Ressource - Plan de formation CIEL (IR)

0. Introduction à la formation (1h)

non mutualisable

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

I. Révisions / approfondissements de début de cycle

> **Info** : L'idée est de conduire ce cycle sur le premier trimestre. Afin que ceux venant d'autres filières rattrapent le retard. A la fin de ce premier projet, le but est que tout le monde dispose d'une infrastructure simple et fonctionnelle.

Séquence P1.1: Bases de l'infrastructure informatique (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)
  - Encodages couleurs
  - Encodages data (ascii, unicode, utf-8,16,32)

Séance 3 - Les Composantes du SI moderne (0,5h)

- Définition du serveur
- Les spécificité matérielles (redondance)
- Les Versions OS spécifiques
- Versions core et cli à moins de ressources, moins de surface d'exposition
- Relation client serveur
- Architecture du SI
- Systèmes de l'usine connectée

Séance 4 - Les différents modèles d'infrastructures (0,5h)

- On premise
- Hybride
- cloud (IaaS, PaaS, SaaS)

Évaluations - 1h

Séquence P1.2: 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 - 1h

Séquence P1.3: Introduction au réseau (10h sio - 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, Cannaux, 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 l2
  - 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 7 (1h)

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

trait d'humour, parler de la couche 8 :D

Évaluations intermédiaire (couche 4 à 7) - 1h

Séquence P1.4: 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)
- Outils de bases :
  - Monitoring de ressources
  - Services

- Registre

Séance 2 - Systèmes linux (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)
- Outils de bases :
  - Monitoring de ressources
  - Services
  - /etc

Évaluations - 1h

Séquence P1.5: Introduction à la cybersécurité (8h)

Séance 1 - Les fondamentaux (1h)

- CIA Triad
- Menaces et risques
  - types de hackers
  - vecteurs d'attaques
  - méthodologie (7 étapes attaques et méthode picerl)
  - 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.
- défense périphérique / défense en profondeur
- cloisonnement / micro segmentation
- zones / sous réseaux en fonction du degré d'exposition et de la criticité (tiering)
- stronghold

Évaluations - 1h

Séquence P1.6: Introduction au développement (4h)

Séance 1 - Introduction au développement (1h)

- languages bas niveau --> haut nivaut
- langages procéduraux vs langages objets
- languages interprétés vs compilés
- languages descriptif
- vibe coding
- Frontend et backend

Séance 2 - Les briques de bases de la programation (2h)

- Les instructions
- Les conditions
- Les boucles
- Les fonctions
- Les bibliothèques
- Classes, objets, propriétés, fonctions sur les objets.

Évaluations - 1h

Séquence P1.7: Gestion de projet (4h)

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

- Présentation du projet IT
  - Mise en œuvre d'une infrastructure d'entreprise sécurisée & redondée
    - IT
    - VoIP
    - vidéosurveillance
- Présentation du projet électronique / IoT
  - Solution de contrôle d'accès.
  - Solution de monitoring de salle serveur.
  - interfaçage avec l'infra de supervision existante.
  - Réalisation d'une interface de monitoring
- Présentation du projet Pentest
  - entrainement aux outils et méthodes du pentest et de la forensic
  - participation aux audits de sécurité, livraison des rapports

Séance 2 - Méthodologie de projet (2h)

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

Évaluations - 1h

> **Info** : Le reste de la formation avancera en mode projets, avec ses différentes étapes de préparation et ses livrables. Elle suivra des cycles comme définis dans les notes de l'introduction à la formation.

> **Conseil** : Il pourra être intéressant d'alterner la progression des différents projets, afin de varier les plaisirs et travailler avec eux l'organisation.

II. Projet IT (1ère année)

Séquence P2.1 : Firewall et segmentation (4h)

Séance 1 - Principes de firewalling (1h)

- principes de bases des règles, ordre de lecture.
- rule shadowing.
- bonnes pratiques
  - zones, groupes, vlan (microsegmentation)
  - aliases, groupes host/ports
  - optimisation des règles, scaling

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 - 1h

Séquence P2.2 : Services et protocoles de bases (12h)

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

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

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

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

Évaluations - 1h

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

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

Séance 4 - DNS - Mise en pratique (2h)

- 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

Évaluations - 1h

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

- Théorie sur le protocole NTP.
- Mise en évidence de l'importance de la synchro horaires (problèmes potentiels).
- Mise en oeuvre sur Cisco Packet Tracer.

