DAT de BIOÉNERGIE TECH pour SpainTurbine

Introduction

Objet du document

Le présent document a pour objectif de décrire l’architecture technique du système d’information de la zone ZONE CLASSIFIÉE « Confidencial » de SpainTurbine (armée espagnole) pour son projet de défense en collaboration avec l'armée espagnole, afin de fournir une base solide pour l’analyse des risques et la mise en œuvre des mesures de sécurité. Il constitue un support pour les activités de gestion des risques conformément à la méthode EBIOS RM et aux recommandations de l’ANSSI, et permet d’identifier les composants, flux et points sensibles du système.

Périmètre

ZONE CLASSIFIÉE « Confidencial » de SpainTurbine (armée espagnole)

Cartographie des systèmes

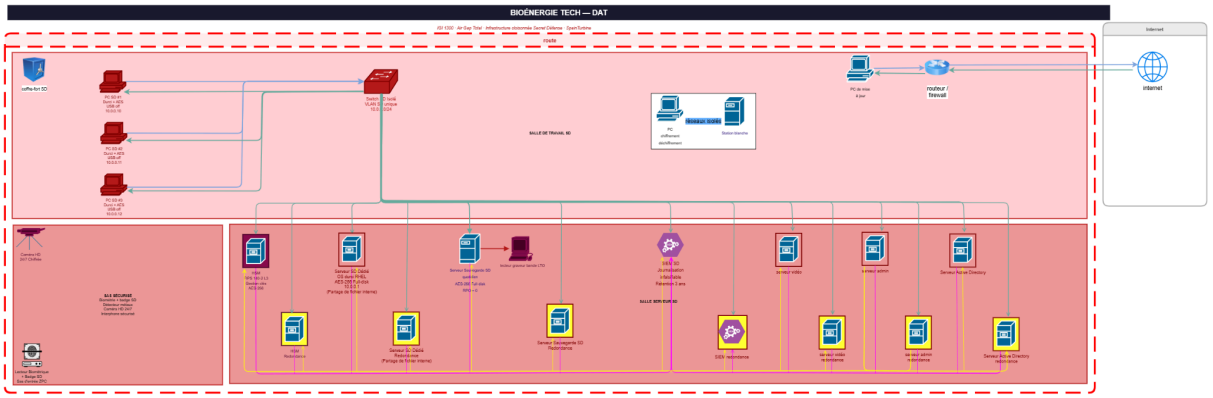
Inventaire des composants

nom	quantité	prix unitaire	total
Switch : Cisco Catalyst 9200	1	10000	10 000,00 €
Pare feu : Cisco Secure Firewall 1120	1	5000	5 000,00 €
PC employés : PC de Bureau HP Elite 800 G9 Tour	6	1 663,87	9 983,22 €
PC de mise à jour : PC de Bureau HP Elite 800 G9 Tour	1	1 663,87	1 663,87 €
PC de chiffrement / déchiffrement : PC de Bureau HP Elite 800 G9 Tour	1	1 663,87	1 663,87 €
souris filaire 1000	1	16	16,00 €
cable Cat6a 10m	10	30	300,00 €
Bobines Cat6a 300m	1	250	250,00 €
PowerEdge R470 Smart Selection Intel® Xeon® 6 Performance 6511P 2,3 GHz, 16C/32T, 72 Mo de cache, Turbo, (150 W), DDR5-6400 32 Go RDIMM, 6 400 MT/s x4 = 128go Disque SSD 3,84 To SATA lecture intensive 6 Gbit/s 512e 2,5" (1 serveur de redondance compris)	2	30000	60 000,00 €
station blanche S3Box Hogo	1	5000	5 000,00 €
coffre fort Fichet-Bauche Carena 120 litre	1	7500	7 500,00 €
lecteur de bande magnétique : HPE StoreEver LTO-8 Ultrium 30750 External Tape Drive	1	6000	6 000,00 €
Lecteur biométrique HID Signo 25B	2	1600	3 200,00 €
caméra Axis M4216-V	1	750	750,00 €
écran : Samsung S24D300GAU	7	100	700,00 €
cable UGREEN HDMI 2.0 1 m (blindage renforcé)	7	10	70,00 €
verrou RJ45 x10	2	30	60,00 €
IBM LTO Ultrium 8 Data Cartridge	15	100	1 500,00 €
verrou USB x10	3	20	60,00 €
Yubico - Security Key C NFC -Clé de sécurité 2FA, USB-C ou NFC, Certification FIDO U2F/FIDO2	5	35	175,00 €
Coffre fort muni de 6 compartiments indépendants avec serrures à code.	1	500	500 €

