MILSEC4 Doctrine défense	P1	Administrateur	100 % bandes scellées ; 0

Réf.	Mesure de sécurité	Risque(s) traité(s)	Référentiel ANSSI / ISO	Priorité	Responsable	Indicateur de suivi
	numéro dans le registre ELK lors de tout mouvement.					scellé brisé non justifié
MP-04	Mise en place d'un détecteur de masses métalliques en sortie de SAS et fouille aléatoire (au moins 10 % des sorties) selon un tirage horodaté ; mention contractuelle pour les sous-traitants.	SO2 — V2.5	MILSEC4 Doctrine défense	P2	RSSI	% sorties contrôlées ≥ 10 %
MP-05	Géolocalisation des cartouches LTO actives par étiquette RFID passive 13,56 MHz et antenne de détection en sortie SAS ; toute sortie non autorisée déclenche une alarme.	SO2 — V2.2, V2.5	ANSSI IoT-NT 2023 (adapté)	P3	Administrateur	100 % bandes étiquetées
MP-07	Mise en place d'un sas d'isolement physique à double porte interlock entre l'extérieur et le local sécurité ; ouverture d'une porte impossible tant que l'autre n'est pas refermée et verrouillée.	SO2 — physique général	Doctrine MILSEC4 ; IGI 1300	P3	Direction Générale	Conformité MILSEC4 confirmée par audit
MP-08	Inspection périodique de la zone par un organisme de détection technique de surveillance (TSCM — Technical Surveillance Counter-Measures) pour détecter les dispositifs d'écoute ou de captation.	SR1 — HUMINT physique	Doctrine défense	P3	RSSI	Inspection ≥ 1/an

5.5 Plan d'action — Mesures organisationnelles et humaines

Réf.	Mesure de sécurité	Risque(s) traité(s)	Référentiel ANSSI / ISO	Priorité	Responsable	Indicateur de suivi
MO-01	Mise en œuvre d'un programme « Insider Threat » : vetting périodique des cinq habilités (12 mois), entretien sécurité bi-annuel avec un psychologue assermenté, lignes d'alerte interne (whistleblowing) confidentielles, anonymes et auditées.	SO2 — V2.7	CERT Carnegie Mellon Insider Guide v6 ; ISO 27002 § 6.1	P1	Direction Générale + RSSI	Taux de couverture vetting ≥ 100 %
MO-02	Séparation des rôles entre administration système et gestion des sauvegardes : nomination d'un	SO2 — V2.6	ISO 27002:2022	P1	Direction Générale	Nombre de rôles

Réf.	Mesure de sécurité	Risque(s) traité(s)	Référentiel ANSSI / ISO	Priorité	Responsable	Indicateur de suivi
	administrateur des sauvegardes distinct, ne disposant pas du Tier 0 AD ; rotation trimestrielle entre les deux rôles.		§ 5.3 ; ANSSI SoD-NT			cumulés = 0
MO-03	Renforcement de la procédure de gestion des supports amovibles : registre nominatif des clés USB enrôlées, durée de vie maximale 12 mois, destruction physique en présence d'un second témoin, suivi des hash d'empreinte par UUID.	SO1 — V1.8	ANSSI USB-NT 2024 § 4	P1	Administrateur + RSSI	100 % clés enrôlées ; 0 clé manquante
MO-04	Mise en place d'une simulation d'attaque insider semestrielle (« red team interne ») : tentative de substitution de bande LTO, tentative de coercition fictive de l'administrateur, tentative d'extraction USB. Restitution en COSEC.	SO2 — V2.7, V2.1	ANSSI Red Team-NT	P2	RSSI + Direction Générale	≥ 2 simulations/an documentées
MO-05	Mise à jour de la PSSI § 4.1.2 pour inclure la procédure « quatre yeux » sur tout accès au coffre LTO, tout export de bande, toute lecture LTO, toute manipulation des clés de chiffrement. Sanction disciplinaire et pénale en cas de manquement.	SO2 — V2.1, V2.6	ANSSI PSSI 2024	P1	RSSI	Date publication PSSI v1.1 ≤ T+3 mois
MO-06	Programme de sensibilisation OSINT pour les cinq habilités : sensibilisation aux risques de profilage LinkedIn, suppression des mentions explicites du projet SpainTurbine sur les profils publics, formation phishing ciblé bimensuelle.	SO1, SO2 — recon humain	ANSSI Sensibilisation 2023	P2	RSSI	Score test phishing ≥ 90 % de bonnes réponses
MO-07	Audit annuel externe SecNumCloud ou équivalent espagnol (ENS) du périmètre cloisonné, incluant un test d'intrusion physique et logique sous mandat de la Direction Générale.	Tous scénarios	ANSSI Référentiel d'audit	P2	RSSI	1 audit / an avec rapport scellé
MO-08	Souscription d'une police d'assurance cyber spécifique défense, couvrant exfiltration de données classifiées, pertes d'exploitation, frais de remédiation et obligations notificatives (ANSSI / CNIL / SpainTurbine).	Tous scénarios — transfert	Recommandations FFA cyber 2024	P2	Direction Financière + RSSI	Police active ; plafond ≥ 5 M€

