Gestion centralisée de logs

CIEL_IR - Séquence Pédagogique 1

Description de la séquence

Niveau pédagogique → BTS CIEL_IR 1ère année

Thème de la séquence → Gestion Centralisée de logs

Positionnement → 1ère année de BTS de la rentrée de septembre à la Toussaint

Prérequis → Aucun

Contextualisation

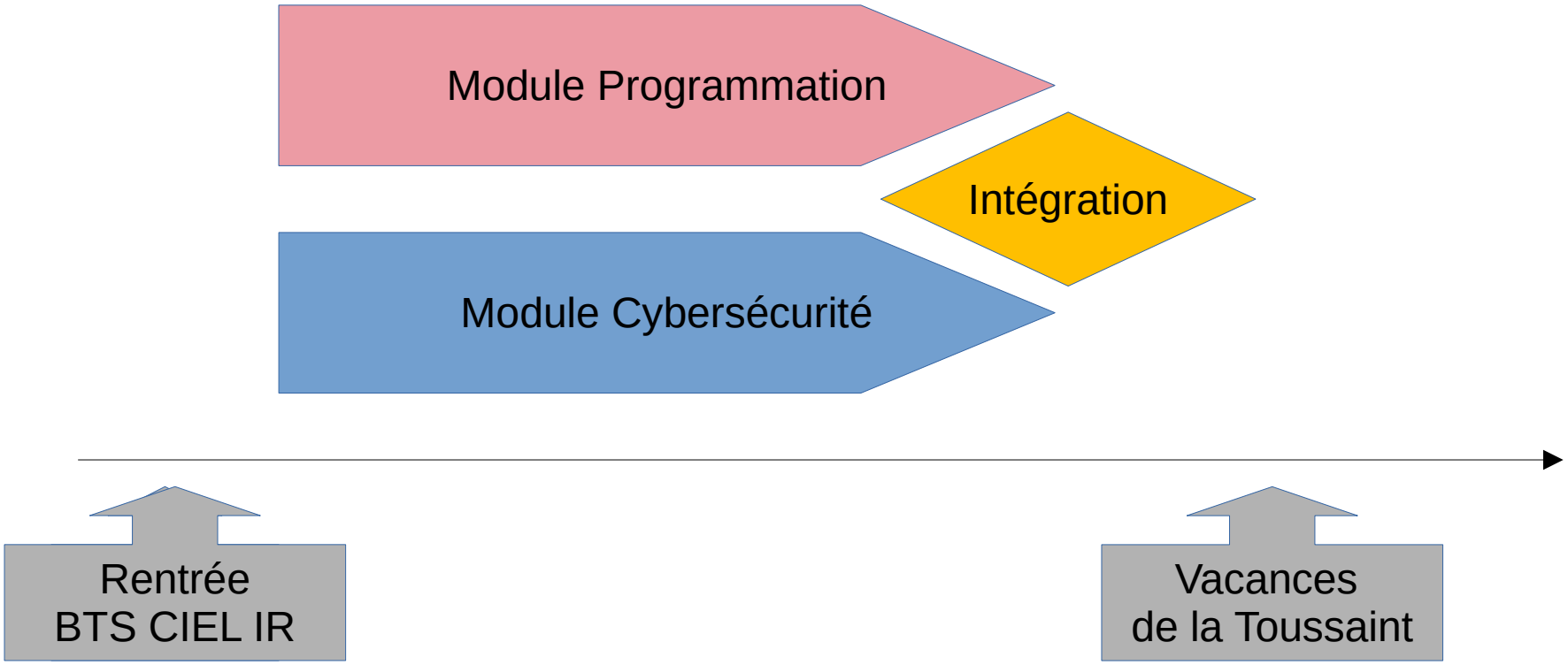
L'entreprise XYZ développe des solutions SAAS à ses clients

L'entreprise XYZ, de part son segment de marché, est exposée fortement au risque cyber

Volonté du RSSI

- Virtualiser le système d'information
- Mettre en place une politique stricte de sécurité basé sur la règle du moindre privilège ou « least privilege »
- Remporter l'adhésion des collaborateurs à la politique de sécurité
- Que chaque collaborateur prenne conscience des contraintes de sécurité