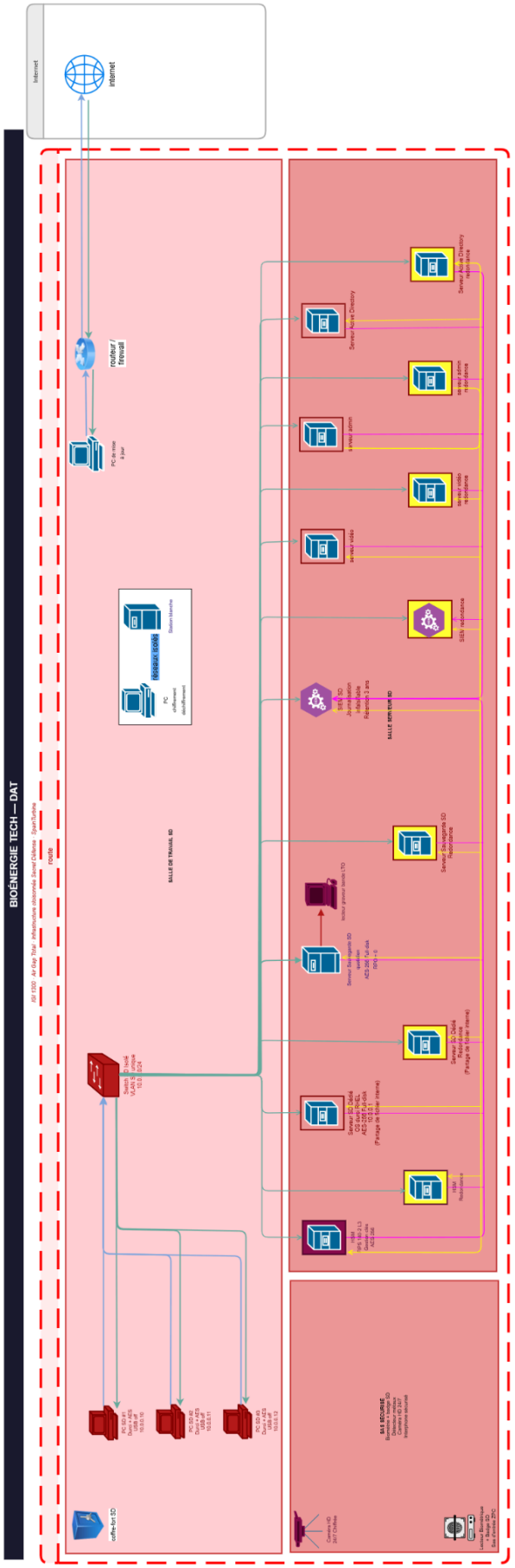
RSSI	1	100 000	100 000€
TOTAL			216 897,96 €

Schéma global

Version horizontal



Version de profil



Accès et administration

Accès internes

Entité concerné	Droit et privilèges	Méthodes d'authentification
PDG	Accès aux locaux	Accès par badge
Employé projet	Accès aux locaux et ordinateur	Accès par badge et yubikey pour les PCs
Administrateur	Accès aux locaux/salle des serveurs	Accès par badge et yubikey pour les serveurs
Employé hors projet	Aucun accès	

Accès externes

Entité concerné	Droit et privilèges	Méthodes d'authentification
Femme de ménage	Aucun accès	
Fournisseur télécom	Accès période de travaux, titre exceptionnel sous supervision de l'administrateur	
Organisme de certification/audit	Accès aux locaux sous supervision d'un employé projet ou du PDG. Accès sous supervision de l'administrateur pour la partie serveurs	
Sous-traitants matériels (Station Blanche)	Accès aux locaux sous supervisions d'un employé projet ou du PDG	Badge nominatif à la journée

Sauvegardes

Infrastructure concernée :

- 1 serveur principal + un serveur de redondance pour chaque serveur.

Média de sauvegarde :

- Bandes magnétiques LTO (Linear Tape-Open) pour les sauvegardes complètes et incrémentales.

Fréquence et politique :

- Sauvegarde complète hebdomadaire, sauvegardes incrémentales quotidiennes.
- Rotation des bandes selon un calendrier défini.

Stockage et sécurité :

- Les bandes sont déposées dans un coffre-fort sécurisé dans le site une fois par semaine.

Objectif :

- Garantir la disponibilité et l'intégrité des données en cas de sinistre, perte ou corruption des serveurs principaux.

