Gabriel DELENNE BTSSIO1

Questionnaire gestion du patrimoine informatique - BTS SIO 2025
Lycée Bonaparte (Toulon)

1 – Respect des Normes et standards

Exploitation des référentiels, normes et standards adoptés par le prestataire informatique

- L'entreprise suit-elle des normes particulières ? (ITIL ou autres)

L'entreprise ne suit pas formellement l'ITIL, mais applique des principes similaires et associés : traçabilité des incidents, hiérarchisation des interventions, et journalisation. Elle s'inspire de bonnes pratiques en matière de cybersécurité (séparation des réseaux, mise à jour, suivi d'inventaire, etc.).

- Comment l'entreprise/l'organisation gère-t-elle les incidents ?

Un outil de ticketing (N-able) est utilisé. L'utilisateur signale un incident, un ticket est généré, et assigné à un technicien. Les incidents sont priorisés selon leur gravité

- Les intervenants sur les incidents ont-ils des attributions spécifiques ? La notion de « niveau » d'intervention est-elle présente ? Si oui, décrire cette organisation en niveaux.

  Oui :
  Niveau 1 : Prise en charge des demandes simples (mots de passe, redémarrage, petits problèmes réseau, mal utilisation). Problème non bloquant pour l'utilisateur
  (Tous capable de faire ces tickets donc répartition entre nous)

  Niveau 2 : Problème demandant à être prioriser par rapport au N1 car il s'agit de problèmes bloquants pour la personne (empêchant de travailler correctement)
  (Tous capable de faire ces tickets donc répartition entre nous)

  Niveau 3 : Interventions complexes ou escalade vers des experts externes (éditeur, fabricant).
  (Un peu plus complexe donc attribution aux personnes qualifiées)

- Y-a-t-il une procédure à suivre comme plus ou moins prévu dans ITIL ou autre procédure interne ? Si oui, décrivez là?

  Procédure interne inspirée d'ITIL : chaque ticket suit une ouverture, un diagnostic, une intervention, puis une clôture avec compte-rendu. Suivi des SLA informels.

- Décrivez le processus de gestion des incidents observé depuis la création du ticket jusqu'à la résolution de l'incident

  1) Signalement de l'utilisateur (via téléphone ou mail)

2) Création d'un ticket dans N-able

3) Affectation à un technicien selon le niveau et la disponibilité

4) Diagnostic, intervention

5) Clôture avec synthèse et éventuellement documentation

6) Archivage du ticket

- Le cas échéant, quel est le logiciel utilisé dans votre entreprise pour **gérer les incidents** (matériels ou logiciels …) ?
  N-able (gestion des tickets, supervision, suivi des incidents)
  En complément : messagerie Outlook, Teams pour la communication rapide.

  Avez-vous participé (ou même seulement observé) à une migration ? Quel était le besoin ? L'existant ? Qu'avez-vous mis en service ?

  Oui, une migration de notre service de téléphonie par IP vers "Wazo"
  Besoin : compatibilité,praticité, performances.
  Existant : Coms pro de chez Free
  Action mise en œuvre : aucune de ma part

- Comment l'entreprise prend-elle en compte la réglementation sur l'usage du numérique ? (CNIL, RGPD ou autres)

L'entreprise applique le RGPD :

Sauvegardes sécurisées
Accès restreint aux données
Désactivation des comptes utilisateurs inactifs
Signature de clauses de confidentialité

- Comment se fait le partage des informations et des connaissances au sein de l'équipe informatique, de l'entreprise et avec quels outils (messagerie électronique, plateforme de travail collaboratif, dossier partagé …) ?

Utilisation de :

Teams pour la communication quotidienne

Outlook pour les mails

Documentation dans des dossiers partagés ou wiki interne

- En matière de **développement de logiciels**, quelles sont les pratiques observées ?

Peu de développement observé, mais des scripts PowerShell et Bash pour automatiser certaines tâches (ex. : ajout utilisateur AD, sauvegardes, surveillance réseau).

- l'entreprise applique-t-elle les principes de méthodes de développement (RAD, Agile ou autres) ?

X

- Comment se fait le partage du code développé au sein de l'entreprise et avec quels outils (outils de gestion de version, serveur ftp…)

X

En matière de **cybersécurité**, quelles sont les pratiques observées?

Cloisonnement réseau chez leurs clients (VLAN)

Supervision active (N-able) RMM

Antivirus / EDR (Withsecure) déployé sur tous les postes de tous les clients

Connexions distantes sécurisées via VPN (Notamment pour le télétravail)

Sauvegardes régulières et hors-ligne

Comment les vulnérabilités connues sont-elles prises en compte ?

