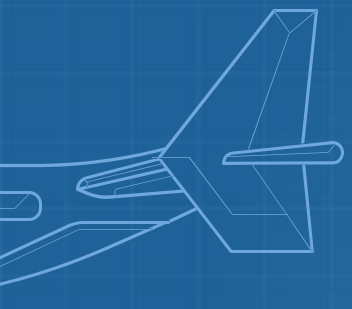
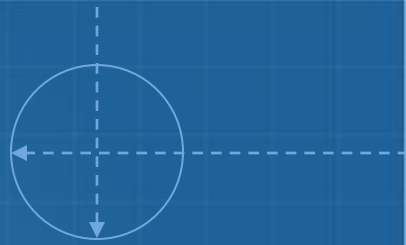
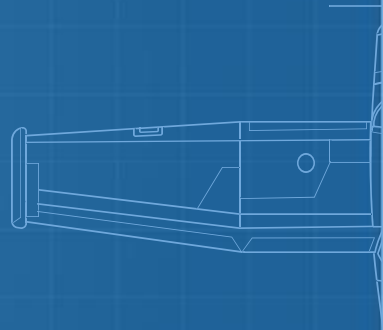
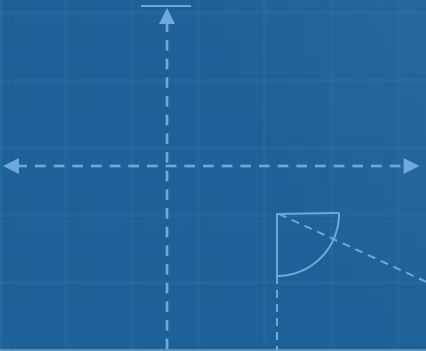


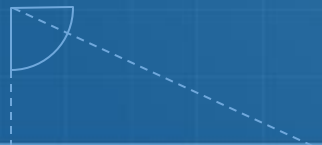


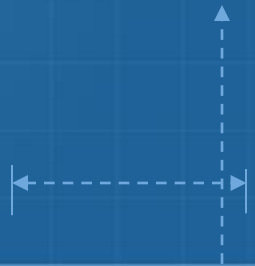
PSSI
BIOÉNERGIE
SPAINTURBINE



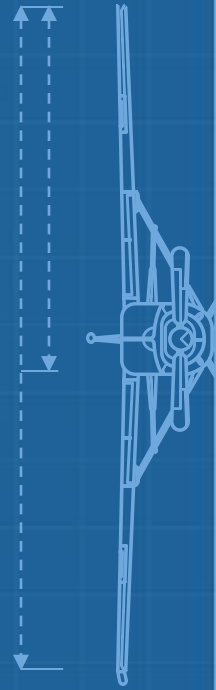
Politique de Sécurité des Systèmes d'Information
– Zone Confidencial



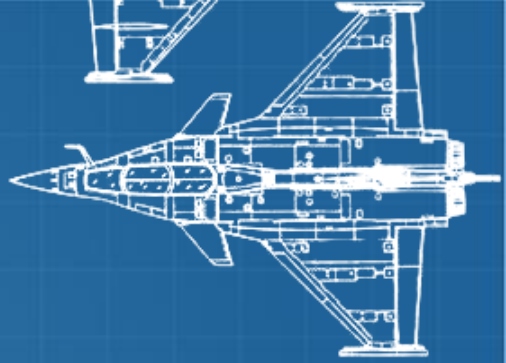




Sommaire



INTRODUCTION PSSI



OBJET DE LA PSSI

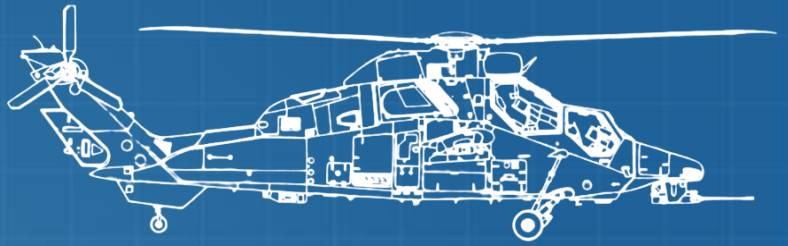
La PSSI fixe les règles assurant la Confidentialité, l'Intégrité, la Disponibilité et la Traçabilité (CID-T) des informations classifiées « Confidencial » du projet SpainTurbine — 120 micro-turbines drones/mois pour l'Armée espagnole, 1,2 M€/an.

PÉRIMÈTRE

Zone classifiée de Chambéry :

- ✓ 5 PC employés
- ✓ 1 PC mise à jour
- ✓ 1 PC chiffrement
- ✓ 2 PowerEdge R470
- ✓ Switch Cisco 9200
- ✓ Firewall Cisco 1120
- ✓ Station blanche
- ✓ Coffres fort
- ✓ Bandes LTO-8.
- ✓ 5 personnes habilitées
- ✓ RSSI
- ✓ DG.

