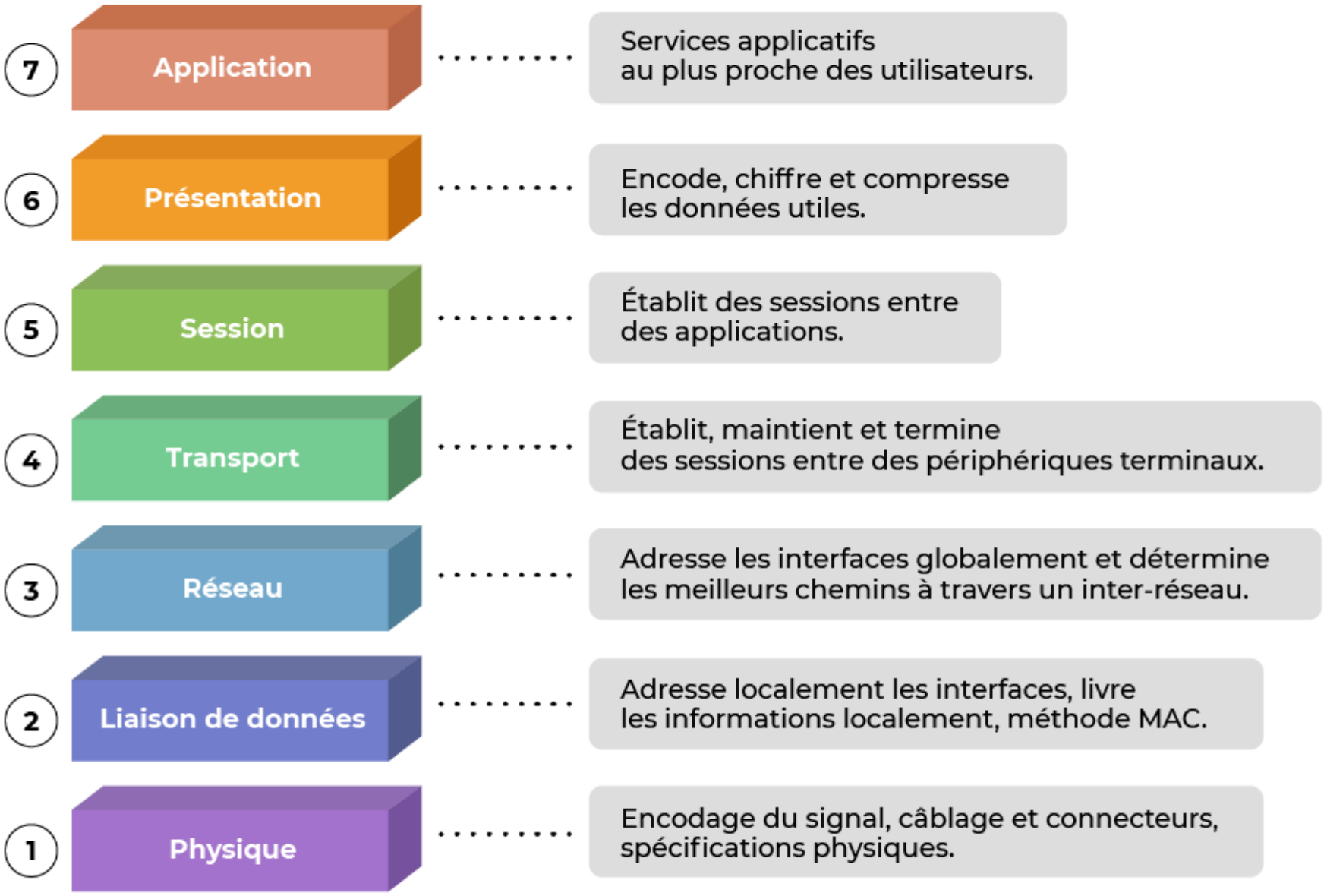
Cours 10 :
La Sécurité en couches

JACQUEMIN Mathieu

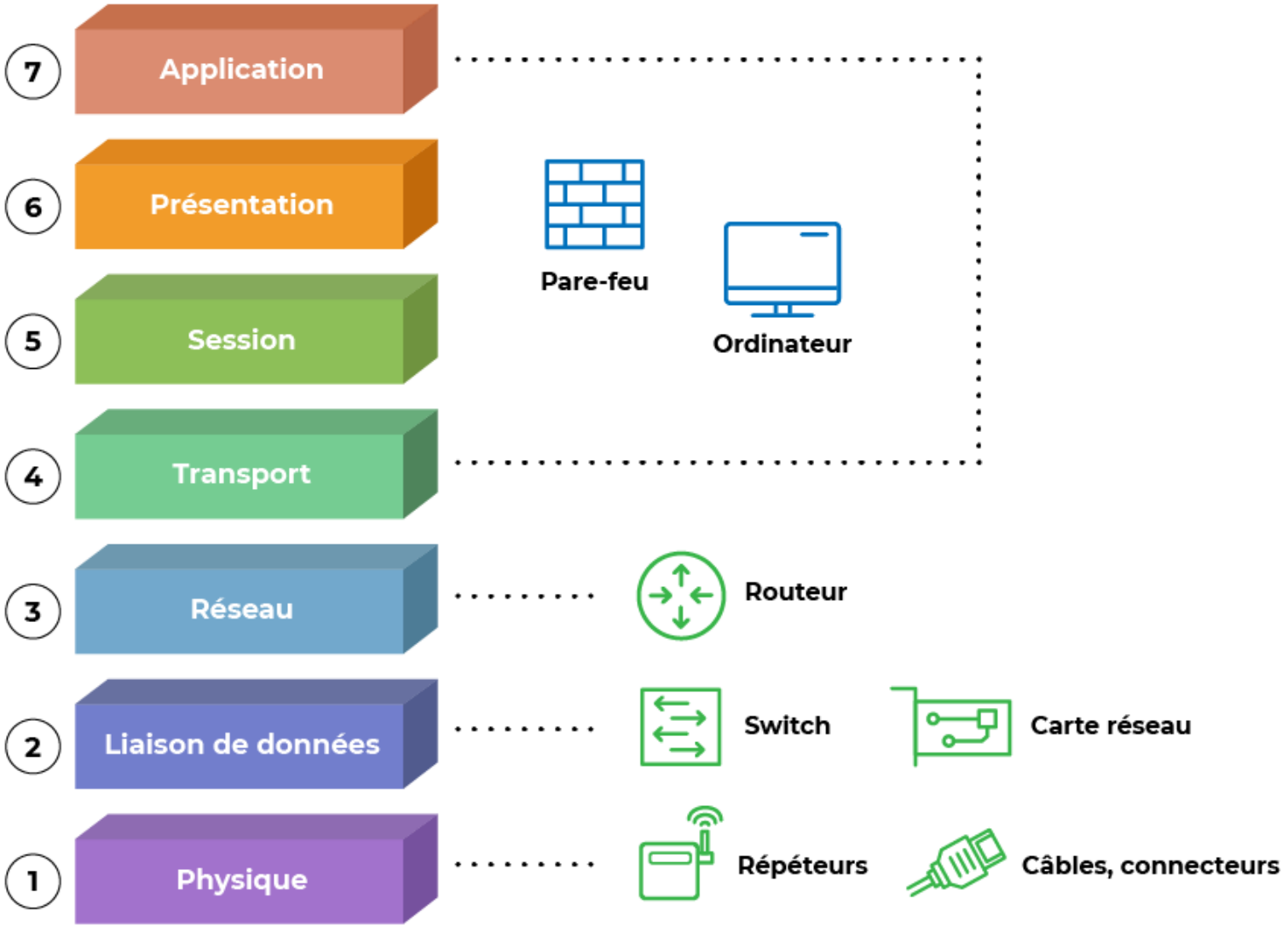
Disclaimer

- Ce cours a été créé dans le but d'informer et d'éduquer les participants sur les sujets liés à la cybersécurité. L'ensemble des techniques présentées le sont à titre pédagogique et préventif afin de pouvoir se prémunir d'attaque potentiel.
- Certaines des techniques présentées sont illégales et dangereuses si elles sont utilisées à mauvais escient, sans maitrise, et sans consentement.
- Il est interdit d'utiliser ces techniques contre toute entité dont vous ne disposez pas le consentement. Dans le cadre d'un accord pour audit, il est obligatoire d'agir dans le cadre d'un contrat parfaitement défini, écrit, et signé par les deux parties.
- Vous devez respecter la loi en vigueur ainsi qu'utilisez les techniques avec éthique et responsabilité.
- Je me dédouane de toute responsabilité en cas de problème ou d'incidents à la suite de ce cours.
- Vous êtes seul responsable de l'usage fait des connaissances enseignées.

