Questionnaire gestion du patrimoine informatique - BTS SIO 2021
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)

La CNMSS suit dans les grandes lignes les préconisations ITIL mais ne s'appuie pas sur le référentiel complet

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

- 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.

L'entreprise gère les incidents par GLPI. Les utilisateurs créent un ticket. Les intervenants de niveau 1 ont pour travail de qualifier la panne et de la résoudre à partir de fiches réflexes. Si cela ne suffit pas, ils transmettent le ticket au niveau 2 (expert domaine)

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

Il existe une procédure interne qui se nomme DAUSIC (dispositif d'accueil aux utilisateurs des systèmes d'information et de communication) cette procédure décrit le cycle de vie d'un incident

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

Création du ticket lors de l'incident -> équipe niveau 1 -> réalisation de tests de niveau 1 à partir de fiches réflexes ; Si résolu -> clôture de l'incident
Sinon -> Envoi au niveau expert (Equipe Système, réseau, applicative)

- Le cas échéant, quel est le logiciel utilisé dans votre entreprise pour **gérer les incidents** (matériels ou logiciels …) ?
  X

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

J'ai réalisé la migration d'un serveur GLPI. Cette migration visait principalement à renforcer la sécurité des données de l'entreprise. J'ai planifié et exécuté la mise à jour vers une version plus récente de GLPI sur un nouveau serveur

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

La CNMSS dispose d'un DPO (délégué à la protection des données) qui fait appliquer la politique de la CNMSS. Il y a également un RSSI qui est le responsable de la sécurité des systèmes d'informations.

- 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 …) ?

Chaque bureau partage ses documents de manière non homogène. Certain utilisent « Sharepoint », d'autres utilisent les dossiers partagés sur un « NAS » .

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

Les pratiques observées incluent l'utilisation de Framework tels que Spring Boot et Symfony, ainsi que l'utilisation de Sonar pour surveiller la qualité et la sécurité du code.

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

Oui, l'entreprise applique les méthodes Agile

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

Le partage du code développé au sein de l'entreprise se fait principalement via GitLab, où le code source est hébergé et géré. La CNMSS utilise Git comme système de gestion de version pour suivre les modifications apportées au code et faciliter la collaboration entre les membres de l'équipe de développement

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

- Comment les vulnérabilités connues sont-elles prises en compte ?

Les vulnérabilités connues sont prises en compte par le biais de mises à jour régulières des logiciels et des systèmes. De plus, des mesures de sécurité telles que la présence d'antivirus sur les postes et les serveurs sont mises en place. Un système d'EDR (Endpoint Detection and Response) est également déployé.

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

La politique de mise à jour des postes clients Windows et des serveurs est rigoureusement suivie pour garantir la sécurité et la stabilité du système informatique de l'entreprise. Les mises à jour critiques et de sécurité sont généralement déployées dès leur disponibilité.

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

Oui, il y a un RSSI (Responsable de la Sécurité des Systèmes d'Information) au sein de l'entreprise. Ses attributions incluent la supervision et la gestion de la politique de sécurité informatique, la mise en œuvre de mesures de sécurité pour protéger les systèmes d'information contre les menaces, la sensibilisation des employés aux bonnes pratiques de sécurité, la gestion des incidents de sécurité, et la veille sur les nouvelles menaces et les réglementations en matière de sécurité informatique.

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 …) ?

L'outil utilisé pour répertorier, gérer et suivre les matériels et les licences, y compris les serveurs, les postes de travail, les commutateurs, etc., est iTop.

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

Comme expliqué précédemment, j'ai planifié, exécuté et mis en service la migration d'un serveur GLPI. Le besoin était de mettre à niveau vers une version plus récente pour renforcer la sécurité et améliorer les fonctionnalités de gestion des services informatiques de l'entreprise.

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

Pour déployer de nouveaux postes de travail ainsi que de nouvelles configurations, la CNMSS utilise principalement Microsoft Endpoint Configuration Manager (MECM). Cet outil nous permet de créer un master, c'est-à-dire une configuration de référence qui est ensuite déployée sur les nouveaux postes de travail.

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

X

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

X

Suivi d'une configuration et de ses éléments

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

L'entreprise utilise l'outil Centreon pour surveiller le bon fonctionnement des matériels, du réseau, des applications, etc. Centreon permet de tester et de surveiller en temps réel divers aspects de l'infrastructure informatique, tels que les performances des matériels, la disponibilité du réseau, ainsi que le bon fonctionnement des applications.

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

Oui, des documentations techniques sont rédigées et conservées dans l'entreprise. Elles sont disponibles sous forme de bases de connaissances partagées, accessibles à l'ensemble des membres de l'équipe. Ces documentations peuvent prendre différentes formes, telles que des fichiers texte, des documents PDF, des wikis internes, ou d'autres formats numériques.

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

Oui, j'ai rédigé une documentation axée sur mon projet de migration. Cette documentation détaillait les étapes de la migration.

- Quelle est la "trace" de votre travail dans votre entreprise ?
La trace de mon travail dans l'entreprise inclut une présentation détaillée devant la direction du service DSI et une vingtaine de personnes, ainsi que la création d'une documentation complète sur le projet de migration. Ces éléments servent de référence et de guide pour l'équipe, démontrant mon implication et la valeur ajoutée de mon travail.

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 ?)
L'entreprise m'a offert l'opportunité de suivre une formation dispensée par un expert technique sur les aspects de sécurité liés à mon projet de migration. Cette formation m'a permis d'approfondir mes connaissances et mes compétences dans en cybersécurité.

- 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 ?
Oui, pour mener à bien ma mission pendant mon stage, j'ai dû m'auto-former en utilisant des tutoriels sur internet ainsi que des documentations spécifiques. J'ai exploré différents forums et consulté la documentation officielle afin de trouver des solutions à divers problèmes techniques rencontrés.

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) ?

J'ai étudié de nouvelles technologies nécessaires pour réaliser mon projet. J'ai dû me familiariser avec le système d'exploitation Linux Red Hat, en particulier les aspects de sécurité comme SELinux. Pour la gestion des bases de données, j'ai approfondi mes connaissances sur MySQL et MariaDB. En ce qui concerne la partie Web, j'ai également étudié Apache, qui est un serveur HTTP largement utilisé, ainsi que FirewallD pour la gestion du pare-feu réseau. Ces compétences étaient essentielles pour assurer le bon fonctionnement et la sécurité des applications Web déployées dans l'entreprise.

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)
La CNMSS est informée des évolutions technologiques métier par la CNAM, et gestion de l'établissement par « Orange Cyber Défense »

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

Pour ma propre veille technologique, j'ai utilisé plusieurs outils tels que Inoreader, Google Alert et Feedly. Ces outils m'ont permis de suivre de près les dernières tendances, les actualités et les publications dans le domaine de la technologie. Inoreader m'a aidé à organiser et à suivre les flux RSS de différents sites web et blogs spécialisés. Google Alert m'a alerté dès qu'un sujet spécifique ou des mots-clés pertinents ont été mentionnés en ligne. Enfin, Feedly m'a permis de regrouper et de lire facilement les derniers articles et publications des sources que j'ai sélectionnées. Ces outils ont été précieux pour rester constamment informé des avancées technologiques pertinentes pour mon travail.