Matrice de flux

Matrice de flux PC mise à jour								
N°	**source**	**destination**	**type de flux**	**description**	**Données échangées**	**Format / Protocole**	**Fréquence / Déclencheur**	**Sensibilité / Sécurité**
F01	Microsoft Update	PC de téléchargement	entrant	Téléchargement des mises à jour Windows	Paquets de mise à jour (KB, .msu/.cab)	HTTPS	Manuel	TLS, anti-malware sur PC
F02	PC de téléchargement	Clé USB	sortant	Copie des fichiers de mise à jour	Paquets de mise à jour téléchargés	Fichiers binaires (.msu/.cab)	Manuel, selon besoin	Vérification hash des fichiers

Station blanche								
N°	**source**	**destination**	**type de flux**	**description**	**Données échangées**	**Format / Protocole**	**Fréquence / Déclencheur**	**Sensibilité / Sécurité**
F01	Clé USB externe	Station blanche	entrant	tout type de fichier pour analyse	tout type de fichier pour analyse		Manuel	
F02	Station blanche	Clé USB externe	sortant	tout type de fichier pour analyse	tout type de fichier pour analyse		Manuel	

SpainTurbine								
N°	**source**	**destination**	**type de flux**	**description**	**Données échangées**	**Format / Protocole**	**Fréquence / Déclencheur**	**Sensibilité / Sécurité**
F01	Postes utilisateurs	Active Directory	Réseau interne	Authentification et gestion des comptes	Identifiants, tickets Kerberos	LDAP(S), Kerberos	À la connexion / renouvellement	TLS interne, comptes AD
F02	Postes utilisateurs	Serveur de logs	Réseau interne	Envoi de journaux système et applicatifs	Logs Windows, événements sécurité	Syslog / agent (ex: NXLog)	En continu	TLS interne, anonymisation possible
F03	Postes utilisateurs	PKI	Réseau interne	Obtention et vérification de certificats	Requêtes de certificats, CRL	HTTP(S), RPC	Selon besoin	Certificats signés, authentification
F04	Active Directory	PKI	Réseau interne	Synchronisation / validation des identités	Informations utilisateurs / groupes	LDAP(S)	Régulier	Authentification mutuelle
F05	PKI	Tous composants	Réseau interne	Diffusion de la liste de révocation (CRL)	Fichiers CRL	HTTP(S)	Périodique	Intégrité assurée par signature
F06	Tous composants	Serveur de logs	Réseau interne	Centralisation de logs sécurité / système	Événements, alertes, erreurs	Syslog / agent	Continu	Accès restreint au SIEM
F07	Tous équipements	Switch central	Réseau interne	Transmission des paquets / routage interne	Données diverses	Ethernet / TCP/IP	Continu	Contrôle des VLAN / ACL

F08	Administrateur	Tous serveurs	Interne (admin)	Supervision, maintenance, configuration	Commandes, scripts, logs	RDP / SSH / HTTPS	Selon besoin	Comptes à privilèges, MFA
F09	Postes utilisateurs	Serveur de fichiers	Réseau interne	Consultation, téléchargement et dépôt de documents confidentiels	Fichiers bureautiques (Word, Excel, PDF, etc.), métadonnées,	SMB v3 / CIFS	À la demande des utilisateurs (lecture/écriture)	Authentification Kerberos, chiffrement SMB, ACL par groupe AD
F10	Serveur de fichiers	Postes utilisateurs	Réseau interne	Transfert de fichiers depuis le serveur vers le poste (lecture)	Fichiers partagés, logs d'accès	SMB v3	À la demande	Chiffrement SMB, vérification des droits d'accès
F11	Caméra vidéo surveillance du SAS	serveur vidéo	Réseau interne	caméra vidéo surveillance du SAS	flux vidéo	RTSP; H264	continue	TLS, VLAN isolé
F12	lecteur biométrique + badge	Serveur Active Directory / IAM	Réseau interne	lecteur biométrique + badge qui permet d'accéder dans le SAS puis dans le local sécurité	données de validation d'accès dans le SAS	OSDP, HTTPS	À la demande	TLS

Stockage bande LTO								
N°	**source**	**destination**	**type de flux**	**description**	**Données échangées**	**Format / Protocole**	**Fréquence / Déclencheur**	**Sensibilité / Sécurité**
F01	Serveurs	coffre fort Fichet-Bauche Carena	entrant	sauvegarde hors ligne	Toutes données		1/semaine	critique

