CONSERVATOIRE NATIONAL DES ARTS ET METIERS

**Correction Examen SEC101 – FOAD IDF**

Session 2

Septembre 2022

Durée  3 heures

Document (s) autorisé(s) : tout document papier

Calculatrice : x

**Téléphone portable : Interdit**

Le sujet comporte 3 pages (dont celle-ci).

Barème d’évaluation : voir ci-dessous

**Les 8 questions à développement court représentent respectivement 2 pts chacune, sauf la dernière à 3 pts.**

**1pt pour la présentation et l’orthographe si et seulement si toutes les questions sont traitées**

**Votre note sur 20.**

**Courage, la première fois ne fut pas la bonne**

**« Qu’importe le flacon, tant qu’on a l’ivresse »**

**Proverbe de fin d’UV**

**NE SERONT NOTEES SEULEMENT CELLES DONT LES REPONSES SERONT ARGUMENTEES.**

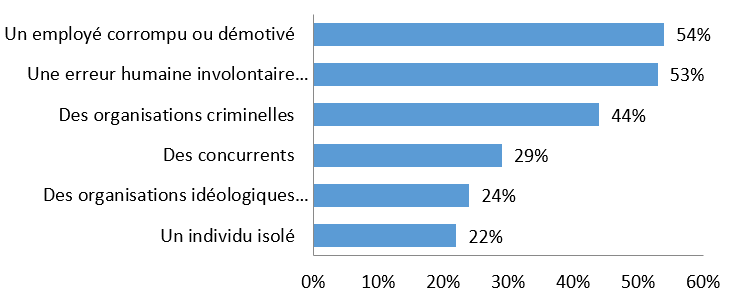
# Questions à développement court

**1/**

***Les cybermenaces profitent non pas tant des failles technologiques qu’humaines***

**La cybercriminalité́ ne s’appuie pas vraiment sur les failles de sécurité́ technologiques pour se développer. Elle prolifère surtout à partir des failles de sécurité́ humaines. C’est ainsi que 99 % des cyberattaques s’alimentent de failles résultant de l’action humaine. On peut voir dans la figure ci-dessous quelles sont les principales sources de failles humaines.**

**Répartition des principales sources de failles humaines**



***Source : Le baromètre cybersécurité 2019 par Sylob, L’Usine Nouvelle et Hub One*« *En 2019, 51 % des attaques ont eu recours à des techniques dépourvues de logiciels malveillants, contre 40 % en 2018, ce qui souligne la nécessité d’aller au-delà des solutions antivirus classiques* »10.**

**La fréquence des « arnaques au Président » (escroquerie aux faux ordres de virement - FOVI) qui n’est pas une cyberattaque à proprement parler - montre à quel point l’humain est au cœur des failles, même les plus évidentes. Ainsi, « *plus de 23 milliards d’euros ont été volés par des cybercriminels depuis 2016, suite à la compromission d’emails centrés sur les individus* »11, que ce soit via l’arnaque au Président, l’usurpation d’identité́ ou par rançonnage. C’est parce que les hackers en sont pleinement conscients que s’est développée l’ingénierie sociale, forme de cybercriminalité qui consiste à exploiter la nature humaine pour mieux la rançonner.**

**Parfois, ces failles sont occasionnées par des tiers appartenant au cercle intime des collaborateurs ou des dirigeants d’entreprise. Ainsi, des systèmes ont été pénétrés et ont perdu leur intégrité via les proches de dirigeants ou directeurs qui possédaient des droits étendus sur les systèmes d’information de l’entreprise. Un exemple connu est celui de la compromission d’un système par l’intégration d’un *malware* téléchargé par l’enfant d’un dirigeant : ce dernier cherchait à télécharger illégalement un film, via Bit Torrent, le logiciel légal de pair à pair *(peer-to-peer)12*.**

**A la lecture de cet extrait :**

**En tant que RSSI, quel serait vos propositions organisationnelles et techniques afin de se prémunir de ce risque ?**

**Correction 1 :**

**On peut noter dans l’extrait de l’article que la plupart des origines des sources humaines sont internes sans que des sources extérieures à l’organisation soit impliquées.**

**Afin de réaliser un ROSI important, des solutions de sécurisation et contrôle des actions des collaborateurs permettent de couvrir partir**