Mise à jour régulière (manuelle ou via scripts)

Veille sur CVE et correctifs via les bulletins Microsoft et articles

Quelle est la politique de mise à jour des postes clients Windows ? des serveurs ?

Automatique via WSUS ou paramétrée dans GPO

Serveurs mis à jour quand il y a besoin, prévention utilisateurs et maintenance annoncée

Y-a-t-il un RSSI ? Quelles sont ses attributions ?

En tant qu'infogérance, pas besoin de RSSI cependant mon tuteur est le RSSI de plusieurs de ses clients
Il supervise :

Les politiques de sécurité informatique

La gestion des accès et droits utilisateurs

La stratégie de sauvegarde et de restauration

La réaction en cas d’incident de sécurité

2 – GESTION DES CONFIGURATIONS

Mise en place d'une gestion de configuration et d'un suivi des incidents

(Par exemple, vous avez déjà vu en PPE l'outil : GLPI couplé avec OCS-Inventory)

Quel est l'outil (application/fichier) utilisé dans votre entreprise pour **répertorier, gérer etc … les matériels et les licences** (serveurs, postes, switch etc …) ?

Snipe-IT (inventaire dynamique)

Matériels, affectation des postes aux utilisateurs
Historique des interventions

- Avez-vous participé (ou même seulement observé) à une migration ? Quel était le besoin ? L'existant ? Qu'avez-vous mis en service ?

  Non, X

- Plus largement quels sont les outils mis en oeuvre pour déployer des nouveaux postes de travail, des nouvelles configurations (scripts, clonage de poste, …)

  Expérience personnalisé OOBE (out of the box), où l'utilisateur va se connecter avec son compte professionnel puis Intunes détecte la connexion et déploie automatiquement ce que l'utilisateur est autorisé et a besoin d'avoir.

Recueil d'informations sur une configuration et ses éléments

- Comment fait l'entreprise pour collecter ces informations ? Décrivez le processus de gestion des matériels/configurations observé depuis la création de la fiche jusqu'au déploiement de logiciels le cas échéant

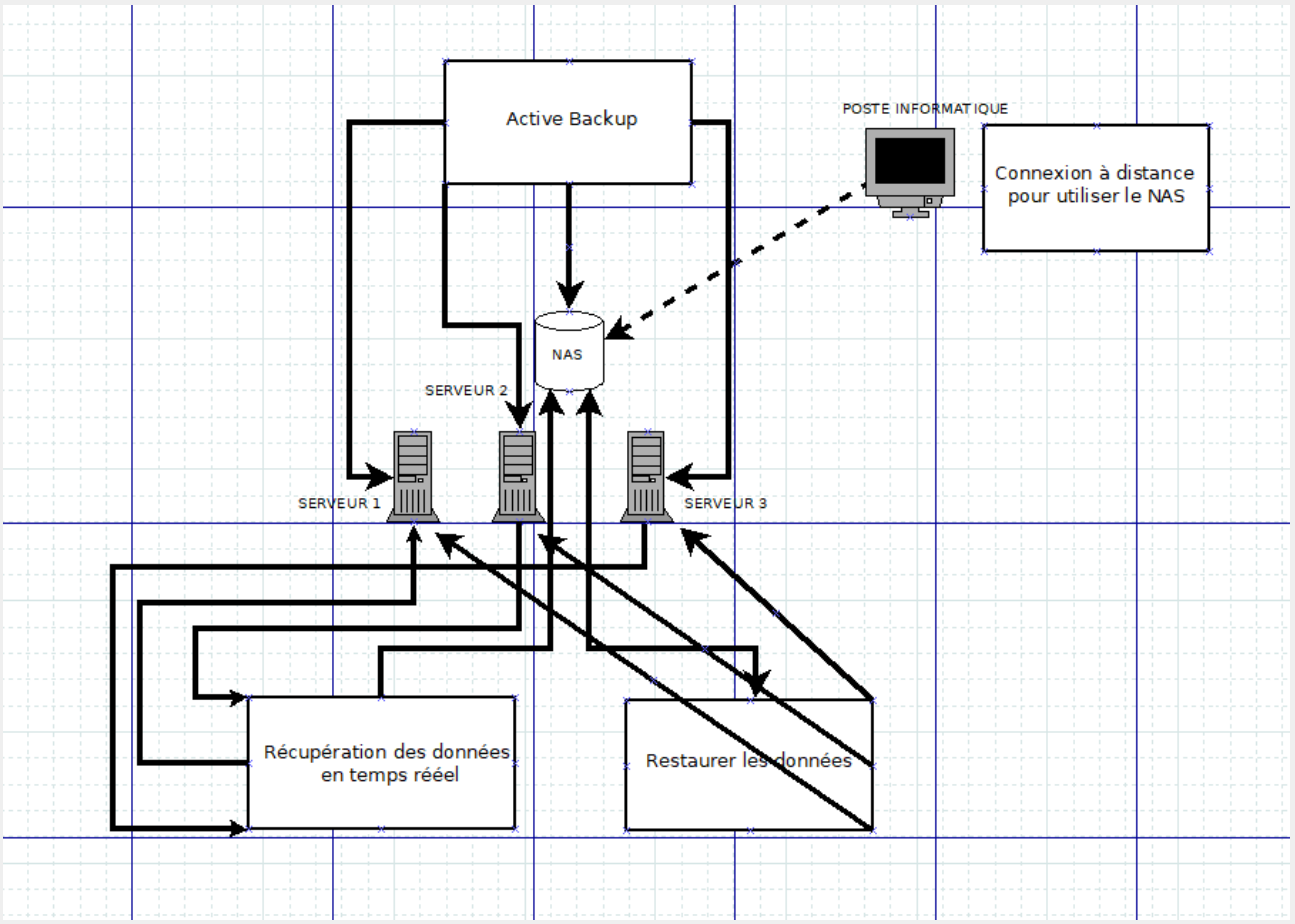
Référencement dans Snipe-IT lors de l'arrivée d'un poste