2 séquences en parallèles
1 thème commun



Module 1 - Programmation

Création d'une application Gestion Centralisée de logs

CIEL_IR - Séquence Pédagogique 1

Module 1 - Objectifs

- **Fondamentaux de la gestion de projet**
- **Fondamentaux de la programmation en langage C++**
- Bonnes pratiques du développement applicatif (documentation, programmation modulaire)
- Utilisation des outils de développement (IDE, DevOps)

Module 1 – Compétences et connaissances visées du référentiel

Compétence	Connaissance
C03 – Gérer un projet (U6)	• Méthode de conduite de projet (cycle en V) • Langage de modélisation UML/SysML • Outils de gestion de projet • Différents acteurs du projets
C06 – Valider un système informatique (U5)	• Tests unitaire et d'intégration • Fiche de recette
C08 – Coder (U6)	• Langages de développement, de description, de création d'API et les IDE associés • Outils de modélisation • Chaînes d'intégration et de déploiement

Module 1 - Organisation

Stratégie pédagogique

- A partir d'un cahier des charges et d'un dossier de conception, les étudiants vont dans une démarche de projet réaliser progressivement l'application demandée

Organisation

- Nombre étudiants 28 (14 étudiants en TP)
- Logiciel (PC sous linux, IDE QtCreator, Gitlab)

Volume horaire de la séquence

- 7 semaines de cours (1H/semaine)
- 7 semaines de TP (5 heures/semaine)

Module 1 – Documents et évaluation

Documents élèves

Projet Gestion Centralisée de logs

Cahier des charges, document de conception, planification du projet, document de validation, itérations successives.

Exercices

Exercices d'applications en libre accès sur notre plateforme documentaire

Cours

Les cours formaliseront les notions abordées dans les activités

Évaluations

Évaluation de chaque TP (livrable attendu, compte rendu de TP)

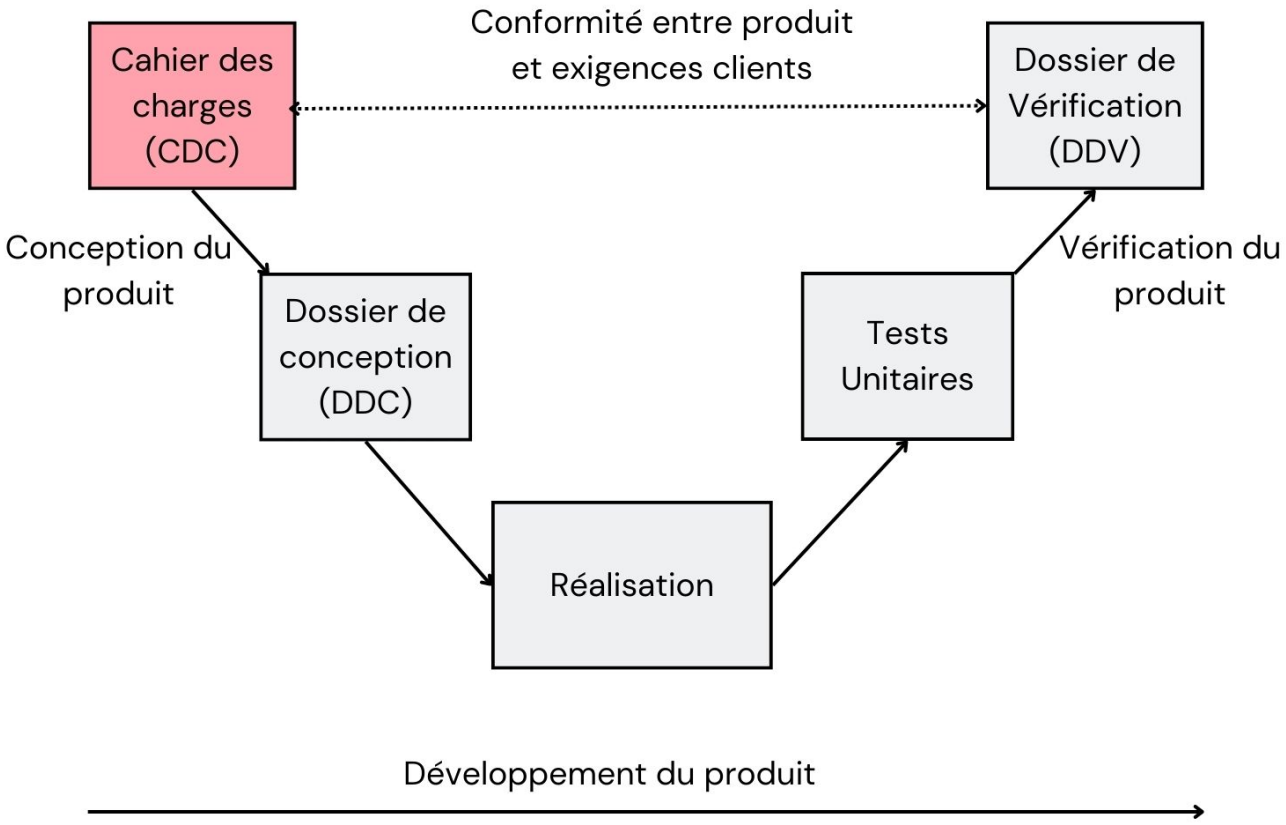
Évaluation hebdomadaire auto-formative (QCM)