Réf.	Mesure de sécurité	Risque(s) traité(s)	Référentiel ANSSI / ISO	Priorité	Responsable	Indicateur de suivi
MO-09	Procédure de mobilité interne renforcée : tout changement de poste ou de périmètre du personnel habilité déclenche une revue à 48 h des droits AD, badge, YubiKey, accès coffres. Notification à l'autorité espagnole.	SO2 — V2.7 ; ER6	ANSSI Cycle de vie identités	P3	RH + RSSI	% mobilités revues sous 48 h = 100 %
MO-10	Exercice de crise « tabletop » spécifique au scénario « exfiltration LTO » à fréquence semestrielle avec mobilisation du COSEC, simulation de notification à SpainTurbine et à l'autorité espagnole.	SO2 — gestion de crise	ANSSI Exercices de crise	P3	RSSI + Direction Générale	≥ 2 exercices/an avec RETEX

5.6 Synthèse des mesures par scénario stratégique

Le tableau ci-dessous récapitule, pour chacun des quatre scénarios stratégiques retenus à l'atelier 3, les mesures du plan d'action qui en assurent le traitement, la stratégie retenue et l'évaluation du risque résiduel.

Scénario	Stratégie	Mesures clés	Risque avant traitement	Risque résiduel attendu
SS1 — APT étatique via flux MAJ	Réduire	MT-01, MT-02, MT-03, MT-04, MT-05, MT-06, MT-07, MT-10, MT-12, MT-13, MT-14, MT-15, MO-03, MO-06, MO-07	**12 — Très élevé**	6 — Modéré
SS2 — Initié coercitif / vol LTO	Réduire + Évitement partiel	MT-06, MT-08, MT-09, MP-01, MP-02, MP-03, MP-04, MP-05, MP-06, MO-01, MO-02, MO-04, MO-05, MO-09	**12 — Très élevé**	4 — Faible à modéré
SS3 — Ransomware via supply chain station blanche	Réduire + Transférer	MT-03, MT-05, MT-08, MT-09, MT-13, MO-07, MO-08	8 — Élevé	3 — Faible
SS4 — Espionnage économique soft	Réduire + Accepter résiduel	MO-06, MO-07, MO-09, MO-10	6 — Modéré	3 — Faible

5.7 Suivi opérationnel — KPI et KRI

Le RSSI tient un tableau de bord sécurité dont la fréquence de restitution est mensuelle pour la Direction Générale et trimestrielle pour le COSEC. Les indicateurs prioritaires associés au traitement des risques EBIOS RM sont les suivants :

Catégorie	Indicateur	Cible	Fréquence	Source de mesure
KPI — Détection	Délai moyen de détection des alertes EDR critiques (MTTD)	≤ 15 min	Mensuelle	ELK / EDR
KPI — Réaction	Délai moyen de réponse aux alertes critiques (MTTR)	≤ 2 h ouvrées	Mensuelle	ELK / Ticketing
KPI — Patch	% correctifs ANSSI critiques appliqués sous 72 h	≥ 95 %	Mensuelle	WSUS hors ligne
KPI — IAM	% comptes inactifs > 60 jours désactivés automatiquement	= 100 %	Mensuelle	AD / ELK
KRI — Insider	Nombre d'alertes Kibana corrélées à un comportement insider atypique	≤ 1 / trimestre	Trimestrielle	ELK UEBA
KRI — Supply chain	Nombre de fichiers Microsoft Update détectés en sandbox dynamique comme suspects	0 / mois	Mensuelle	S3Box Hogo + Sandbox
KRI — Coffre	Nombre d'ouvertures du coffre Fichet-Bauche en mode mono-opérateur	= 0	Hebdomadaire	Registre + Vidéo
KRI — LTO	Nombre de scellés brisés ou anomalies relevées sur cartouches LTO	= 0	Hebdomadaire	Registre LTO
KRI — Phishing	Taux de clic sur exercice phishing trimestriel des 5 habilités	≤ 5 %	Trimestrielle	Sensibilisation
KRI — Audit	Nombre d'écarts ouverts > 90 jours par l'audit annuel	≤ 0	Annuelle	Rapport d'audit