CONTEXTE & ENJEUX



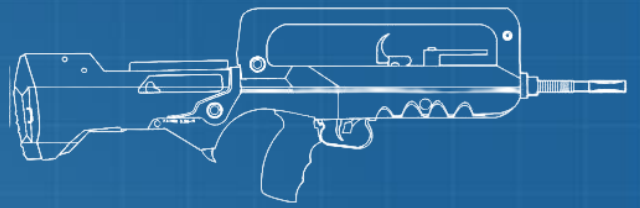
BIOÉNERGIE TECH

- PME industrielle de 49 collaborateurs à Chambéry
- Cellules/modules de batteries et turbines mini-hydrauliques
- Forte coactivité Seveso (CHEMICALIA à 40 m, métallurgistes à 80–100 m)
- Clientèle civile et défense (DGA, ANSC, AéroBat, AlpEnergy).

PROJET SPAINTURBINE

- 120 micro-turbines/mois pour drones militaires au profit de l'armée espagnole (1,2 M€/an)
- Classification « Confidencial »
- Doctrine : rien ne sort, rien n'entre sans validation
- SI dédié air-gap. Budget sécurité 114 400 € HT (~9 % du CA contrat).

ACTIFS PRIMORDIAUX



PLANS R&D

Plans, formulations et paramètres machines des micro-turbines drones (Confidencial — C/I/T).

PROCESSUS

Processus de fabrication, contrôle qualité et expédition des micro-turbines (Critique — D/I).

SAUVEGARDES

Sauvegardes LTO-8 chiffrées + coffre fort (Critique — C/I/D).

JOURNAUX

Journaux ELK + enregistrements vidéo Axis M4216-V (Sensible — I/D/T).

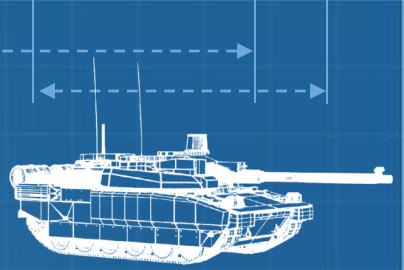
DONNÉES RH

Données personnelles des 5 salariés habilités et sous-traitants : habilitations, biométrie, vidéo (Sensible — C/I, RGPD).

RÉPUTATION

Réputation contractuelle vis-à-vis Armée espagnole, DGA, ANSC. Brevets et secrets de fabrication (Confidencial — C/I).

CADRE NORMATIF & GOUVERNANCE



RÉGLEMENTAIRE

- RGPD (UE 2016/679)
- Loi Informatique & Libertés
- Directive NIS 2 (UE 2022/2555) — entité essentielle défense
- IGI 1300 sur le secret défense
- Code pénal art. 413-9
- Clauses défense du contrat SpainTurbine.

NORMATIF

- ISO/IEC 27001:2022 (SMSI)
- ISO 27002:2022
- ISO/IEC 27035 (incidents)
- ISO 22301 (continuité)
- Référentiel ANSSI EBIOS Risk Manager v1.5 pour l'analyse de risques.

GOUVERNANCE

- Portage Direction Générale
- RSSI
- DPO
- Administrateur SI
- COSEC trimestriel
- Cellule de crise activée par le RSSI
- Cycle PDCA
- Revue annuelle de la PSSI
- Revue post-incident majeur.

SOURCES DE RISQUE – EBIOS RM

SR1 – ÉTATIQUE

Service de renseignement étatique étranger : exfiltration des plans via compromission supply chain Microsoft Update (capacité APT).

SR2 – INITIÉ

Salarié coercé (kompromat, finance) : vol/substitution de cartouche LTO + clés de chiffrement.

SR3 – ACTIVISTE

Activiste : sabotage symbolique, défacement (vraisemblance faible à moyenne).

SR4 – CYBER

Groupe cybercriminel : rançongiciel via chaîne d'approvisionnement station blanche (gain financier).

