Ci-dessous les exigences de la R31 et notre plan d'architecture informatique.
Attention cela ne concerne pas l'infrastructure de la DSI DERICHEBOURG mais uniquement celle de la Station centrale de télésurveillance.
Q1 : J'ai vu le profile du poste. Ça veut dire que je travaillerais dans la Station centrale de télésurveillance. Est-ce que cette station est comme SOC ou CERT?

2 phases :Conception / réalisation (Forfait une fois)
Travail de conception (1 à 2 semaines de travail)
Mise en application / suivi / audit (forfait de prestation assistance mensuelle)
Fréquence 1 fois par mois

Ce poste comporte 2 phases: la conception et la réalisation.
Dans la phase de conception, il faut fournir une charte informatique et un plan de sécurité PSSI selon le référentiel APSAD D32 N3.
Dans la phase de réalisation, comme PDIS/PRIS, il faut mettre en œuvre les mesures de cybersécurité, suivre les incidents/les alertes, veiller sur les vulnérabilités et les cybermenaces et réaliser des audits de sécurité périodiques.

Nous devons produire :
une charte informatique,
un plan de sécurité PSSI,
référent RSI
prise en compte du référentiel APSAD D32 niveau de sureté 3

Charte informatique:
Une charte informatique est un texte visant à faire respecter les obligations liées au RGPD. Elle fixe les droits et obligations en matière d'utilisation du système informatique au sein d'une entreprise, d'une administration. Par example, elle définit les conditions d'accès des salariés aux fichiers de l'entreprise (fichier de clients ou personnel).

Plan de sécurité PSSI:
Il est recommandé de satisfaire au niveau d'exigence correspondant au référentiel APSAD D32 Niveau de sureté 3.

Référentiel APSAD D32:
Ce référentiel a pour objectif d'accompagner les utilisateurs et installateurs dans la conduite d'un projet de conception et d'installation des systèmes de sécurité ou de sureté résistants aux cyberattaques sur un réseau informatique.
Il préconise une méthodologie en quatre étapes:

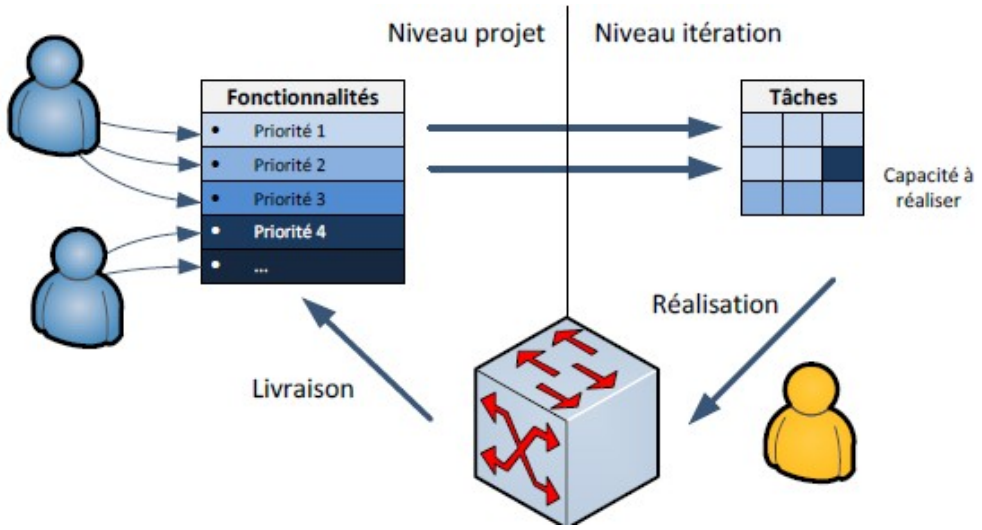
- **1ère phase <Analyse de besoins et de risques numériques> consiste à identifier les besoins à partir du contexte de l'installation**
- **2ème phase <conception> consiste à proposer les solutions techniques aptes à répondre aux besoins préalablement identifiés pour l'installation du système**
- **3ème phase <réalisation de l'installation> débute à la réception de la commande par l'installateur. Elle comporte la réalisation de l'installation, le contrôle et la mise en service, la formation, l'assistance des utilisateurs et de la réception de l'installation.**
- **4ème phase <maintenance> correspond à toute la période d'activité de l'installation. Elle pour objet de maintenir en bon état le système installé et de veiller à ce qu'elle reste adaptée aux besoins et des risques.**

Pourquoi mettre en place référentiel APSAD D32?
Pour la prévention et la protection de la cybermenace, il faut creuser les vulnérabilités du SI, telles que