5.8 Risques résiduels et conditions d'acceptation

Après mise en œuvre du plan d'action, des risques résiduels demeurent. Ils sont nominativement listés ci-dessous, datés, et acceptés par décision formelle du Directeur Général après visa du RSSI. La revue est annuelle dans le cadre du cycle EBIOS RM continu.

Réf.	Risque résiduel	Justification de l'acceptation	Conditions de réévaluation
RR-01	Compromission du firmware d'un composant matériel (HP, Dell, Cisco,	Coût d'une politique « zero trust hardware » disproportionné pour une PME de 49 salariés ; veille CVE	Tout incident firmware notifié par un constructeur de la zone classifiée déclenche une réévaluation immédiate.

Réf.	Risque résiduel	Justification de l'acceptation	Conditions de réévaluation
	HPE, IBM) en amont de la livraison.	quotidienne et contrats de support actifs.	
RR-02	Compromission d'un sous-traitant maintenance (Hogo station blanche, ThermoVent, DataSys Rhône-Alpes) au-delà du cadre contractuel.	Mesures contractuelles, audit annuel, clauses miroir PSSI. Une supervision permanente nominative serait disproportionnée.	Réévaluation à chaque changement de sous-traitant ou à chaque incident notifié dans le secteur.
RR-03	Coercition simultanée de deux des cinq habilités (contournement du quatre yeux).	Probabilité considérée comme très faible compte tenu du vetting et du programme insider threat. Coût d'un triple contrôle systématique disproportionné.	Tout signal faible identifié dans le programme insider threat déclenche une revue dédiée.
RR-04	Sinistre majeur sur le site de Chambéry (incendie, accident industriel CHEMICALIA, attentat).	Couvert par PCA/PRA et assurance ; PSSI § 7.	Toute évolution du voisinage industriel ou tout signalement Préfecture déclenche une revue.
RR-05	Fuite OSINT d'informations non classifiées mais utiles à un attaquant (organigramme, ancienneté des collaborateurs).	Programme MO-06 ; sensibilisation continue.	Audit annuel OSINT externe ; revue trimestrielle des profils LinkedIn.

5.9 Plan de mise en œuvre et jalons

Le plan de mise en œuvre est jalonné en trois vagues, en cohérence avec les priorités P1 à P3. La gouvernance du plan d'action est confiée au RSSI, qui tient un tableau de bord d'avancement consolidé restitué mensuellement à la Direction Générale et trimestriellement au COSEC.

Vague	Échéance	Mesures incluses	Budget estimé	Validation
V1 — Quick wins critiques (P1)	T0 + 3 mois	MT-01, MT-02, MT-03, MT-05, MT-06, MT-08, MP-01, MP-02, MP-03, MO-01, MO-02, MO-03, MO-05	≈ 80 000 € HT (EDR + sandbox + scellés + caméras + vetting + ressources humaines projet)	DG + RSSI
V2 — Renforcement (P2)	T0 + 6 mois	MT-04, MT-07, MT-09, MT-10, MT-11, MT-12, MT-13, MT-14, MP-04, MP-06, MO-04, MO-06, MO-07, MO-08	≈ 60 000 € HT (WSUS, hardware Cisco, assurance, audit, équipements complémentaires)	DG + RSSI

Vague	Échéance	Mesures incluses	Budget estimé	Validation
V3 — Amélioration continue (P3)	T0 + 12 mois	MT-15, MP-05, MP-07, MP-08, MO-09, MO-10	≈ 40 000 € HT	RSSI

Le budget cumulé du plan d'action est estimé à environ 180 000 € HT sur douze mois, soit un effort complémentaire d'environ 15 % du chiffre d'affaires annuel du contrat SpainTurbine. Cet effort est porté à l'arbitrage de la Direction Générale conformément au § 8.3 de la PSSI, qui rappelle que la doctrine retenue consiste à concilier protection requise, continuité d'activité, performance opérationnelle et viabilité économique de la PME.