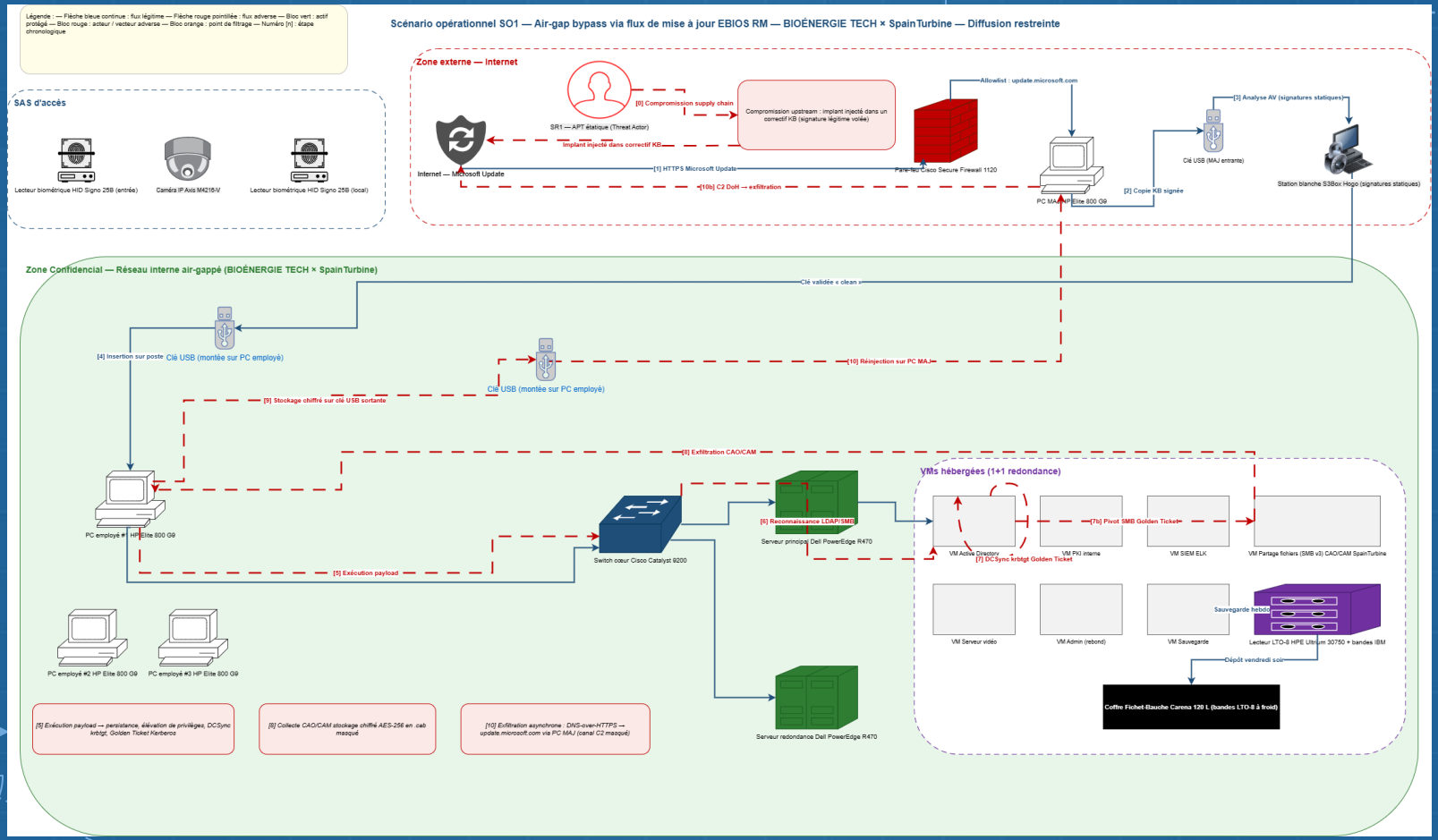
SR5 – CONCURRENT

Concurrent industriel : espionnage OSINT, captation des secrets de fabrication (avantage commercial).

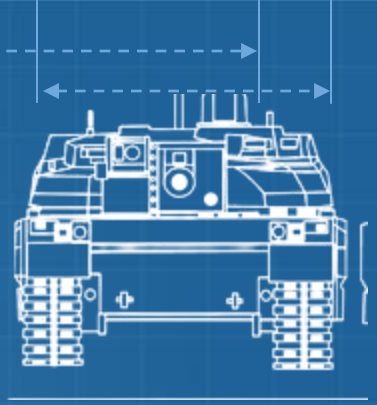
SR6 – ERREUR

Salarié négligent : divulgation accidentelle, perte de support amovible.

SCÉNARIO SO1 — AIR-GAP BYPASS VIA MAJ



GESTION DES ACCÈS - IAM



BESOIN D'EN CONNAÎTRE

Moindre privilège opposable.
4 niveaux :

- Confidencial
- Sensible
- Interne
- Public

Habilitation nominative validée par le DG (et autorité espagnole pour Confidencial).
Séparation des rôles exploitation / administration / audit.

MFA & CHIFFREMENT

MFA obligatoire : badge + YubiKey C NFC FIDO2 + biométrie HID Signo 25B pour SAS et local sécurité.