Attribution dans l'Active Directory ou l'azure AD suivant les clients

Installation des logiciels nécessaires(automatique ou non)

Sauvegarde via Active Backup for Business pour certains des serveurs

- Comment avez-vous fait pour réaliser un schéma réseau par exemple, pour décrire le contexte technique dans lequel vous êtes intervenu ?



Besoin d'une documentation pour un de leur NAS qui gère le backup et la restauration de certains des serveurs chez leurs clients.

- Comment fait votre entreprise pour tester / surveiller le bon fonctionnement des matériels, du réseau, des applications, etc … ?

Via **N-able** (alertes matérielles, disponibilité, usage disque/CPU)

Intunes et Exchange via la console Admin (Applications installés et suivi des connexions)

Supervision réseau (pings, ports ouverts, accès partagés)

- Des documentations techniques sont-elles rédigées et conservées ? Sous quelle(s) forme(s) ?

Documentation technique interne dans dossiers partagés

Formats : .docx, .pdf, fichiers Excel, captures d'écran

- Avez-vous, vous-même rédigé une doc sur une mise en place de configuration ?

Oui.

- Quelle est la "trace" de votre travail dans votre entreprise ?

Tickets fermés signés dans N-able

Documentation dans le dossier de l'équipe IT

2 – GESTION DES COMPÉTENCES

Repérage des compléments de formation ou d'auto-formation utiles à l'acquisition de nouvelles compétences

- L'entreprise vous a-t-elle proposé de suivre une formation particulière (Interne dans votre entreprise, ou dans un centre de formation, ou chez un fournisseur par exemple ?)

Oui, certification Veeam.

- Avez-vous eu à vous auto-former (c'est-à-dire tout seul) à l'aide de tutoriaux internet ou documentations spécifiques, pour pouvoir réaliser une mission durant votre stage ?

Certaines fois, la plus part du temps encadré en interne.

Étude d'une technologie, d'un composant, d'un outil ou d'une méthode

- Avez-vous étudié une nouvelle technologie durant votre stage ? Un nouvel outil ? Le(s)quel(s) ?

Active Backup for Business (sauvegardes centralisées)

Intunes

VPN

Entra ID

Azure AD et CLI pour tests d'authentification

N-able pour la gestion de parc et de tickets +++

Veille technologique

- L'entreprise a-t-elle mis en place des processus de veille technologique ?
(Pour elle-même et/ou pour être capable de répondre aux attentes ses clients)
- Si oui quels outils sont utilisés ? Comment s'organise cette veille dans votre entreprise.

Pas de veille organisée formellement, mais les techniciens échangent des nouveautés.

- Qu'avez-vous mis en œuvre pour votre propre veille technologique ?

Utilisation de **Feedly**, **YouTube**

Sites spécialisés : IT-Connect, Comment Ça Marche, Microsoft Learn

J’ai élargi ma veille sur les solutions de sauvegarde et de supervision, en lien avec les outils utilisés durant le stage (N-able, Active Backup).