Évaluation sommative des objectifs (Évaluation de TP, deux évaluations sur table)

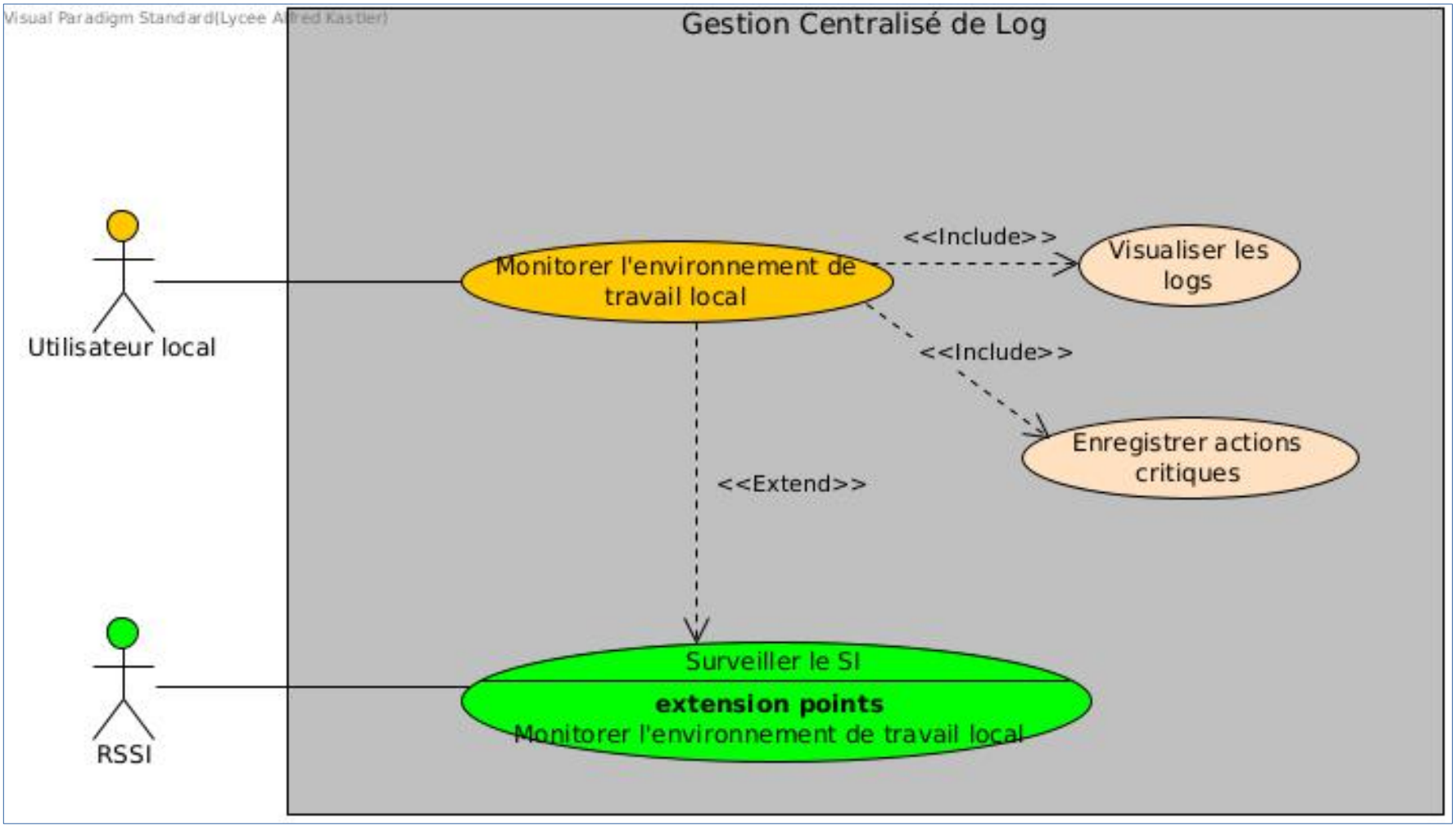
Module 1 – Déroulé de la séquence

Documents étudiant