Séance 4 - DNS - Mise en pratique (2h)

- Mise en pratique sur linux (ntp)
- Mise en pratique sur windows
- Mise en pratique sur OPNsense (Client/serveur/relai)

Évaluations - 1h

Séquence P2.3 : Gestion de l'identité (7h)

Séance 1 - Active directory : Notions de bases (1h)

- Principes & protocoles AD (LDAP, Kerberos)
- Forêts, domaines, OU
- Utilisateurs et ordinateurs
- Netlogon et sysvol
- (Spécifique CIEL) présentation des failles kerberos

Séance 2 - Active directory : Mise en pratique 1 (2h)

- Création de domaine
- Création d'utilisateurs et de groupes
- intégration de postes au domaine (Windows et linux)
- Utilisations des outils de diagnostics (dcdiag, etc...)

Séance 3 - Active Directory : notions avancées (1h)

- Sites et services
- Domaines parents/enfants
- Trusts & niveau fonctionnel

Séance 4 - Active directory : Mise en pratique 2 (2h)

- Déclaration des sites
- Déclaration des subnets
- Ajustement du DNS

Évaluations - 1h

Séquence P2.4 : Serveurs de fichiers (6h)

Séance 1 - Différents protocoles et théorie associée (2h)

- Protocoles de partages de fichiers (SMB, NFS, SMB over QUIC)
- Gestion des autorisations
  - Priorité refuser sur autoriser
  - Différenciation des droits de partages et droits systèmes.
- Présentation des partages par défaut et partages administratifs
- Mise en œuvre de partage de fichiers sous windows (partages équipes et publics)
- Partages personnels pour les utilisateurs et droits associés (énumération, etc...)
- (Spécifique CIEL) Démonstration Eternalblue via SMBv1

Séance 2 - Methode AGDLP (1h)

- Portée et types de groupes
- Principes et avantages de la méthode AGDLP
- Mise en pratique
- Intérêt dans des contextes multi-domaines

Évaluations - 1h

Séance 3 - Racine DFS (1h)

- Mise en place d'une racine DFS pour rendre transparent les changements de serveurs ou maintenances

Séance 4 - Serveurs de fichiers linux (samba4) (2h)

- Mise en place de partages à destination des applications sur linux.

Séquence P2.5 : Hardening AD et filer (6h)

Séance 1 - outils théoriques GPO (1h)

- GPO utilisateurs & ordinateurs
- GPO de sites
- Bonnes pratiques autour des GPO
- Limiter la portée des GPO
- Délégations

Séance 2 - Mise en place LAPS (2h)

- Mise en place de LAPS pour les comptes admins locaux.
- Prouver le fonctionnement par le biais des cahiers de test

Séance 3 - Audit de sécurité avec PingCastle + rémédiation (2h)

- Mise en place d'une racine DFS pour rendre transparent les changements de serveurs ou maintenances

Évaluations - 1h

Séquence P2.6 : Installation stack LAMP GLPI (6h)

Séance 1 - Définition & Installation du stack LAMP (2h)

- Installation et utilisation d'un serveur de base de donnée (MYSQL)
- Utilisation SQL et création de base de donnée
- Création de la base de donnée, de l'utilisateur, attribution des droits
- Sécurisation de l'instance MYSQL (limitation des écoutes, notions de bases localhost, %, etc...)

