

Brouillon - Plan de formation

Attention : Cette page est en cours de rédaction et son contenu peut être faux ou inexact. Merci de lire cette page avec toutes les précautions nécessaires.

0. Introduction à la formation (1h)

non mutualisable

- *présentation de la formation*
- *test de positionnement*

Séquence 1: Révisions début de cycles (8h)

Séance 1 - Un ordinateur (2h)

- Définition
- Différents types de matériels pour différents usages
- Les composants matériels
- Bios / UEFI
- Une séquence de démarrage de A à Z
- Les systèmes d'exploitation (familles et types) + architectures

Séance 2 - systèmes de numération (4h)

- Base 2 / Base 10 / base 16 (3h)
- (Spécifique CIEL) (1h)

- o Encodages couleurs
- o Encodages data (ascii, unicode, utf-8,16,32)

Séance 3 - La relation client/serveur (1h)

- Définition du serveur
- Les spécificité matérielles (redondance)
- Les Versions OS spécifiques
- Versions core et cli à moins de ressources, moins de surface d'exposition

Évaluations (non mutualisable) - 1h

Séquence 2: Introduction à la virtualisation (8h)

Séance 1 - Les types d'hyperviseurs (1h)

- Type1 vs type2
- Evolution des serveurs au cloud
- Containeurs

Séance 2 - Caractéristiques et limitations (2h)

- CPU
- Mémoire
- Stockage et VSAN
- Réseaux et SDN

Séance 3 - Installation de son hyperviseur de LAB (4h)

- Installation de proxmox VE + interface graphique

- Paramétrage de base
- Upload des isos
- Création des templates
 - Win11
 - Ubuntu Desktop
 - Win srv 2k25 (GUI et core)
 - Ubuntu Server
- Sysprep / cloud-init & conversion en template
- Explications sur le clonage et snapshots

Explications des principes de séparation des environnements (DEV/UAT/PROD)

Évaluations (non mutualisable) - 1h

Séquence 3: Introduction au réseau (10hsio - 15h CIEL)

Séance 1 - Principes généraux (1h)

- Définition
- Topologies
 - (spécifique CIEL) Topologies des réseaux mobiles / radio et industriels
- LAN / WAN
- Introduction au modèle OSI, principes de construction du trafic réseau

Séance 2 - Modèle OSI - Couche 1 (1h)

- ethernet
 - norme ethernet
 - Bitrate & bande passante
 - atténuation, bruit
 - types câbles ethernet (droits croisés)
 - catégories de câbles
 - (Spécifique CIEL) appareils de mesures et de diagnostic.
- Fibre optique

- types de fibres
- connectique
- (Spécifique CIEL) Outils de mesures et de diagnostics + Episseuse
- WLAN
 - SSID, Canaux, protections et chiffrements (introduction sommaire)
 - (Spécifique CIEL) co-enseignement physique
 - Longueurs d'onde / fréquences
 - Canaux
 - (CIEL co-enseignement physique)
 - Supports de propagation (guidé/non guidé)
 - Principes de transmission en espace libre
 - Caractérisation temporelle et fréquentielle des signaux
 - Appareils de mesures (oscilloscope, analyseur de spectre)

Séance 3 - Modèle OSI - Couche 2 (1h)

- MAC address
- Ethernet frame structure (MAC src/dst, ethertype, FCS)
- switch
- VLAN (802.1Q) – untag, tag, trunk
- Broadcast domain (au sens collision) & tempête de broadcast
- (spécifique ciel) Réseaux industriels (Modbus over IP, CAN, RS485,12C) - introduction
- (spécifique ciel) WPAN/WLAN spécifications.

- TP Cisco packet tracer :
 - switch I2
 - PC
 - tables MAC / requêtes ARP / RARP
 - VLANs

Séance 4 - Modèle OSI - Couche 3 (2h)

- Addressage IPv4 (addr, network, mask, subnetting, broadcast)
- Sous-réseaux, CIDR
- Routage et tables
- TTL, fragmentation
- NAT/PAT
- ICMP (ping, traceroute)
- (spécifique CIEL) réseaux IoT (LPWAN, 802.15.4)
- (spécifique CIEL) architecture réseaux cellulaires.

- TP Cisco packet tracer :
 - réseaux
 - vlan & acl
 - routage
 - nat/pat (avec sortie "internet")

Évaluations intermédiaire (couche 1 à 3) - 1h

Séance 5 - Modèle OSI - Couche 4 (1h)

- Protocoles principaux : UDP / TCP
 - statefull et stateless
 - TCP handshake (syn / syn-ack / ack)
 - UDP datagrams
 - Flow control
 - IP/port = définition de socket.

Séance 6 - Modèle OSI - Couche 5 (1h)

- Établissement de session, maintenance, teardown
- Checkpoint, dialog control
- TLS handshake, smb session sip dialog
- (spécifique CIEL) MQTT, VoIP signaling

Séance 7 - Modèle OSI - Couche 6 (1h)

- Encodage
- Serialization (json xml)
- Encryption
- compression
- (spécifique CIEL) Niveaux de sécurité attendu - privacy by design

Séance 8 - Modèle OSI - Couche 8 (1h)

- Différents services (abordés après dans des modules dédiés)
- (Spécifique CIEL) services VoIP, IoT, Indus, etc...