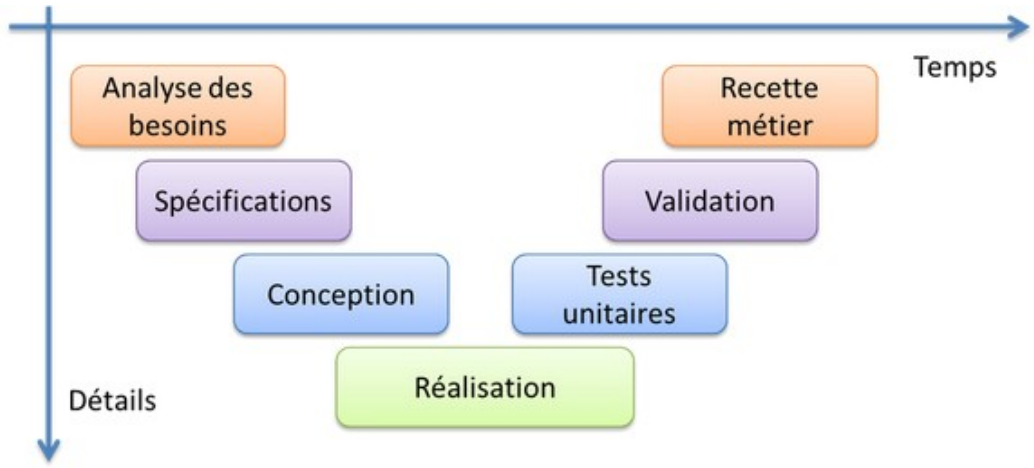
- **Mauvaise architecture et Cloisonnement**
- **Insuffisance voire absence de protection des données (chiffrement)**
- **Défaut de sensibilisation personnel + mauvaise hygiène SI**
- **Absence de mise à jour et suivi régulier**

PSSI: Politique de sécurité du système d'information.
RSI: Responsable du système d'information.
APSAD: Assemblée plénière de sociétés d'assurances dommages.
CNPP: Centre national de prévention et de protection

Mode Agile ou Mode V ? (Méthode Agile ou Cycle en V)
La différence entre les 2 sont:
Agile est itérative et participative. On developpe des petits morceaux d'application qu'on fait valider par l'utilisateur avant de passer aux suivants. C'est l'utilisateur qui pilote au fur et à mesure le développement. Un cycle de développement, une itération, prend 1 à 3 semaines.



V repose sur un développement de bout en bout, c'est-à-dire de la fabrication de l'application jusqu'à la livraison finale. Un cycle de développement prend plusieurs mois.



HORUS:
Horus est un produit de AzurSoft
Horus est un logiciel de supervision d'alarme permettant la réception, le décodage , le traitement , la présentation et l'archivage de toutes sortes d'évènements issus des centrales d'alarme.
Horus fonctionne sous windows
Horus gère plusieurs dizaines de milliers de transmetteurs.
Horus distribue les alarmes entre plusieurs opérateurs en utilisant des modes disponibles.

Quelles sont les taches ou missions?

Exemple de PSSI
--Oui, j'ai déjà réaliser PSSI en xx pour tracer les accès afin de pouvoir réagir en cas de violation de données.
Il faut satisfaire au niveau d'exigence national:

- **Mettre en place le système de journalisation. C'est-à-dire l'enregistrement dans des fichiers journaux ou logs des activités des utilisateurs, des anomalies et des évènements liés à la sécurité**
- **Protéger les équipements de journalisation et les informations journaliées contre les accès non-autorisés.**
- **Examiner périodiquement les journaux d'évènements pour y détecter d'éventuelles anomalies**
- **Assurer que les gestionnaires de ce système notifient, dans les plus brefs délais, toute anomalie ou tout incident de sécurité au responsable de traitement.**
- **Notifier toute violation de données aux personnes concernées pour qu'elles puissent en limiter les conséquences.**

Pour le 2ème exemple de PSSI chez yy pour protéger le réseau informatique interne:
Limiter les accès internet en bloquant les services non nécessaires (VoIP)

- **Gérer le réseau WIFI. C’est-à-dire ils doivent utiliser un chiffrement WPA2 (Non WEP) avec un mot de passe complexe et les réseaux ouverts aux invités doivent etre séparés du réseau interne.**
- **Imposser un VPN pour l’accès à distance**
- **Limiter les flux réseau au strict nécessaire en filtrant les flux entrants ou sortants sur les équipements(pare-feu, proxy). Par exemple, si un serveur web utilise obligatoirement HTTPS, il faut autoriser uniquement les flux entrants sur le port 443 et bloquer tous les autres ports.**
- **Cloisonner le réseau en réseau interne et réseau DMZ par des passerelles.**
- **Mette en œuvre des systèmes de détection d’intrusion qui peuvent analyser le trafic réseau pour détecter les attaques.**

Sécuriser les postes de travail: