**DEFINITION OF CYBER SEC**

La cybersécurité est une solution défensive pour protéger tout système connecté à Internet contre les cybermenaces et les attaques. Objectifs de la cybersécurité Il convient de toujours appliquer les règles de cybersécurité pour protéger les données des entreprises, petites et grandes, comme des personnes.

**IMPORTENCE DE LA CYBER SEC**

prévenir et de protéger contre les attaques malveillantes tous les types d'appareils électroniques, depuis les ordinateurs, les serveurs et les réseaux informatiques jusqu'aux téléphones mobiles et aux imprimantes, pour empêcher que ces appareils ne soient attaqués et ainsi protéger les données personnelles

**DEFINITIONS**

**Vulnérabilité** : Faiblesse au niveau d'un bien

**Menace** : Cause potentielle d'un incident

**Attaque** : Action malveillante

**Test d'intrusion** : essayer d'accéder au système à l'aide des techniques utilisées par les attackant malveillant

**Ingénierie sociale** : vise a manipuler et prendre confiense des victims a fin de prendre des info sensible .

**Interception des communications** : obtenir plus d'informations sur l'environnement

**ANSSI** : autorite national securite system d'info

**PSSI** : politique securite system d'info / les règles de sécurité applicables à la protection du SI

**CVE** : Common Vulnerabilities and Exposures / Un dictionnaire de vulnérabilités

**CWE** : Common Weaknesses Enumeration / types de faiblesses logicielles

**EXPLOIT-DB** : Archive des exploits publics et des logiciels vulnérables correspondants

**SAST** : Tests statiques de sécurité des applications / sur source code avant de publier l'app

**DAST** : Tests dynamiques de sécurité des applications / teste effectué en cours d'exécution

**L'AUTENTIFICATION** : consiste à savoir l'identité

**LE CONTROLE D'ACCES** : contrôler s'il a le droit d'y accéder a des ressource ou une entité

**LA CONFIDENTIALITE** : Il s'agit de garantir que des données prive soit inaccessible

**LA DEFENSE EN PROFONDEUR**

Une stratégie de cybersécurité de défense en profondeur est d'ajouter plusieurs couches et bariieres a fin de rendre la tâche plus difficile à un attaquant pour acceder au resaux .

**MODULE ZERO TRUST**

zero trust est une stratégie de cybersécurité centrée sur ne jamais faire confiance, donner le minimun de permission .

**ISO 27001**

Ce standard définit les exigences et les thecnique à mettre en place

**ISO 27002**

Ce standard présente un guide de bonnes pratiques

**ISO 27005**

Ce standard permet de gestionner les risks