Kerberos AES-256 / LDAPS sur Active Directory.

PKI interne, SMB v3 chiffré, TLS partout.

CYCLE DE VIE

Arrivée : habilitation, charte, formation, badge + YubiKey.

Mobilité : revue des droits sous 48 h.

Départ : révocation immédiate, journaux conservés 36 mois.

Revue trimestrielle des comptes par admin + RSSI.

MATRICE D'ACCÈS – ZONE CONFIDENCIAL

PDG

- PDG : accès aux locaux uniquement
- Badge nominatif + biométrie
- Habilitation : Confidencial.

ADMIN SI

- Locaux + salle serveur + équipements réseau + ELK + PKI.
- Badge + YubiKey + biométrie + comptes à privilèges nominatifs.
- Habilitation : Confidencial.

AUDITEUR EXT.

- Accès locaux et/ou serveurs sur autorisation écrite
- Badge journalier + biométrie, supervision permanente.
- Habilitation : Confidencial.

5 SALARIÉS

- Locaux + PC employés + serveur de fichiers (besoin d'en connaître).
- Badge + YubiKey + biométrie SAS.
- Habilitation : Confidencial

MÉNAGE

- Aucun accès à la zone classifiée.
- Aucun moyen d'authentification provisionné.
- Habilitation : Public

SOUS-TRAITANT

- Accès locaux pour intervention planifiée.
- Badge journalier nominatif + biométrie, supervision par employé projet ou PDG.
- Habilitation : Sensible

SÉCURITÉ PHYSIQUE

SAS

SAS biométrique : 2 lecteurs HID Signo 25B + caméra Axis M4216-V.

Contrôle d'accès double facteur, traçabilité visuelle.

VERROUS

Verrous physiques : 30 verrous USB + 20 verrous RJ45.
Prévention de connexion non autorisée de supports ou câbles.

AIR-GAP

Air-gap total : aucune interconnexion réseau avec le SI corporate, aucun accès Internet direct sur les postes opérationnels.

COFFRES

Coffres : Fichet-Bauche Carena 120 L ignifuge pour bandes LTO.
Coffre 6 compartiments à serrures à code pour clés cryptographiques.

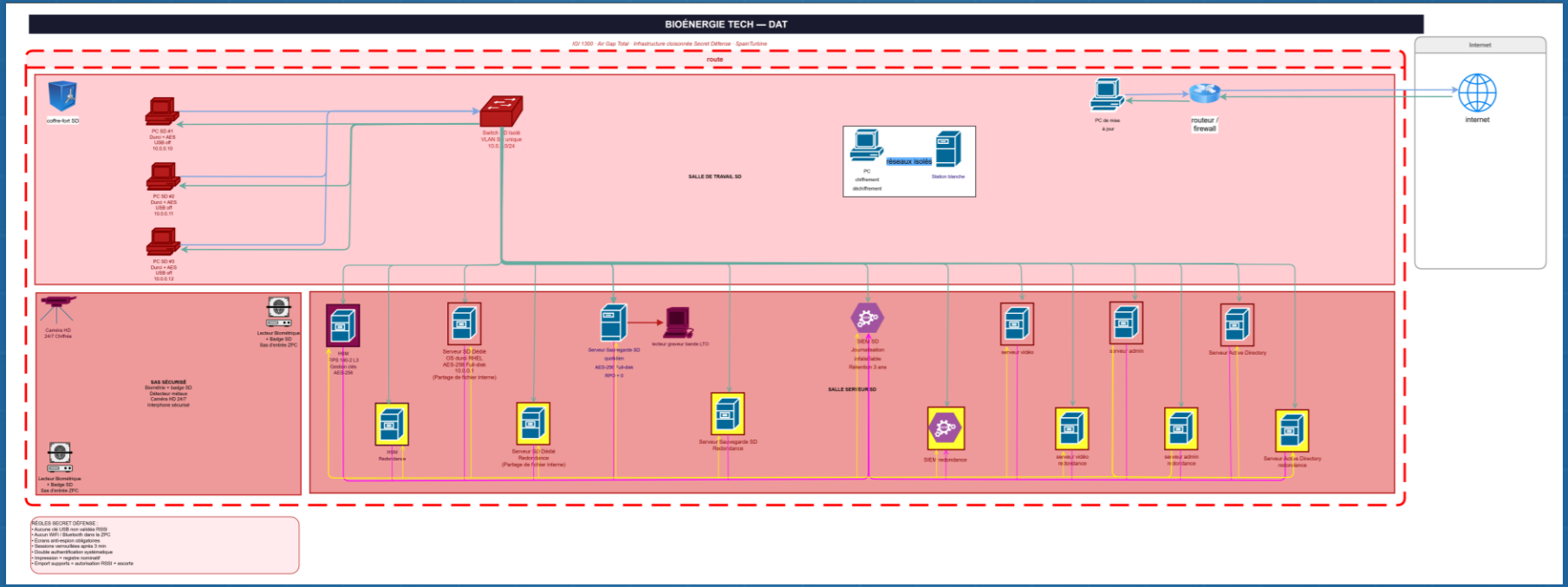
VIDÉO

Vidéosurveillance : caméra IP H.264 RTSP sur VLAN isolé, enregistrement 30 jours, accès restreint RSSI + DPO.