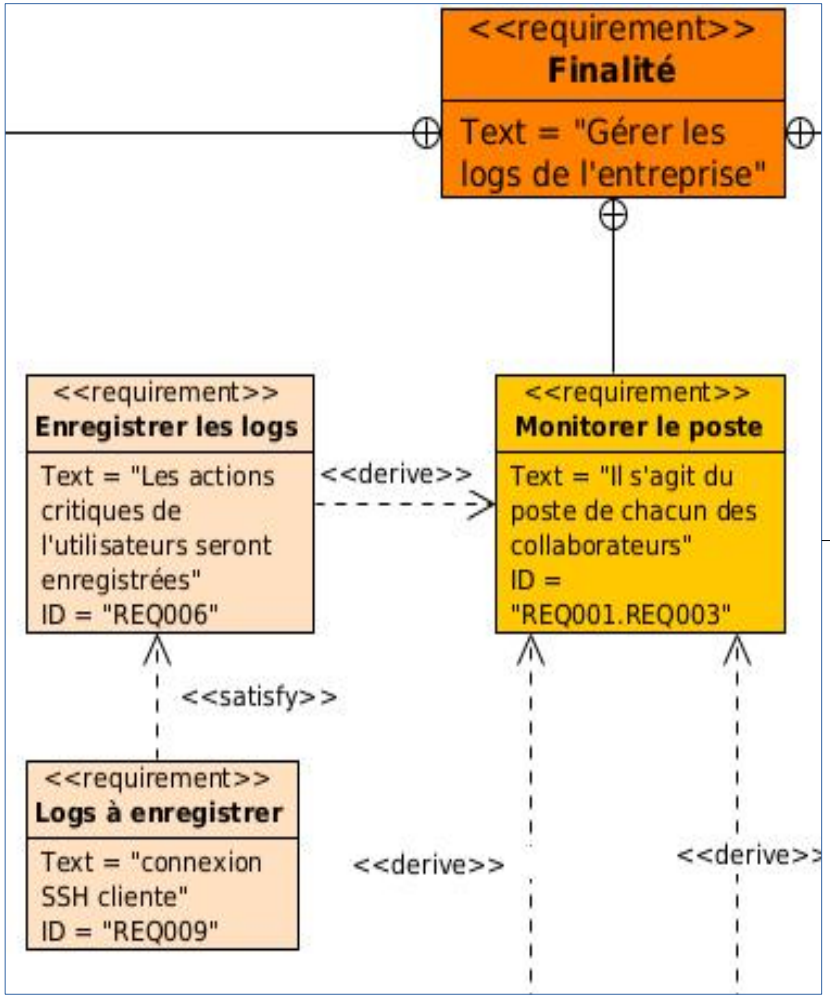
- Cahier des charges
- Dossier de conception
- Planning
- Dossier de vérification
- Site web section (prise en main des outils DevOps)