- Installation apache2 + PHP
- Introduction des notions de backend - frontend
- Virtualhost, paramétrage et sécurisation serveur web
- Notions fondamentales sur le protocole HTTP (request, headers, etc...)
- (Spécifique CIEL) Exploitations de failles web HTTP + Reverse shell (avec P0wny par exemple)

Séance 2 - Installation GLPI (2h)

- Téléchargement et installation de GLPI
- Configuration de base
- Présentation ITIL

Séance 3 - Mise en situation pro (1h)

- Qualification de demandes, incidents, problèmes, etc
- Définition des acteurs : demandeur, technicien, superviseur, validateur, etc...
- Mise en places de formulaires et de catalogue de services
- Liaison LDAP
- (Spécifique CIEL) Déclaration et gestion des incidents de sécurité

Évaluations - 1h

Séquence P2.7 : Chiffrement / PKI / Certificats / HTTPS (8h)

Séance 1 - Introduction kalilinux (1h)

- Installation Kalilinux
  - (les outils seront introduits au fur et à mesure)

Séance 2 - chiffrement, hash, signatures (1h)

- Cour théorique sur le chiffrement, hash, signatures
- TP - Chiffrement, hash, signature

TP KALI 1 - VulnBank (system intrusion) CIEL X SIO (2h)

Séance 3 - Cours sur les PKI / CA / Certificats (2h)

- Réponse aux problématiques des flux non chiffrés.
- Cours sur la PKI / Certificats.
- (Spécifique CIEL) Algorithme RSA fonctionnement clé publique, privée : co-enseignement mathématiques

Séance 4 - Mise en oeuvre root CA / Intermediate (2h)

- Mise en oeuvre simple avec openSSL --> préparation offline CA
- Installation configuration de ADCS --> Préparation domain CA
- Mise en oeuvre avec OPNSense --> Préparation CA pour le VPN

Évaluations - 1h

Séquence P2.8 : Projet récap / Ferme RDS (6h)

Séance 1 - Présentation du projet (1h)

- Présentation du projet
- Préparation pour l'intégration à l'infrastructure déjà déployée
- Présentation des schéma techniques

- Notions sur les architectures de services distribuées et redondance (Sessions HOST, licencing server, gateways, Broker)

Séance 2 - Mise en oeuvre de la solution (2h)

- Déploiement des différents composants
  - Stockage des disques de profils
  - Sessions Hosts
  - Serveur de licences
  - Broker
  - Gateways
- Création des groupes d'applications
- Définition des permissions
- Installation des applications

Séance 4 - Gestion et maintenance (2h)

- Exercices sur la gestion et la maintenance de la solution
  - Définition d'une fenêtre de maintenance
  - Déroulé d'une maintenance / Mise à jour applicative
    - Avertissement des utilisateurs
    - Passage du serveur en mode drainange
    - mise à jour de l'application
    - remise en ligne du serveur
    - Passage du second serveur en drainage
    - Fermeture des connexions
    - Mise à jour de l'application
    - Rétablissement du service en mode nominal
    - Avertissement des utilisateurs de la fin de maintenance / Mise à jour

L'évaluation se fait sur les cahiers de tests remplis.

Séquence P2.9 : Gestion de cycle de vie du parc (10h)

Séance 1 - Notions théoriques sur la gestion de parc (1h)

- Présentation de la gestion de parc
  - Intérêt, stratégies, outils
- Déploiement, images, protocoles PXE, TFTP
- Mises à jour, repos, scheduling, politiques de mise à jour
- Fin de vie, EOL, veille produit, etc...
- Gestion des assets avec GLPI et agents inventaire

Séance 2 - Installation d'une solution de déploiement FOG (4h)

- Installation FOG
- Paramétrage DHCP, NTP, PXE
- Préparation des images (masters)
- Déploiement de postes (windows / Linux)

Séance 3 - Gestion des mises à jour (2h)

- Point sécu sur l'importance des mises à jour
- Dépréciation WSUS, spécifier les implications
- mise en place des groupes, GPO de scheduling des mises à jours
- vérification du patching

Séance 4 - Inventaire GLPI (2h)

- Configuration de l'inventaire
- Installation des agents
- Vérification des données de l'inventaire
- Requêtes SQL custom pour savoir si le poste dispose des derniers correctifs

Évaluations - 1h

Séquence P2.10 : Supervision de parc (7h)

Séance 1 - Notions sur la supervision (2h)

- Interêt de la supervision et de l'alerting
- Protocole historique de la supervision (SNMP)
- WMI et CIM instances
- WINRM & powershell

Séance 2 - Installation Zabix (1h)

- Installation Zabix
- Paramétrage
- Mise en place authentification & permissions

Séance 3 - Déploiement des agents (1h)

- Déploiement des agents sur les endpoint
- Déploiement des sondes sur les équipements réseaux
- création GPO installation de l'agent OU déploiement dans l'image

Séance 4 - Création / peuplement des dashboards (2h)

- Création des différents dashboards
- ajout des ressources nécessaires
- Mise en production des dashboards
- mise en place des permissions

Évaluations - 1h

TP KALI 2 - Web exploitation avec WebGoat et DamnVulnerableWebApplication

> **Info** : A ce stade, l'on devrait avoir terminé l'année 1, la suite du programme IT est pour l'année 2.