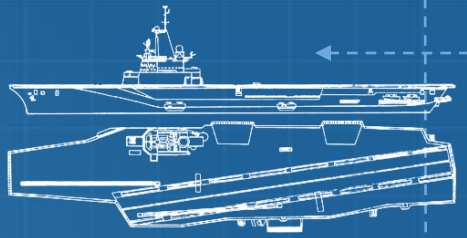
RÉSILIENCE

Résilience : onduleur 30 min + groupe électrogène mutualisé, détection incendie à gaz inerte en salle serveur.

SÉCURITÉ RÉSEAU / SYSTÈMES / APPLICATIONS



GESTION DES INCIDENTS



01 → 02 → 03 → 04

PRÉPARER

- ❑ Gouverner, identifier les actifs, protéger.
- ❑ Cartographie DAT
- ❑ Veille CVE
- ❑ Sensibilisation continue.

DÉTECTER

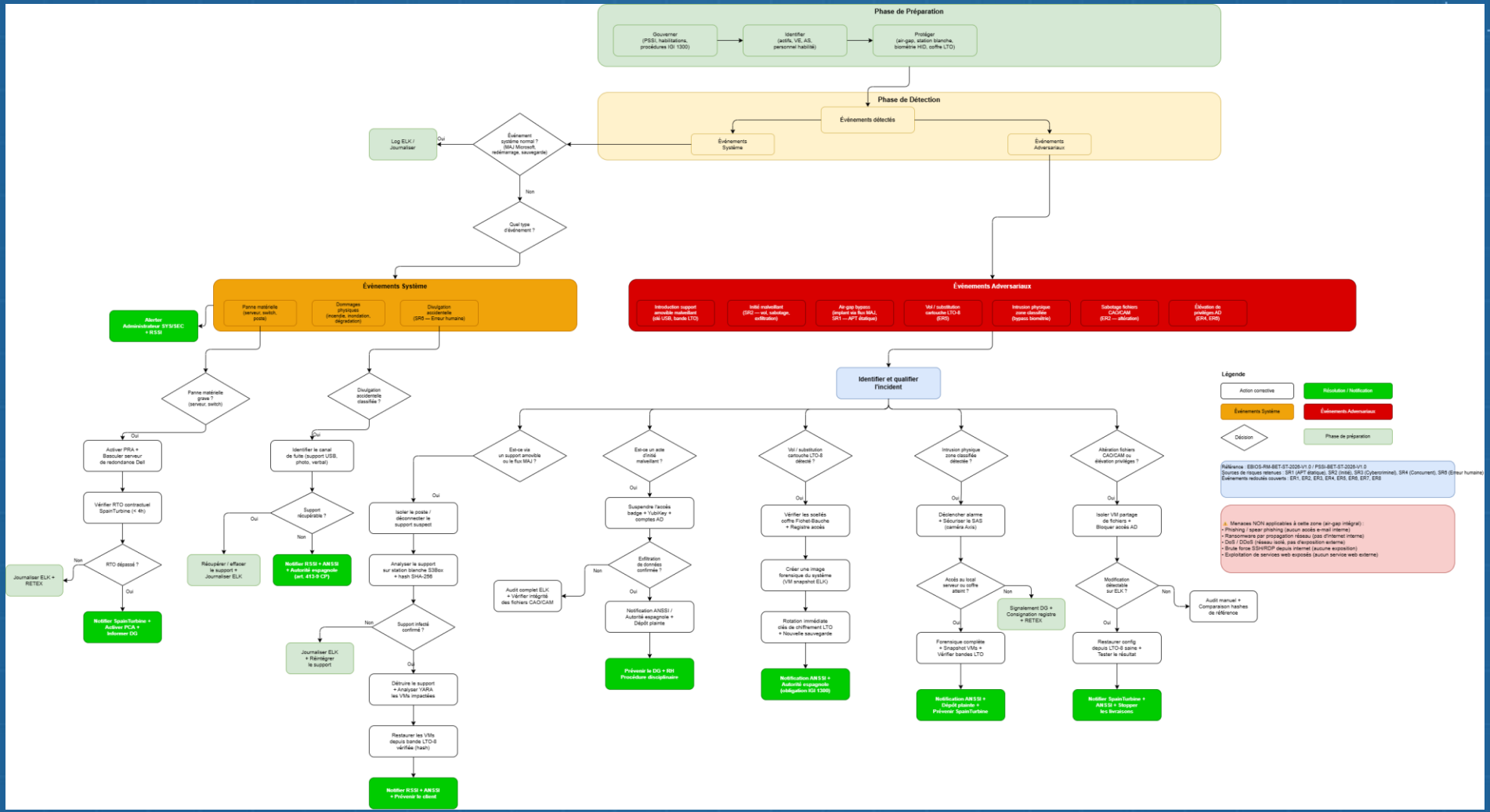
- ❑ Centralisation des journaux dans ELK
- ❑ Qualification immédiate par l'administrateur :
  - Evénement système normal (MAJ, stockage)
  - ou anormal ?

