1)Cybersécurité = effort continu pour protéger les systèmes mis en réseau et connectés à Internet, ainsi que pour protéger toutes les données contre l'utilisation ou le méfait non autorisés

2)Internet des objets (ioT) = un grand réseau d'objets physiques, dont des capteurs et des équipements

3)Les trois composants du principe CIA (Confidentiality, Integrity and Availability) = confidentialité, intégrité et disponibilité

4)a) Confidentialité = également appelé protection des renseignements personnels, signifie que l'accès aux données est limité uniquement au personnel autorisé b) Les méthodes pour assurer la confidentialité = cryptage des données, ID et mot de passe, authentification à deux facteurs, etc…

5)a) Intégrité = le terme qui désigne l'exactitude, la cohérence et la fiabilité des données b) Les méthodes pour assurer l'intégrité = permissions des fichiers, contrôle d'accès des utilisateurs, contrôle des versions et sommes de contrôle

6)Disponibilité = le terme indiquant que les services et les données sont bien conservés, tout en étant accessibles à tout moment

7)Menaces internes pour la sécurité = attaques provenant de l'intérieur même de l'entreprise

8)Menaces externes pour la sécurité = attaques provenant de l'extérieur de l'entreprise

9)Chapeaux blancs (White hat) = des personnes ou des entreprises qui entrent par effraction dans les réseaux ou dans les systèmes informatiques pour découvrir les failles de sécurité ; ces personnes visent l'amélioration de la sécurité de ces systèmes

10)Chapeaux noirs (Black hat) = des personnes ou des entreprises qui profitent de toute vulnérabilité à des fins illégales, financières ou politiques

11)Agresseurs organisés = entreprises de cybercriminels, hacktivistes, terroristes et de pirates financés par un État

12)Guerre cybernétique = un conflit basé sur Internet et qui implique la pénétration dans les réseaux et les systèmes informatiques des autres pays

13)Stuxnet = un programme malveillant conçu pour endommager l'usine d'enrichissement nucléaire de l'Iran ; ce programme est un exemple d'attaques financées par un État

14)Partenariat multilatéral international contre les cybermenaces (IMPACT, International Multilateral Partnership Against Cyber Threats) = un partenariat mondial des gouvernements, secteurs et académies du monde entier dédié à l'amélioration des capacités globales face aux cybermenaces

15)Éthique = des codes de conduite qui sont, quelques fois, mais pas toujours, imposés par les législations