Info: Pour la seconde année, l'intégralité du travail se fera en serveur core pour windows.

Conseil : Pour commencer l'année, procéder aux révisions de la première année en faisant reproduire l'infra de première année avec du windows core et du powershell.

III. Projet IT (2ème année)

Séquence P2.11 : Protocoles réseaux avancés pour l'automatisation et la redondance (8h)

Séance 1 - Le routage dynamique (3h)

- RIP + déréciation
- EIGRP
- OSPF
- TP mise en pratique sur les 3 protocoles

Séance 2 - Les protocoles de redondance (2h)

- STP / RSTP
- TP RSTP avec topologie en boucle puis full mesh (cicso paquet tracer)
- VRRP (keepalived sous ubuntu)

Séance 3 - Mise en application sur OPNsense (2h)

- mise en place de CARP et OPNSync

Évaluations - 1h

Séquence P2.12 : Sauvegardes et politiques associées (8h)

Séance 1 - théorie sur la sauvegarde et l'archivage (1h)

- Stratégie de PCA et de PRA
- Stratégies de sauyvegardes
- Rétention
- différence entre sauvegarde et archivage
- stratégies d'archivages
- Quelle stratégie pour quel besoin / contrainte légale (RGPD, impératif de conservation, etc...)
- hot storage vs cold storage

Séance 2 - mise en oeuvre (Veeam) (4h)

Séance 3 - mise en oeuvre (proxmox backup) (2h)

Évaluations - 1h

Séquence P2.13 : La connexion à distance avec le VPN (9h)

Séance 1 - VPN Client (openvpn) (4h)

- Fonctionnement openVPN
- Mise en oeuvre sur OPNsense (classique)
- Ajouter l'authentification LDAP

Séance 2 - VPN site à site avec IPSEC (4h)

- Fonctionnement IPsec
- Mise en oeuvre sur OPNsense
- sécurisation avec les règles de firewall
- moindre exposition sur les phases 2

Évaluations - 1h

Séquence P2.14 : une avancée dans la gestion de l'identité, le SSO (6h)

Séance 1 - principes et théories sur le SSO (5h)

- principaux protocoles, openID et SAML
- Mise en pratique avec ADFS

Évaluations - 1h

Séquence P2.15 : La cybersécurité moderne, le SOC (11h)

Séance 1 - Théorie autour du SOC et des outils (2h)

- Le SOC théorie et organisation
- Les outils du SOC
  - IDS / IPS
  - EDR / XRDR
  - SIEM
  - WAF

Séance 2 - Mise en place de l'IPS/IDS (2h)

- mise en oeuvre et tests de snort sur OPNsense
- construction et écriture de règles

Séance 3 - SIEM / EDR/XDR (3h)

- mise en oeuvre et installation de Wazuh
- déploiement des agents
- focus sur les dashboard et les processus de gestion des incidents de sécu

Séance 4 - le WAF (2h)

- Théorie sur le fonctionnement du WAF
- Rappel sur la structure des requêtes HTTP
- Mise en œuvre (solution à déterminer)
- tests et reporting

Séance 5 - Les outils de recherche de vulnerabilité (1h)

- présentation des outils
- création d'un stack OpenVAS

Évaluations - 1h

Séquence P2.16 : Autres besoins de l'usine connecté (30h)

Séance 1 - Services de messagerie (8h)

- Les principaux protocoles de messagerie
  - SMTP
  - POP / IMAP
  - les champs DNS associés (MX, SRV, DMARK, DKIM, ...)