TRAITER

- ❑ Événements Système (défaillance, dommage, divulgation)
- ❑ Adversaires (vuln., brute force, malware, ...).
- ❑ Arbre de décision interne.

RETEX

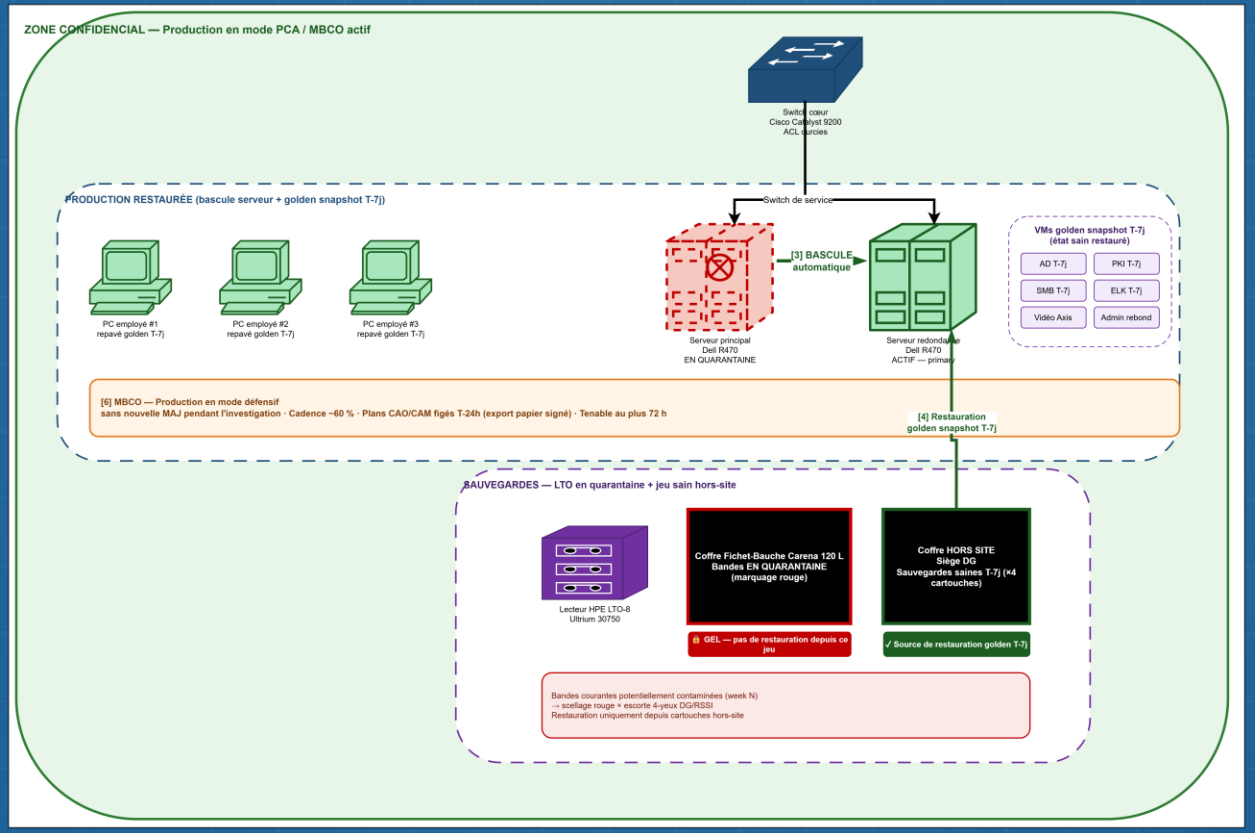
- ❑ Notification ANSSI < 24 h (NIS 2)
- ❑ Notification CNIL < 72h (RGPD)
- ❑ SpainTurbine + ANSC < 24 h
- ❑ RETEX écrit
- ❑ Revue COSEC trimestrielle
- ❑ MAJ des règles ELK.