Séquence 4: Notions sur les systèmes (5h)

Séance 1 - Systèmes windows (2h)

- Version / information systèmes
- Structure système de fichier
- Utilisateurs et groupes
- Devices et drivers
- Disques, formatage, systèmes de fichiers
- Sécurité (antivirus / pare-feu)
- Protocoles de gestion à distance (RDP)

Séance 2 - Systèmes windows (2h)

- Version / information systèmes
- Structure système de fichier
- Utilisateurs et groupes
- Devices et drivers
- Disques, formatage, systèmes de fichiers
- Sécurité (antivirus / pare-feu)
- Protocoles de gestion à distance (SSH)

Séquence 5: Introduction à la cybersécurité (8h)

Séance 1 - Les fondamentaux (1h)

- CIA Triad
- Menaces
 - types de hackers
 - vecteurs d'attaques
 - Golden rules

Séance 2 - Acteurs réglementaires et normatifs - (1h)

- CNIL, ANSSI, Cert-FR
- Malveillance.gouv
- RGPD et NIS2

Séance 3 - Méthode Ebios (4h)

- Lecture et déroulé du guide de la méthode Ebios

TP ou travail d'alternance : appliquer la méthode EBIOS à un processus de l'entreprise et livrer un rapport

Séance 4 - les approches Zero trust et security by design (1h)

- moindre exposition et limitation des informations exposées.
- cloisonnement / microsegmentation
- zones /
- stronghold

Évaluations (non mutualisable) - 1h

Séquence 6: Gestion de projet (4h)

Séance 1 - Présentation des 3 projets du cycle (2h)

- Présentation du projet IT
 - Mise en œuvre d'une infrastructure d'entreprise sécurisée
 - IT
 - VoIP
 - vidéosurveillance
- Présentation des 2 projets électroniques
 - Solution de contrôle d'accès
 - Solution de monitoring de salle serveur
- Présentation du projet de développement
 - Interfacer à travers des API les deux solutions
 - Réaliser un dashboard de monitoring et un système d'alerte

Séance 2 - Méthodologie de projet (1h)

- Étapes d'un projet
- Documents à fournir à chaque étape.
- méthodologie de déroulé de projet
 - scrum / agile / 3Ops
- KANBAN

Évaluations (non mutualisable) - 1h

Info : Le reste de la formation avancera en mode projets, avec ses différentes étapes de préparation et ses livrables. Elle suivra des cycles ' besoin --> outils théoriques --> mise en oeuvre --> tests unitaires --> livrables --> audit sécu --> mise en évidence des failles --> sécurisation --> rapport'.

I. Projet IT

Séquence P1.1 : Firewall et segmentation (4h)

Séance 1 - Principes de firewalling (1h)

- principes de bases des règles, ordre de lecture.
- rule shadowing.
- bonnes pratiques.

Séance 2 - Installation et paramétrage de base (1h)

- Création des réseaux sur Proxmox
- Installation OPNsense
- Découverte de l'interface
- mise à jour de firmware
- mise en place de la sauvegarde
- réglages de sécurité

Séance 3 - Mise en oeuvre (1h)

- Explication des bonnes pratiques (aliases, zones, network groups, microsegmentation)
- Mise en place des règles
- Utilisation du logging et repérage de flux
- mise en place des Gateway et de l'Outgoing NAT

Évaluations (non mutualisable) - 1h

Séquence P1.2 : Services et protocoles de bases (2h)

Séance 1 - DHCP - théorie et entraînement (1h)

- Théorie sur le protocole DHCP + DHCP helper
- Mise en oeuvre sur Cisco Packet Tracer.

Séance 2 - DHCP - Mise en pratique (3h)

- Mise en pratique sur linux (KEA DHCP).
- Mise en pratique sur windows.
- Mise en pratique sur OPNsense (KEA DHCP).

Séance 3 - DNS - Théorie et entraînement (1h)

- Théorie sur le protocole DNS.
- Mise en oeuvre sur Cisco Packet Tracer.

Séance 4 - DNS - Théorie et entraînement (3h)

- Mise en pratique sur linux (bind)
- Mise en pratique sur windows
- Mise en pratique sur OPNsense (DNS Resolver et DNS Forwarder)
- (Spécifique CIEL) POC d'une exiltration DNS et du DNS Poisoning

7.3 NTP (2h)

- Protocole NTP
- Relai NTP

EVAL (1h)

8. Gestion de l'identité (AD, LDAP, Kerberos)

8.1 Active directory

- Principes LDAP (domaines, sites, OU)
- Active directory (domain and trust)
- Active directory (niveaux fonctionnels)
- Active directory (site et services)
- Active directory (Users and computers)
- Intégration des PC et serveurs au domaine (win + Linux)

8.2 SAMBA Idap

- Mise en œuvre samba 4 sur linux

8.3 GPO

- Définition et types de GPO
- Mise en application

8.4 audit sécu et remédiation avec pingcastle + GPO

- Fonctionnement de l'authentification kerberos
- Failles exploitables

EVAL (1h)

9. Premier stack LAMP

9.1 Le protocole HTTP (2h)

- Construction d'une URL
- Messages http
- Versions du protocole
- Matrice des status code
- Requests header and body (spécifique ciel)
- Response header and body (spécifique ciel)

9.2 installation stack LAMP (4h)

- Installation de mariaDB

- o Introduction aux bases de données et au SQL
- Installation de apache2
 - o Introduction qux serveurs web
 - o Virtualhosts
 - o Modules et sites
- Introduction à PHP
 - o Fichiers de configurations PHP
- Mise en place de wordpress (à titre d'exemple)
- Démonstration avec wireshark des limitation de http (sans S)

EVAL (1h)

Revision #5

Created 2026-07-17 13:12:00 UTC by Olivier

Updated 2026-07-17 16:49:32 UTC by Olivier