Rappel Modèle OSI



Rappel Modèle OSI



Introduction

Nos Systèmes d'Information (SI) sont en dangers !

- la prolifération des virus, bots et autres malwares
- le vol de données (ou fuite de données)
- L'altération d'information
- la compromission de données

DICT

Les indicateurs de sécurité informatique

Disponibilité

Intégrité

Confidentialité

Traçabilité

DICT

Disponibilité

Tout d'abord, la disponibilité du SI assure que les données ou les composants amenant certaines fonctionnalités soient toujours en mesure d'offrir les services pour lesquels ils ont été conçus.

→ Accessible et utilisable

Intégrité

les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.

→ Source sure et non modifiée

DICT

Confidentialité
Seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.
→ Seulement les personnes habilitées

Traçabilité (ou « preuve »)
Garantir que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées. Il faut être capable de savoir qui réalise quoi, et quand.
→ Impossible de nier

EXEMPLES

Attaque par déni de services (DOS) → Perturber la disponibilité

Perturber la confidentialité ← **Espionnage**

Vol de données → Perturber l'intégrité et la confidentialité

Perturber la traçabilité et l'intégrité ← **Usurpation d'identité**

La couche 1: Physique

Les menaces ?

Involontaires :

Problème matériel
Catastrophe naturelle
Incendie / Inondation
Surcharge électrique
Déconnexion et dégradations

Volontaires :

Vol de matériel
Destruction
Accès ou Connexion non autorisé
Remplacement d'un matériel

La couche 1: Physique

Se défendre ?

Redondance de matériel (sur site et distant)
Alarme incendie / inondation et matériel ignifugé / protégé
Onduleurs
Climatisation
Cable Management
Salle dédiée à l'informatique

Salle verrouillée
Baies et armoires verrouillées
Contrôle d'accès
Vidéosurveillance
Matériel fixe (difficilement emportable)
Chiffrement des disques et périphériques mobiles
Surveillance des journaux d'accès (logs)
Désactiver port du switch par défaut

La couche 2 : Liaison

Les menaces ?

Involontaires :

Boucle
Perte de configuration

Volontaires :

Usurpation ARP
Saturation DHCP
DHCP Rogue

La couche 2 : Liaison

Se défendre ?

Spanning Tree
Switch redondants
Sauvegarde de la configuration

Avoir une bonne sécurité couche 1
Activer la sécurité par port et autoriser certaines adresses MAC
Réduire la surface d'attaque grâce au VLAN

La couche 3 : Réseau

Les menaces ?

Involontaires :

Panne matérielle
Panne de liaison internet

Volontaires :

Usurpation IP
Attaque par saturation de bande passante (DOS / DDOS)
Route Poisoning

La couche 3 : Réseau

Se défendre ?

Redondance des routeurs et des pares-feux
Redondance de liens internet
Sauvegarde des configurations

Avoir une bonne sécurité couche 1 et 2
Utiliser des ACL
Avoir un matériel performant et moderne
Activer une solution de prévention d'intrusion et de détection d'intrusion pour détecter un comportement malicieux (IPS/IDS)

Les couches 4, 5, 6 et 7

Les menaces ?

Involontaires :

Mauvais paramétrage
Mauvaise manipulation
« Bug » Logiciel

Volontaires :

Usurpation d'identité
Détournement de données
Augmentation de privilèges
Espionnage
Utilisation d'exploits de faille

Les couches 4, 5, 6 et 7

Se défendre ?

Sauvegarde (règle des 3-2-1)
Journaux

Mises à jour !
Désinstaller / Désactiver tout logiciel non utilisé
Mot de passe fort, unique et aléatoire
Double authentification

Analyse de risque

L'analyse de risque ou l'évaluation de risque est un ensemble de technique permettant d'avoir une vue exhaustive des risques pour une entreprise.

Son objectif est de donner des priorités sur la mise en place de mesure de gestion des risques

Un risque se qualifie selon sa :

- Probabilité d'occurrence / Vraisemblance
- Gravité/Impact

Moodle