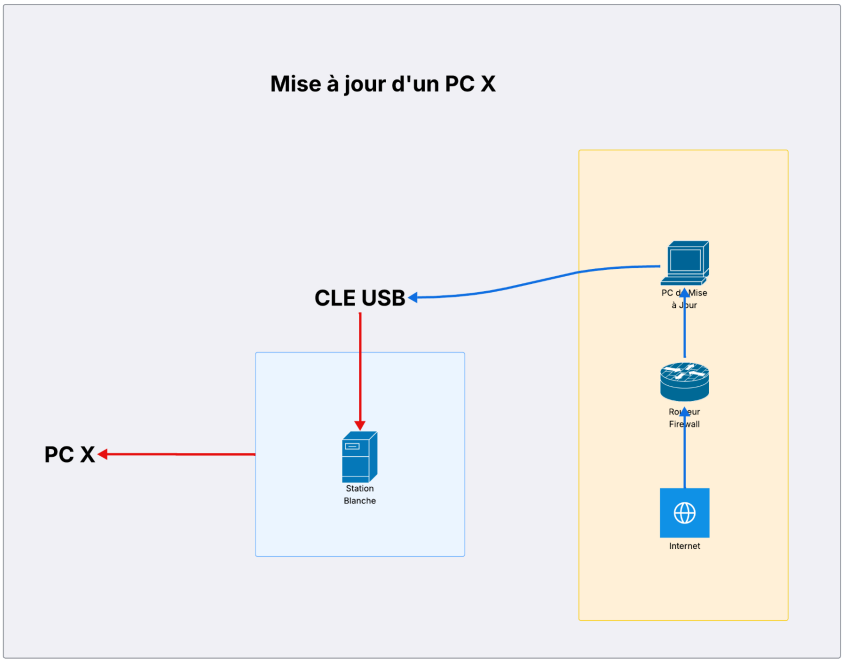
Gestion des journaux d’évènement

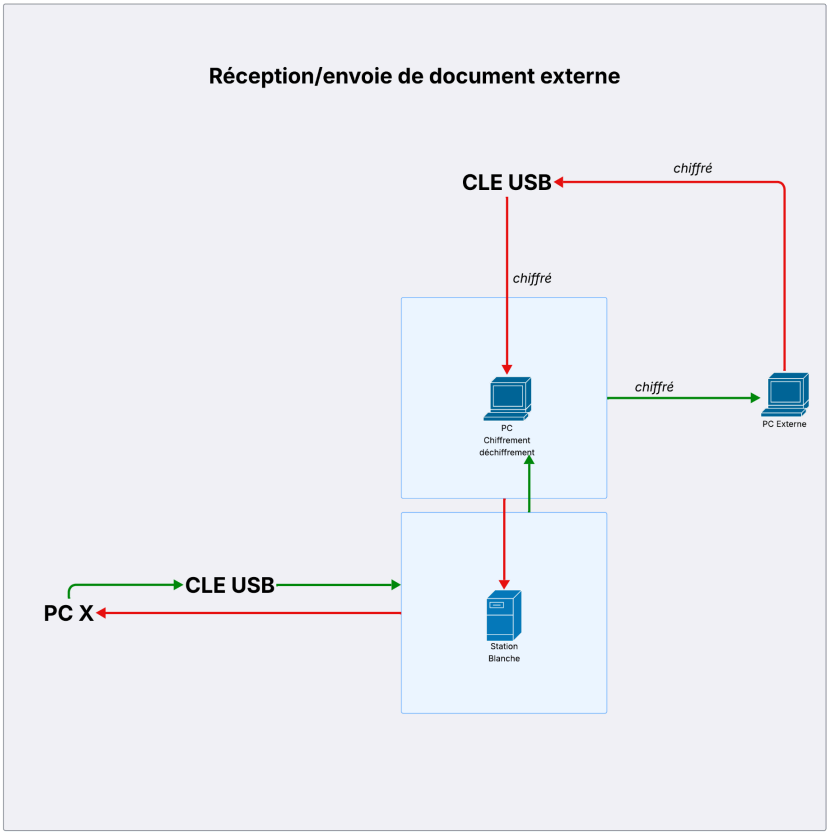
Pour la gestion des journaux d'événements, nous allons utiliser la pile ELK (Elasticsearch, Logstash et Kibana) pour le SI de la ZONE CLASSIFIÉE « Confidencial » de SpainTurbine (armée espagnole).

Supervision

Pas de supervision (genre Centreon) car ELK fait déjà très bien l’affaire.

ANNEXE 1 : Schémas des flux





Stockage des bandes LTO