**Solutions organisationnelles :**

* **Assurer des droits au justes besoins suivant le profil des utilisateurs. On évitera que les dirigeants et responsables supérieurs aient des droits sur tout le SI.**
* **Sensibiliser aux risques**
* **Au recrutement, s’assurer de la probité des personnes**
* **Faire signer une charte d’utilisation des ressources informatiques**
* **Vérifier le niveau de satisfaction des collaborateurs sur la condition de carrière et permettre l’évolution ou le départ de façon saine.**

**Solutions techniques :**

* **Mettre en place une politique d’audit, de journalisation et d’alertique**
* **Mettre en place une solution de tracage des documents**
* **Mettre une sauvegarde régulière et la rester tout autent**
* **Mettre en place un FW nouvelle génération avec analyse de flux et interdire les flux exotique même initier depuis les zones de confiance ( politique de zero trust )**

# Questions à développement court

**2/ Le cyber threat intel (CTI) (renseignement sur la menace cyber ) est un processus complet.**

**En expliquant son fonctionnement, vous expliquerez comment il est intégré à un SOC et pourquoi les RSSI doivent aussi suivre les alertes**

**Correction : le CTI est la production d’indicateur permettant de se prémunir et détecter les attaques informatiques. Pour cela, on va analyser les assets ( biens de l’organisme) et les sources de menaces via les modes d’attaques des groupes pouvant cibler le ou les SI.**

**En produisant des IOC ( indicator of compromission) le CTI est integré à la recherche de traces ou éléments pouvant poindre sur une attaque informatique. La forme évoluée de ceci est le hunting. C’est-à-dire de rechercher des signaux faibles dans les alertes déjà générées pour détecter des attaques complexes type APT**

**3/l’analyse de risque est une activité importante dans de nombreux domaines dont la cybersécurité. En vous basant sur un exemple d’attaque de ransomware, vous expliquerez les étapes de traitement du risque propre à ce type d’incident de sécurité.**

**Le traitement du risque est composé de 3 phases :**

* **Identifier les mesures potentielles relevant de la prévention, de la préparation, de l’intervention et du rétablissement :**
  + **Sensibiliser à ce risque (prévention)**
  + **Desactiver les modules inutiles sur le système d’exploitation ( prévention)**
  + **Mettre en place une solution anti-virale (préparation)**
  + **Solution de sauvergarde ( prévention )**
  + **Mettre en place un edr (intervention et rétablissement )**
* **L’évaluation et la sélection des mesures.**
  + **Vérifier l’impact des mesures sur le SI**
    - **Disponbilité**
    - **Cout licences**
    - **Cout formation**
    - **Complexite de mise en œuvre**
    - **Décrire les test de non régression**
* **Planification et de la mise en œuvre des mesures retenues.**
  + **Planifications des Mises en prod**
  + **Dérouler les test de non régression**
  + **Communiquer sur les indisponibilites ou les objectifs**

**4/la mise en place d’une certification IS0 22301 est en cours. Que pouvez-vous utilisez afin de faciliter ou nourrir la mise en place d’un SMSI au sein de la même entité.**

**Vous penserez à synthétiser votre réponse pour argumenter votre projet au près d’une gestion.**

**La norme ISO 22301 explique la mise en place d’un système de management de la continuité d'activité. A ce titre, elle rejoint**

* **les analyses de risques, `**
* **le listing des biens,**
* **la responsabilité des parties internes et externes**
* **la mise en place des communités de pilotage et de contrôle**

**à ce titre les certifications croisées sont plus rentables mais nécessite une séléction rigoureuses des organismes de certifications.**

**5/l’intelligence économique est plus qu’une activité de la sphère géopolitique. Comment l’intégrer dans la cybersécurité sans la réduire à une activité de CTI ?**

**Correction : l’IE permet de lister les biens immatérielles de l’organisme plus finement que ne serait le faire une analyse des fichiers et dossier vu par une équipe d’exploitation. De plus, l’approche géopolitique assure une plus grande connaissance des sources de menaces exogènes à l’organisme. Enfin l’approche et les techniques propres à l’OSINT permettent de se placer dans la position d’un groupe de hacker réalisant la première étape de la killchain ( le repérage )**

**6/ Proposer 4 indicateurs de performance permettant de prouver que l’investissement dans un SOC est pertinent. On parle de retour sur investissement de sécurité (ROSI), peut-on le comparer à un ROI classique ?**

**Correction :**

* **Nombre d’alertes par jours et son évolution**
* **Connaissance du périmètre et des postes à jour (évolution mensuel)**
* **Délai de traitement moyen constaté par ticket d’incident**
* **Détection apportée par le CTI par rapport aux règles de base proposées par les éditeurs des éditeurs de sécurités.**

