**TP1 BIS**Partie 1 :   
  
Définition :

La gestion des incidents est le processus permettant de détecter, enregistrer, diagnostiquer et résoudre les pannes informatiques. Un incident est un événement imprévu perturbant le fonctionnement normal d’un service informatique.

1/Quel incident peut concerner le serveur web de l’entreprise sur le diagramme Figma ?

Sur le Figma, le serveur web de l’entreprise Friendly Loans est hébergé sur une machine virtuelle Azure.

Un incident possible pourrait être une attaque de type clickjacking ou framejacking exploitée par le pirate Albert Gonzalez.

Cela signifie qu’un hacker insère le site Friendly Loans dans une iframe invisible sur un autre site pour tromper les utilisateurs et leur faire cliquer sur de faux boutons.

Ce type d’attaque peut provoquer le vol de données utilisateurs, une perte d’accès au serveur web ou encore une atteinte à la confidentialité des informations.

2/Donner la liste des logiciels critiques installés sur le disque ssd du serveur physique auquel avait trait la question précédente.

Les éléments visibles montrent que :

-Le serveur fonctionne sous Linux (série B)

-Il héberge une application web monolithique SPA

-Il utilise les services cloud Azure et Salesforce

Les logiciels critiques sont donc :

-Le système d’exploitation Linux

-Le serveur web (Apache ou Nginx)

-L’application Friendly Loans

-Les services Microsoft Azure

-Salesforce CRM

Ces logiciels sont critiques car une panne de l’un d’eux peut rendre le site totalement inutilisable.

3/Quelle est la relation entre GLPI et cet incident ?

GLPI est un logiciel de gestion de parc informatique et de tickets d’incidents.

Il sert à déclarer et suivre l’incident détecté sur le serveur web, par exemple une attaque de type clickjacking.

GLPI centralise les informations, permet d’assigner le ticket à un technicien et de suivre la résolution jusqu’à la clôture.

4/Quel logiciel peut jouer le rôle d’intermédiaire entre GLPI et l’incident ?

Le logiciel intermédiaire est un outil de surveillance qui détecte automatiquement les incidents et les envoie à GLPI.

Exemples :

-OCS Inventory

-FusionInventory (plugin GLPI)

-Nagios ou Zabbix pour la supervision réseau

Ces outils surveillent l’état du serveur et communiquent avec GLPI pour créer ou mettre à jour les tickets d’incidents.

5/Quelles seraient les bonnes pratiques ITIL par rapport à la gestion de cet incident ?

Le référentiel ITIL donne les bonnes pratiques suivantes :

-Détection et enregistrement : l’incident est signalé automatiquement par un système de supervision ou un utilisateur via GLPI.

-Classification : identifier le type d’incident, ici une faille de sécurité.

-Diagnostic initial : analyser les journaux du serveur Azure pour comprendre l’origine du problème.

-Escalade : transmettre l’incident à un administrateur système si nécessaire.

-Résolution et clôture : corriger la vulnérabilité et tester avant de clore le ticket.

-Retour d’expérience : documenter l’incident pour éviter qu’il ne se reproduise.  
  
Partie 2 :

Quels sont les outils que vous auriez pu combiner (voir le cours) pour faire une supervision réseau et avoir une visualisation des métriques de performance ?

Pour faire une supervision réseau et visualiser les métriques de performance, j’aurais combiné Zabbix (ou Nagios) pour la supervision du réseau et des serveurs, avec Grafana pour l’affichage graphique des données collectées.

Cette combinaison permet de suivre l’activité du parc en temps réel et de représenter les performances sous forme de tableaux de bord visuels.

Partie 3 :  
  
Quelles sont les mesures prises (dans le scénario du Figma) pour sécuriser le parc informatique ?

Dans le scénario Figma, la sécurité du parc est assurée grâce à l’hébergement sur le cloud Azure, au chiffrement des données (AES-256 et TLS), à la limitation des accès réseau, et à la mise en place de politiques RGPD (cookies, confidentialité, intégrité).

Des protections applicatives comme le Content Security Policy et le X-Frame-Options renforcent la défense contre les attaques web (XSS, clickjacking).

Partie 4 :  
  
Trouvez dans le scénario Figma la demande utilisateur ?  
  
Dans le scénario Figma, la demande utilisateur est la création d’un ticket dans GLPI par Francis pour signaler ou suivre une alerte de supervision envoyée par Zabbix.  
Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Quel est le cycle de vie d’une demande utilisateur (voir le cours) ?

Le cycle de vie d’une demande utilisateur comprend : la soumission, la validation, le traitement, la livraison et la clôture.