Phase de Préparation
Gouverner (PSSI, habilitations, procédures IGI 1300)
Identifier (actifs, VE, AS, personnel habilité)
Protéger (air-gap, station blanche, biométrie HID, coffre LTO)
Phase de Détection
Événements détectés
Événements Système
Événements Adversariaux
Log ELK / Journaliser
Événement système normal ? (MAJ Microsoft, redémarrage, sauvegarde)
Oui
Non
Qual type d'événement ?
Événements Système
Panne matérielle (serveur, switch, poste)
Dommages physiques (incendie, inondation, dégradation)
Divulgation accidentelle (SR6 — Erreur humaine)
Alerter Administrateur SYS/SEC + RSSI
Panne matérielle grave ? (serveur, switch)
Activer PRA + Basculer serveur de redondance Dell
Vérifier RTO contractuel SpainTurbine (< 4h)
RTO dépassé ?
Non
Journaliser ELK + RETEX
Oui
Notifier SpainTurbine + Activer PCA + Informer DG
Divulgation accidentelle classifiée ?
Oui
Identifier le canal de fuite (support USB, photo, verbal)
Support récupérable ?
Oui
Récupérer / effacer le support + Journaliser ELK
Non
Notifier RSSI + ANSSI + Autorité espagnole (art. 4 f3 9 CP)
Événements Adversariaux
Introduction support amovible malveillant (clé USB, bande LTO)
Initié malveillant (SR2 — vol, sabotage, exfiltration)
Air-gap bypass (implant via flux MAJ, SR1 — APT étatique)
Vol / substitution cartouche LTO-8 (ER5)
Intrusion physique zone classifiée (bypass biométrie)
Sabotage fichiers CAO/CAM (ER2 — altération)
Élévation de privilèges AD (ER4, ER6)
Identifier et qualifier l'incident
Est-ce via un support amovible ou le flux MAJ ?
Oui
Isoler le poste / déconnecter le support suspect
Analyser le support sur station blanche S3Box + hash SHA-256
Support infecté confirmé ?
Non
Journaliser ELK + Réintégrer le support
Oui
Détruire le support + Analyser YARA les VMs impactées
Restaurer les VMs depuis bande LTO-8 vérifiée (hash)
Notifier RSSI + ANSSI + Prévenir le client
Est-ce un acte d'initié malveillant ?
Oui
Suspendre l'accès badge + YubiKey + comptes AD
Exfiltration de données confirmée ?
Non
Audit complet ELK + Vérifier intégrité des fichiers CAO/CAM
Oui
Notification ANSSI / Autorité espagnole + Dépôt plainte
Prévenir le DG + RH Procédure disciplinaire
Vol / substitution cartouche LTO-8 détecté ?
Oui
Vérifier les scellés coffre Fichet-Bauche + Registre accès
Créer une image forensique du système (VM snapshot ELK)
Rotation immédiate clés de chiffrement LTO + Nouvelle sauvegarde
Notification ANSSI + Autorité espagnole (obligation IGI 1300)
Intrusion physique zone classifiée détectée ?
Oui
Déclencher alarme + Sécuriser le SAS (caméra Axis)
Accès au local serveur ou coffre atteint ?
Non
Signalement DG + Consignation registre + RETEX
Oui
Forensique complète + Snapshot VMs + Vérifier bandes LTO
Notification ANSSI + Dépôt plainte + Prévenir SpainTurbine
Altération fichiers CAO/CAM ou élévation privilèges ?
Oui
Isoler VM partage de fichiers + Bloquer accès AD
Modification détectable sur ELK ?
Non
Audit manuel + Comparaison hashes de référence
Oui
Restaurer config depuis LTO-8 saine + Tester le résultat
Notifier SpainTurbine + ANSSI + Stopper les livraisons
Légende
Action corrective
Résolution / Notification
Événements Système
Événements Adversariaux
Décision
Phase de préparation
Référence : EBIOS-RM-BET-ST-2026-V1 0 / PSSI-BET-ST-2026-V1 0
Sources de risques retenues : SR1 (APT étatique), SR2 (Initié), SR3 (Cybercriminel), SR4 (Concurrent), SR6 (Erreur humaine)
Événements redoutés couverts : ER1, ER2, ER3, ER4, ER5, ER6, ER7, ER8
Menaces NON applicables à cette zone (air-gap intégral) :
- Phishing / spear-phishing (aucun accès e-mail interne)
- Ransomware par propagation réseau (pas d'internet interne)
- DoS / DDoS (réseau isolé, pas d'exposition externe)
- Brute force SSH/RDP depuis internet (aucune exposition)
- Exploitation de services web exposés (aucun service web externe)

PCA — CONTINUITÉ D'ACTIVITÉ

Scénario SS1 – APT étatique via flux de mise à jour (SO1)
Gravité : G4 ; Pertinence : P3 ; Niveau : 12 (Très élevé).

