QCM PEI – Analyse de la menace

Une seule bonne réponse par question. Surlignez la bonne réponse en jaune et soumettez dans moodle votre rendu au format PDF avant le 16 décembre 2022 à 23h59.

1. **L’analyse de la menace cyber se concentre sur l’étude (3 pts):**
   1. Des vulnérabilités logicielles
   2. Des moyens de protection contre les attaques informatiques
   3. Des groupes de pirates informatiques
   4. Des risques liés aux usages du numérique
2. **Les rançongiciels (3 pts) :**
   1. Sont des logiciels malveillants dont le but est de détruire de la donnée
   2. Sont utilisés à des fins d’espionnage
   3. Sont des groupes de pirates réalisant des arnaques informatiques
   4. Sont apparus à la fin des années 1980
3. **Quels sont les trois types d’analyse de la menace selon l’ANSSI (3 pts) :**
   1. Stratégique, tactique/opérationnelle, technique
   2. Humaine, machine/système, électromagnétique
   3. Système, réseau, utilisateur
   4. Cybersécurité, Cyberdéfense, Gestion des risques
4. **Pourquoi la Corée du Nord réaliserait des attaques informatiques ? (3 pts) :**
   1. Pour soutenir son programme nucléaire militaire
   2. Pour voler des secrets industriels liés à la transition écologique
   3. Pour montrer aux Nations Unis l’excellence de ses universités
   4. Pour se venger de sa défaite lors de la seconde guerre mondiale
5. **Dans le piratage de la blockchain d’Axie Infinity développée par Sky Mavis (2 pts) :**
   1. Les attaquants ont piraté la blockchain Ethereum pour voler les jetons numériques
   2. Les pirates ont envoyé un mail de phishing pour rentrer dans le réseau de Sky Mavis
   3. Le gouvernement chinois a ordonné à ses mineurs de bitcoin de valider de fausses transactions
   4. Europol a arrêté la plupart des pirates
6. **Le Crime-as-a-Service (2 pts):**
   1. Est un blackmarket sur le darknet Tor
   2. Est le groupe de pirate qui s’est introduit dans le réseau de Colonial Pipeline
   3. Désigne l’ensemble des services disponibles pour les cybercriminels
   4. Est le nom des logiciels du type Stuxnet
7. **La Cyber Kill Chain (2 pts):**
   1. Est une vulnérabilité dans la sandbox JVM
   2. Est une liste de pointeurs vulnérables à un buffer overflow
   3. Est une manière de découper une attaque informatique en étapes intermédiaires
   4. Est un mécanisme de suppression automatique dans les logiciels malveillants
8. **La logique criminelle est avant tout guidée (1 pt) :**
   1. Par des motivations économiques
   2. Par des motivations ludiques
   3. Par des motivations idéologiques