Module 1 – Cahier des charges



Module 1 – Extrait exigences et validation



2.3. Enregistrer les logs

Référence de l'essai : ESS03

Exigences client vérifiées : REQ006

But de l'essai : Vérifier que les connexion ssh clientes sont bien enregistrées dans le fichier logSSH.txt

Moyens utilisés :

- PC sous Linux, Application GCL

Procédure d'essai:

- Lancer GCL
- Sélectionner l'enregistrement de log SSH dans le menu
- Exécuter une commande dans un shell
- Exécuter une commande ssh user@srv dans un shell
- Exécuter une commande ssh user@srv -p port dans un shell

Résultats attendus :

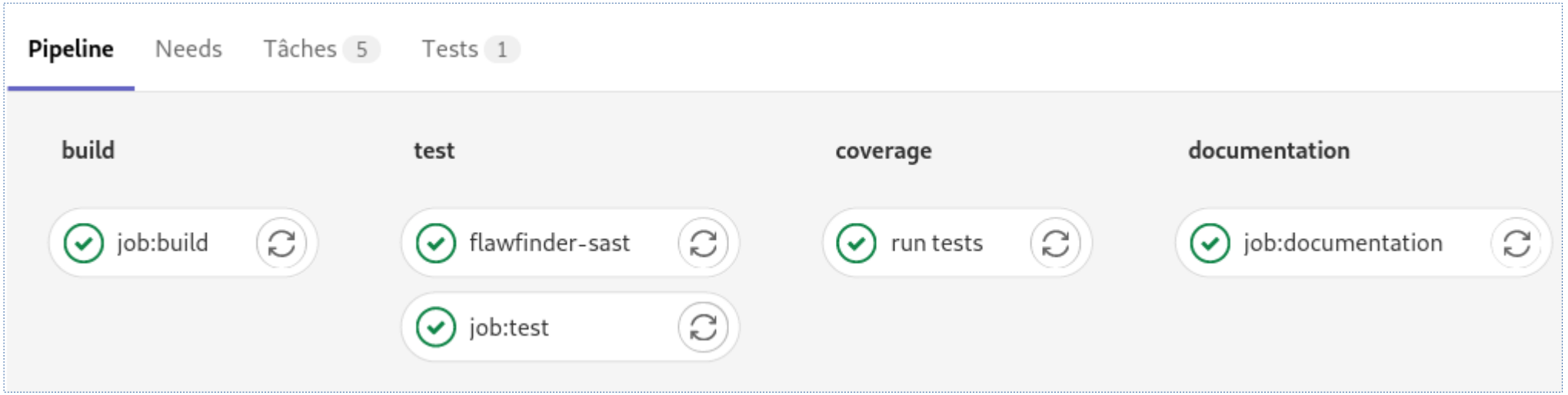
Etape	Valeur attendue	Tolérance
Les deux commandes ssh sont enregistrées dans le fichier	Structure SSH correctement remplies	NULLE

Statut de l'essai (conforme ou non conforme) :

Module 1 – Extrait fiche séquence

Réf. & Durée	Titre & Description
INFO 5h **Semaine 1 (Itération 1)**	**Création d'un menu (variable, cin, cout, if else)** ✔ Mise en œuvre de l'IDE ✔ Prise en main (1/2) des outils DevOps (git, Gitlab, pipeline CI, documentation) ✔ Connaissance des documents du projet
…	
INFO 5h **Semaine 3 (Itération 3)**	**Modularité de l'application (menu.h, menu.cpp)** ✔ Valider les exigences du CDC (ESS01, REQ014) → DevOps
…	
INFO 5h **Semaine 5 (Itération 5)**	**Création de sshLog()** ✔ Lire et extraire les informations depuis varlog/syslog ✔ Écrire les informations dans un fichier sshLog.txt ✔ Valider les exigences du CDC (ESS02, ESS03)
INFO 5h **Semaine 6 (Évaluation TP)**	**Évaluation de TP** ✔ Préparation 2h30 ✔ Évaluation 2h30
INFO 5h **Semaine 7 (Itération 6)**	**Envoi des informations sur le serveur centralisé** ✔ Coordination avec prof2 (SSH, srv web) ✔ Valider les exigences du CDC (ESS04)