Stratégie : isolement immédiat, basculement vers une chaîne de mise à jour de secours, restauration sur image saine pré-incident.



PRA – plan de reprise d'activité

R-01 SERVEUR

Effondrement du bâtiment → Bande LTO sur nouveau serveur ;
RTO ≤ 48 heures ; RPO ≤ 24h (réplication cluster).

R-02 LTO LIGNE

Corruption logique → bande coffre Fichet-Bauche, vérif scellé + hash SHA-256, restauration ciblée ;
RTO ≤ 4 h ; RPO ≤ 24 h.

R-05 APT SO1

APT post-MAJ : isoler PC MAJ + station blanche, imagerie forensique, chaîne MAJ secours, rotation krbtgt ×2, notif ANSSI < 24 h.

R-03 LTO HORS SITE

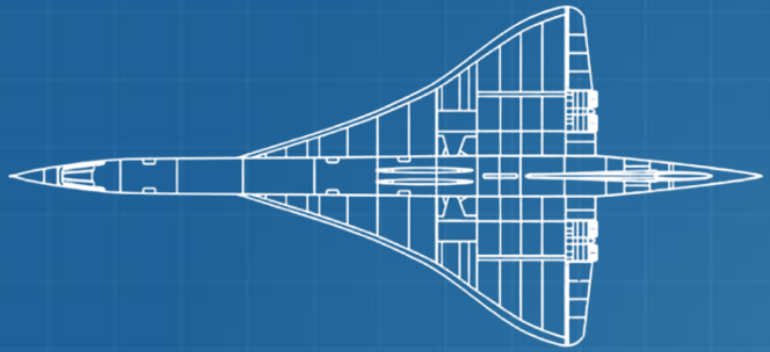
Compromission du jeu courant → 4 cartouches hors site (siège DG), quatre yeux DG+RSSI, repavage golden image ;
RTO ≤ 24 h.

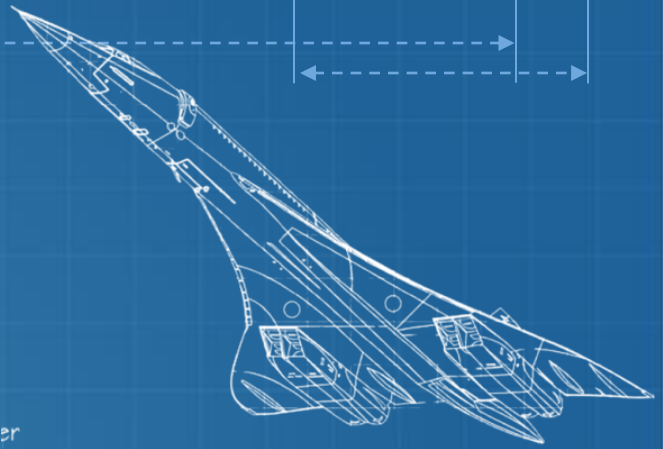
R-06 VOL SO2

Vol/substitution LTO : vérif intégrité + vidéo, restauration hors site, rotation PKI/krbtgt/YubiKey, saisine ANSSI/ANSC/DGA.

R-07 RANSOMWARE

Ransomware : isolement du switch < 30 min, preuves, repavage golden, restauration LTO immuable, refus du paiement de la rançon.





≤ 4 h

RTO — délai max d'interruption pour AD, fichiers, ELK

≤ 24 h

RPO — perte max de données (sauvegarde incrémentale LTO-8 quotidienne)

≤ 72 h

MTPD — seuil avant pénalités contractuelles SpainTurbine

KPI & TABLEAU DE BORD SÉCURITÉ

INDICATEUR	CIBLE	FRÉQUENCE	RESPONSABLE	STATUT
Patch CVE critiques < 72 h	≥ 95 %	Hebdomadaire	Admin SI	OK
Couverture EDR (5 PC + 2 serveurs)	100 %	Mensuelle	Admin SI	En cours
MTTD / MTTR incident majeur	24 h / 48 h	Trim.	RSSI	OK
Tests de restauration LTO	100 %	Mensuelle	Admin SI	OK
Comptes inactifs > 30 j	0 %	Mensuelle	Admin SI	OK
Nombre d'incidents détectés / qualifiés / clôturés	100%	Mensuelle	RSSI	OK
Taux de salariés sensibilisés dans l'année	100%	Annuelle	RSSI	OK
Nombre de RETEX clos	100% à 90j	Trimestrielle	RSSI	OK

MERCI

Questions du jury ?