PROGRAMMATION PYTHON

Types de variables

```
a = “Bonjour“       # chaine de caractères : str
b = 5               # nombre entier  : int
c = 1.5             # nombre à virgules : float
d = True            # True ou False : bool
```

Print et Input

```
nom = input(“Quel est votre nom? “)
print(“Vous vous appelez “ + nom)                  # concaténation de chaine
print(f“Vous vous appelez {nom}“)                  # chaine formatée
print(“Vous vous appelez %s“ % nom)                # chaine formatée (ancien format)
```

Commentaires

```
# Commentaire sur une ligne
“““ Commentaire
            sur
                plusieurs lignes“““
```

Conversions

```
age = 30
print(“Votre age est: “ + str(age))        # conversion de int vers str, et concaténation

age_str = “30“
age_int = int(age_str)                     # conversion de str vers int.
                                           # Utiliser un bloc try/except en cas d’erreur
```

Boucle While

Boucle tant que la condition est vraie

```
nom = ““
while nom == ““:
        nom = input(“Quel est votre nom? “)
```

IUC-Prépa Exam

ETUDE DU CONTEXTE

1- Quels sont les critères traditionnels de la sécurité ? La DSI souhaite ajouter le critère de traçabilité dans le périmètre de son étude. Proposer une définition de ce critère
2- Définir les notions : Risque, Menace, Vulnérabilité. Donnez une équation du risque.
3- Dans notre contexte, à quoi sert la matrice des risques informatiques.
4- Quelles sont les bonnes pratiques pour réduire ces risques informatiques.
5- Vous avez croisé votre Directeur Général dans le couloir qui en substance disait au DSI« Il faut que l'on se fasse certifier 27001, c'est primordial ! Il faut gérer l'incertitude, maintenir une inquiétude raisonnée et entretenir une véritable vigilance en mettant en place une politique de défense en profondeur»
   a) Définir le concept de défense en profondeur.
   b) Qu'est-ce qu'un SMSI, donnez un exemple d'outil pouvant faire référence.
   c) Cette norme est fondée sur le PDCA. Donnez son principe et décrivez les différentes étapes.
   d) Pour une garantie majeure de sécuriser les infrastructures, l'entreprise mise sur les outils de type SIEM. De quoi s'agit-il et donnez deux exemples.

Exercice1.

Dans le cadre de sa mission de fournisseur d'énergie, SITRAELEC doit prendre en compte la sécurité de ses réseaux de distribution et de gestion. M. CHANGA, l'adjoint à la DSI, a la responsabilité de la sécurité des systèmes d'information (RSSI).

Abonné aux alertes du site du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR), l'avis du 14 mai 2019 concernant notamment trois vulnérabilités (exécuter des commandes système arbitraires avec les privilèges du serveur de base de données local : élévation de privilège) publiquement connues (CVE) a attiré son attention. Ces vulnérabilités décrivent plusieurs failles de sécurité découvertes dans le logiciel utilisé dans le réseau de distribution d'électricité (ICS) de SITRAELEC, à savoir le logiciel SIMATIC WinCC.

1. CVE, qu'est-ce que c'est?
2. En quoi va consister la vulnérabilité liée à « Une élévation de privilèges »

Pour mieux appréhender la situation, il organise un appel d'offre pour faire auditer la sécurité de son réseau. Deux offres sont proposées :

3. Un scan de vulnérabilités: à l'aide de sondes spécialisées placées à différents endroits du réseau, l'expert découvrira automatiquement les vulnérabilités des équipements ;
4. Un test d'intrusion: sans aucune information préalable, l'expert tentera de pénétrer le réseau de l'entreprise depuis Internet et de s'approprier des informations confidentielles.