**Le ROI permet de connaitre la rentabilité d’un investissement. Dans le ROSI on va calculer par exemple le cout qu’aurez créer une attaque informatique pour l’organisme.**

**Donc il ne faut pas voir la rentabilité mais les économies potentielles aux ressources consacrées.**

**7/ une SMSI ne se copie pas, il doit être créé dans un cadre précis et sur un périmètre maitrisé. Qui peut réaliser ce projet ? doit-il être forcément certifié pour mener à bien celui-ci ?**

**Le RSSI peut réaliser ce type de projet mais un responsable de projet SMSI peut etre désigné. La certification d’une personne ne permet de s’assurer que ses compétences quant à un cadre normatif nullement que ces compétences ne sont pas suffisantes à la mise en place. On pourra néanmoins préférer une personne ayant une certification 27001 Lead Implementor.**

**Finalement, c’est le SMSI qui doit être certifié.**

**8/La gestion des vulnérabilités est de la responsabilité du RSSI. Mais en amont et en aval des actions sont réalisées afin de pouvoir valider ce processus de sécurité opérationnelle. En paraphrasant, quelles sont les informations et actions requises ?**

**Actions et informations**

* **En amont :**
  + **La tenue de la liste des biens supports portant les vulnérabilités ( informations)**
    - **Technique : reseau système web**
    - **Personnel :: suivi formation, sensibilisation, charte, engagement de responsabilité**
    - **Financement :: budget nécessaire et consenti**
  + **Abonnement à un CERT et flux de mise à jour de sécutité**
* **En aval :**
  + **Suivi indicateur incident**
  + **ROSI**
  + **Pourcentage des biens supports techniques patchés**
  + **Réagir aux diffusions de vulnérabilités des éditeurs et CERT**

**9/**

**Dans cette question : Octo leebe c’est le leader français de la conservation de données de santé et des rdv médicaux**

**En tant que chef de la section infrastructure du groupe, vous avez une deuxième casquette de DPO.**

**Pierre votre nouvel admin système se plaint des lenteurs et temps d’accès aux bases de données. Il ne jure que par Amazon et ses services cloud. Lors de la réunion de début de semaine, il annonce lors de son tour de parole avoir transférer sur le week-end l’ensemble des services de stockage ainsi que les données utilisateurs de votre groupe « Octo leebe ». D’après son analyse, les technologies et capacités de stockage en France par l’entreprise ne correspondaient plus aux standards de l’industrie.**

**Indicateurs à l’appui, il annonce avoir solutionné les problèmes de performances de l’infra et du site web…**

**Quelle est votre réaction ? quelles sont les actions à mener sans délais ?**

**(Question sans intérêt ) Pierre va-t-il être promu au poste de team leader system le mois prochain ?**

**Correction :**

**En tant que DPO vous devez sans délai déclaré un transfert des données de santé à la CNIL ainsi que communiquer auprès des utilisateurs. Ceci en préparant un message avec les responsables de octo leebe.**

**En effet, votre structure quoique lente est certifiée HDS ( hebergeur de données de santé ) donc son périmètre et contexte sont fixés. Amazon est aussi HDS mais les données sont stockées dans le cloud dont le *cloud act* et le *patriot act* s’appliquent. Les répercussions sont importantes en terme juridique.**

**Techniquement :**

* **Le compte de pierre est suspendu, mais il reste à disposition pour expliquer les actions qu’il a mené.**
* **Il faut connaitre les impacts techniques sur les solutions de stockage et réaliser une série de test à prioriser afin de ne pas se perdre en action stériles.**
* **Evaluer un rollback**
* **Vérifier la disponibilité des données et prendre contact avec le service d’hebergement d’AMAZON**
* **Vérifier qui était d’astreinte ce WE (surement Pierre)**
* **Communiquer aux équipes internes**
* **Préparer beaucoup de café**

**Une cellule de crise doit se constituer afin de gérer la situation dans le temps et la complexité en laissant les équipes techniques répondent aux questions.**

**Il n’y a pas bonnes ou de mauvaises réponses quant à la situation, le pragmatisme doit prédominer sur l’instinct et les actions portées par des émotions trop fortes comme la rage ou l’inscription à cours de MMA.**

**Vous doutez de la reconversion de Pierre chez amazon et vous envisagez plutôt quelque chose dans la culture du chanvre sur l’altiplano : Ceci ne fait aucun doute dans votre esprit au moment de la réunion de lundi à 23h00 avec la cellule de crise mais le café est bon.**