- Les sécurités
  - antispam
  - normes de protections
  - phishing et campagnes de phishing
- Mise en oeuvre dun serveur de messagerie et de se protections

Séance 2 - Services de VoIP (8h)

- fondamentaux de la téléphonie --> évolution vers la voie sur IP
- les principaux protocoles VoIP (SIP, RTP, TFTP (rappel), H.323
- Les codecs
- Les SDA, le PABX / PBX
- Mise en place d'un serveur ASTERISK
- Mise en place d'une appliance ISSABEL

Séance 3 - Mise en oeuvre d'un VLAN Industriels & IoT (8h)

- les différents supports de communications et leur sécurisation
  - wifi
  - radio
  - gestion de la sécurité (authentification / radius / certificats)
- les principaux protocoles industriels (rappel modbus over ip / série, etc...)

Séance 4 - les protocoles réseaux d'optimisation (4h)

- théorie et mise en oeuvre de QoS et priorisation de flux
- théorie et mise en place du multicast
- paramétrage RSTP multivlan et priorisation des routes dans le trafic

Évaluations - 1h

IV. Projets Électronique année 1

Séquence P3.1 : Conception de la solution (6h)

Séance 1 - Etude de projet (2h)

- Etude du cahier des charge
- Prise en compte des moyens et contraintes
- Etude des flux : Badge → arduino → API → MariaDB

Séance 2 - Conception de la solution (4h)

- Bases théoriques sur la réalisation des diagrammes (UML/SYSML)
- Élaboration des diagrammes
  - Architecture réseau
  - Schéma électronique
  - Modèle de données

L'évaluation se fait sur la base d'une présentation orale appuyée sur les livrables attendus.

Séquence P3.2 : Prise en main arduino (5h)

Séance 1 - Arduino (1h)

- Prise de connaissance du matériel des kits arduino
- Initiation à l'IDE VScode avec l'extention arduino
- réalisation de programmes simples (C++, crosscompilation)

Séance 2 - Prise en main de GIT (1h)

- Prise en main de GIT
- Création des Token personnels
- Méthodologie de projet DEV/SEC/OPS
- Bonne pratiques sur le développement et la documentation.
  - Branches PROD / DEV / UAT
  - Documentation MARKDOWN

- Licence & propriété intellectuelle
- Commentaires

Séance 3 - Spécification technique de la solution (2h) Co-enseignement

- GPIO, interruptions, communication série
- Lecture NFC (RC522)
- Lecture clavier matriciel
- TP : lire un badge + afficher UID

Évaluations - 1h

Séquence P3.3 : Réseau & API (4h)

Séance 1 - Rappel réseau & introductions nouvelles notions (2h)

- Rappel TCP / IP
- Rappel HTTP
- apprentissage API REST et JSON
- Sécurité des API : Tokens, API Key, APP key, secrets

Séance 2 - Mise en place de l'API (1h)

- Création d’une API REST en Python/PHP
- Endpoints :
  - `/auth/badge`
  - `/auth/code`
  - `/sensors/push`
- Tests via Postman

Évaluations - 1h

Séquence P3.4 : Base de donnée & sécurité (8h)

Séance 1 - Modélisation de la BDD (4h)

- Théorie sur la modélsation de BDD (MCD, MRD, etc...)
- Modélisation des bases de données pour le projet (badges, accès, utilisateurs, logs, capteurs)
- Création de la BDD, insertion du jeu de donnée de base, jointures
- Dump et restauration

Séance 2 - Sécurisation (3h)

- Rappel hash, chiffrement, signatures
- Hash des mots de passe et validation de l’authentification.
- sécurisation de l'API (injection, actions non autorisées, ouverture, IP sources autorisées, etc...)
- gestion des droits SQL

Évaluations - 1h

Séquence P3.5 : Réalisation de la solution 1 (?h)

Séance 1 - Réalisation du système 1 - Contrôle d'accès (?h)

- Réaliser la solution Arduino + NFC + Clavier code + api + BDD + interface web
  - Lecture NFC / UID, Gestion des leds / Buzzer
  - Gestion des requêtes API
  - Lecture du code
  - Vérification API
  - Déclenchement servo. Relai Rack
  - Endpoint `/auth/badge`
  - `Endpoint `/auth/code`
  - Retour JSON : autorisé / refusé
- Réaliser la documentation (MARKDOWN GIT)
- Réaliser et remplir les cahiers de tests