Conclusion

La présente analyse de risques, conduite selon la méthode EBIOS Risk Manager (ANSSI, v1.5) et adossée à la PSSI PSSI-BET-ST-2026-V1.0 et au DAT BET-ST-2026 de BIOÉNERGIE TECH, démontre que la zone classifiée « Confidencial » dédiée au projet SpainTurbine est confrontée à un niveau de menace très élevé, principalement porté par deux scénarios stratégiques convergents : la compromission du SI cloisonné par air-gap bypass via flux de mise à jour (SS1) et la coercition d'un personnel habilité conduisant au vol physique d'une cartouche LTO-8 et des clés de chiffrement associées (SS2). Ces deux scénarios sont cotés à 12/16, justifiant la priorité maximale accordée à leur traitement.

Le socle de sécurité existant — cloisonnement intégral, station blanche, MFA fort, PKI interne, SIEM ELK, sauvegardes hors ligne, sécurité physique multi-facteurs — constitue un point de départ solide pour une PME industrielle de cette taille. Toutefois, l'étude met en évidence plusieurs angles morts qu'il convient de traiter rapidement : l'absence de modèle de tiering Active Directory et de PAW, l'absence d'EDR comportemental, la station blanche limitée à des signatures statiques, la vidéosurveillance partielle de la zone coffre, l'absence de procédure « quatre yeux » sur les coffres et de scellés numérotés sur les cartouches LTO, et l'absence d'un programme insider threat structuré.

Le plan d'action proposé combine quinze mesures techniques, huit mesures physiques et dix mesures organisationnelles, alignées sur les guides de durcissement de l'ANSSI (Active Directory 2022, Stations blanches 2022, NT-022 Journalisation, EDR-NT 2023, USB-NT 2024, Cloisonnement-NT 2024) et sur l'ISO/IEC 27002:2022. Son déploiement, jalonné sur douze mois pour un budget estimé à 180 000 € HT, doit porter les risques résiduels SS1 et SS2 à un niveau « modéré » à « faible », conforme à l'exigence contractuelle SpainTurbine et au régime de protection « Confidencial ».

La revue annuelle de l'analyse de risques EBIOS RM, prévue par la PSSI § 6.3, permettra d'ajuster en continu les sources de risques, les scénarios stratégiques et opérationnels, et le plan de traitement. Toute évolution structurelle de l'architecture (par exemple l'ajout d'une seconde ligne de production, l'intégration d'un nouveau sous-traitant, ou la signature d'un contrat connexe avec un autre client défense) déclenchera une réévaluation anticipée du présent rapport.

Annexes

Annexe A — Acronymes et glossaire

Acronyme	Signification
ACL	Access Control List — liste de contrôle d'accès
AD	Active Directory
ANSSI	Agence nationale de la sécurité des systèmes d'information
APT	Advanced Persistent Threat — menace persistante avancée
CAO / CAM	Conception Assistée par Ordinateur / Computer-Aided Manufacturing
CIRT	Computer Incident Response Team
COSEC	Comité de Sécurité de l'Information BIOÉNERGIE TECH
D.I.C.	Disponibilité, Intégrité, Confidentialité
DG	Direction Générale
DLP	Data Loss Prevention
EBIOS RM	Expression des Besoins et Identification des Objectifs de Sécurité – Risk Manager
EDR	Endpoint Detection and Response
ELK	Elasticsearch, Logstash, Kibana — pile SIEM
ER	Événement Redouté
GPO	Group Policy Object — stratégie de groupe Windows
HSM	Hardware Security Module
IGI 1300	Instruction Générale Interministérielle n° 1300 sur la protection du secret défense
KPI / KRI	Key Performance / Risk Indicator
LTO	Linear Tape-Open — bandes magnétiques de sauvegarde
MFA	Multi-Factor Authentication
MTTD / MTTR	Mean Time To Detect / Respond
NIS 2	Directive (UE) 2022/2555 — Network and Information Security
OSINT	Open-Source Intelligence
OV	Objectif Visé (par une source de risque)
PAW	Privileged Access Workstation

Acronyme	Signification
PCA / PRA	Plan de Continuité / de Reprise d'Activité
PKI	Public Key Infrastructure
PSSI	Politique de Sécurité des Systèmes d'Information
RaaS	Ransomware-as-a-Service
RGPD	Règlement Général sur la Protection des Données (UE) 2016/679
RPO / RTO	Recovery Point / Time Objective
RSSI	Responsable de la Sécurité des Systèmes d'Information
SAS	Sas d'accès — chambre tampon entre deux zones de sécurité distinctes
SR	Source de Risque
SS / SO	Scénario Stratégique / Scénario Opérationnel
TSCM	Technical Surveillance Counter-Measures
UEBA	User and Entity Behavior Analytics
VE	Valeur Essentielle (bien essentiel)
WDAC	Windows Defender Application Control
WSUS	Windows Server Update Services
YARA	Moteur d'analyse de signatures par règles