Séance 2 - Réalisation du système 1 - Logs et dashboard (?h)

- Réaliser la solution de logging
  - UID
  - utilisateur
  - date/heure
  - porte ou rack (status / Horrodatage)
- Réaliser le dashboard
  - Tableau récapitulatif des accèss
  - Status portes (ouvert / Fermé)
  - Filtres et exports CSV

Séance 3 - Réalisation du système 1 - Interface d'administration (?h)

- CRUD badges
- CRUD utilisateurs
- Attribution badge
- Utilisateur

L'évaluation se fait sur les cahiers de tests remplis.

Séquence P3.6 : Tests de sécurité de la solution 1 (?h)

Séance 1 - Tests de sécurité

- Injection SQL
- Injection de code dans les API
- Bruteforce
- Accès non autorisé

L'évaluation se fait sur les rapport de pentest

III. Projets Électronique 2

Séquence P4.1 : Conception de la solution (6h)

Séance 1 - Etude de projet (2h)

- Etude du cahier des charge
- Prise en compte des moyens et contraintes
- Identification des flux IoT : capteurs → Raspberry Pi → base → Grafana

Séance 2 - Conception de la solution (4h)

- Élaboration des diagrammes
  - Architecture réseau
  - Schéma électronique
  - Modèle de données

L'évaluation se fait sur la base d'une présentation orale appuyée sur les livrables attendus.

Séquence P4.2 : Prise en main Rpi (6h)

Séance 1 - Arduino (1h)

- Prise de connaissance du matériel des kits raspberry PI
- Initiation au raspberry (Architecture ARM, OS, Python)
- réalisation de programmes simples

Séance 2 - Raspberry PI (4h) Co-enseignement

- GPIO, interruptions, communication série
- OS, services, Python, librairies capteurs

- Lecture et caractéristiques des capteurs
  - Température
  - Humidité
  - Luminosité
  - Niveau d’eau
  - Détecteur de présence

Évaluations - 1h

Séquence P4.3 : Réseau & API (2h)

Séance 1 - Mise en place de l'API (1h)

- Envoi données → API
- Stockage dans MariaDB

Évaluations - 1h

Séquence P4.4 : Base de donnée & sécurité (8h)

Séance 1 - Modélisation de la BDD (4h)

- Théorie sur la modélsation de BDD (MCD, MRD, etc...)
- Modélisation des bases de données pour le projet (badges, accès, utilisateurs, logs, capteurs)
- Création de la BDD, insertion du jeu de donnée de base, jointures
- Dump et restauration

Séance 2 - Sécurisation (3h)

- Rappel hash, chiffrement, signatures
- Hash des mots de passe et validation de l’authentification.

- sécurisation de l'API (injection, actions non autorisées, ouverture, IP sources autorisées, etc...)
- gestion des droits SQL

Évaluations - 1h

Séquence P4.5 : Réalisation de la solution 2 (?h)

Séance 1 - Réalisation du système 2 - Logs et dashboard (?h)

- Datasources
- Panels
- Alerting
- Dashboard
  - Courbes température / humidité
  - Indicateurs nid d’abeille (honeycomb)
  - Couleurs : vert → jaune → orange → rouge

Séance 2 - Fusion des dashboards 1 & 2 (?h)

- Fusion des dashboards
  - Dashboard unique
  - Logs accès + capteurs
  - Alertes combinées

Séance 3 - Documentation finale pour le 'client' (?h)

- Manuel utilisateur
  Manuel technique

L'évaluation se fait sur les cahiers de tests remplis et des livrables

Séquence P4.6 : Tests de sécurité de la solution 1 (?h)

Séance 1 - Tests de sécurité

- Injection SQL
- Injection de code dans les API
- Bruteforce
- Accès non autorisé

L'évaluation se fait sur les rapport de pentest

Revision #49
Created 2026-07-17 13:12:00 UTC by Olivier
Updated 2026-08-13 09:00:25 UTC by Olivier