Annexe B — Cartographie synthétique des couples SR/OV → SS → SO

Source de risque	Objectif visé	Scénario stratégique	Scénario opérationnel	Vraisemblance
SR1 — APT étatique	OV1 Exfiltration plans CAO	SS1	SO1 — Air-gap bypass via MAJ	V3 — Forte
SR1 — APT étatique	OV2 Implantation persistante	SS1	SO1 — Air-gap bypass via MAJ	V3 — Forte
SR2 — Initié sous coercition	OV1 Exfiltration directe (USB/photo)	SS2	SO2 — Vol LTO + clés	V3 — Forte
SR2 — Initié sous coercition	OV3 Vol cartouche LTO	SS2	SO2 — Vol LTO + clés	V3 — Forte
SR3 — Cybercriminel	OV1 Rançon	SS3	Variante SO1 (canal supply chain Hogo)	V2 — Significative

Source de risque	Objectif visé	Scénario stratégique	Scénario opérationnel	Vraisemblance
SR4 — Concurrent	OV1 / OV2 Espionnage soft	SS4	Cinématique OSINT/ingénierie sociale	V2 — Significative

Annexe C — Références et corpus normatif mobilisé

- ANSSI — La méthode EBIOS Risk Manager, version 1.5 (2018) et guide d'application 2024.
- ANSSI — Recommandations de sécurité Active Directory (PA-019, version 2022).
- ANSSI — Recommandations relatives à l'administration sécurisée des systèmes d'information (NT-014).
- ANSSI — Recommandations sur la journalisation (NT-022).
- ANSSI — Guide d'hygiène informatique, version 2022.
- ANSSI — Guide stations blanches et postes d'analyse de supports (2022).
- ANSSI — Recommandations de mise en œuvre d'une politique de cloisonnement (Cloisonnement-NT 2024).
- ANSSI — Recommandations pour la sécurisation des sauvegardes (Sauvegardes 2023).
- ANSSI — Guide d'application du chiffrement et de la gestion des clés cryptographiques (clés-NT).
- ANSSI — Recommandations EDR (EDR-NT 2023).
- ANSSI — Recommandations relatives à l'usage des supports amovibles (USB-NT 2024).
- ANSSI — Guide d'utilisation Cisco IOS-XE (2022) et bulletins CERT-FR associés.
- ISO/IEC 27001:2022 — Systèmes de management de la sécurité de l'information.
- ISO/IEC 27002:2022 — Code de bonnes pratiques pour la gestion de la sécurité de l'information.
- ISO/IEC 27005:2022 — Gestion des risques liés à la sécurité de l'information.
- ISO/IEC 27035 — Gestion des incidents de sécurité de l'information.
- MITRE ATT&CK Framework, Enterprise Matrix v15 (2025).
- MITRE D3FEND, version 0.14 (2024).
- CERT Carnegie Mellon, Common Sense Guide to Mitigating Insider Threats, 6th Edition (2022).
- CISA Alert AA21-008A — Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments.
- ENISA Threat Landscape 2024–2026 (sections « Supply chain » et « Defence sector »).
- Instruction Générale Interministérielle n° 1300 sur la protection du secret de la défense nationale.
- Référentiel équivalent espagnol de classification « Confidencial » (Centro Criptológico Nacional).
- Directive (UE) 2022/2555 dite « NIS 2 » et sa transposition française.
- Code pénal français — articles 413-9 et suivants (atteintes au secret de la défense nationale).

Annexe D — Cycle de revue de l'analyse

La présente analyse fait l'objet d'une revue annuelle conformément à l'article 6.3 de la PSSI BIOÉNERGIE TECH. Elle est par ailleurs revue de manière anticipée dans les cas suivants : signature d'un nouveau contrat défense, intégration d'un nouveau sous-traitant, modification structurelle de l'architecture (ajout de VM, changement de version Active Directory, modification du périmètre physique), incident

majeur sur le SI cloisonné ou chez un fournisseur de l'écosystème, ou évolution du cadre réglementaire (NIS 2, IGI 1300, équivalent espagnol).