Module 1 – Outils DevSecOps



- Versionning du code
- Compilation du code
- Tests Unitaires
- Test SAST (Static Analysis Security Testing)
- Coverage
- Documentation du code

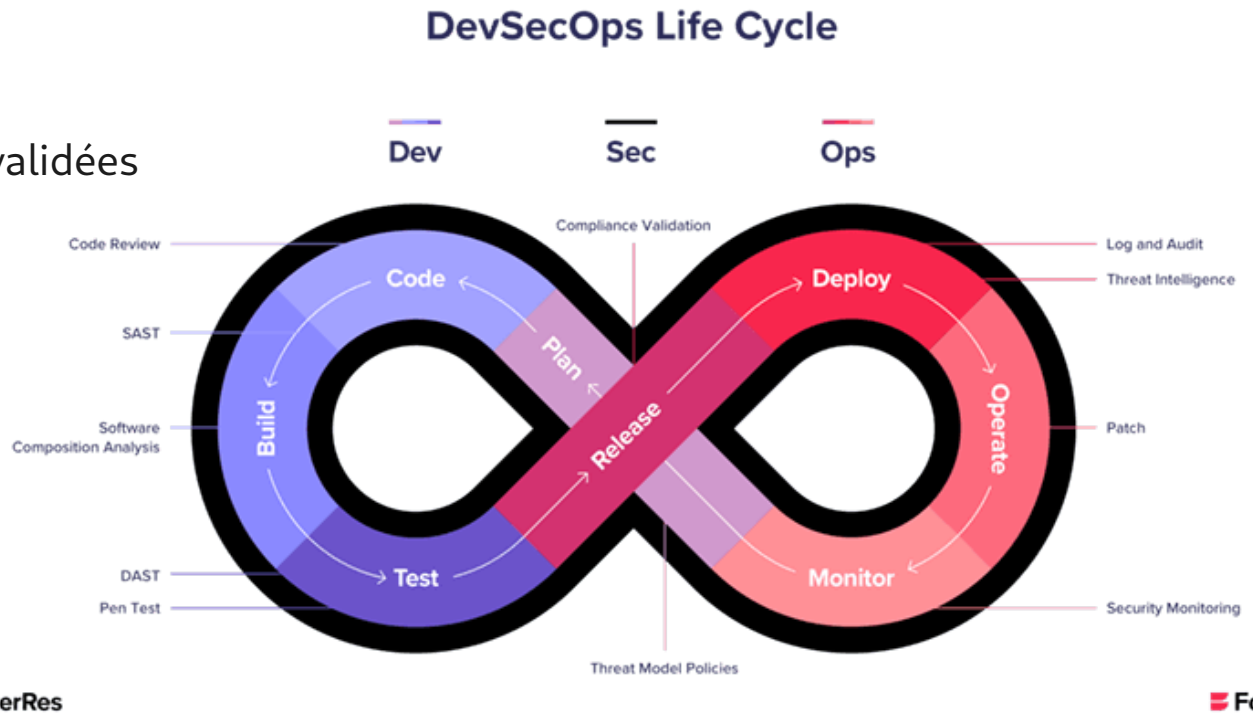
Module 1 – Responsabilités partagées

Enseignant

- Mettre en place les outils de développement
- Mettre en place les outils DevOps

Étudiants

- Responsabilité du code produit
- Vérifier la conformité du code
- S'assurer que les étapes DevOps sont validées



Module 1 - Conclusion

Évaluation

- Évaluation de chaque itération (livrable attendu, compte rendu de TP)
- Évaluation hebdomadaire auto-formative (QCM)
- Évaluation sommative des objectifs (Évaluation de TP, deux évaluations sur table)

Séquence préparé pour Eduscol

- Fiche de séquence et de séance
- Documents du projet (Cahier des charges, dossier de conception, séances étudiant, planning, dossier de validation)
- Programme C++ corrigé enseignant

Module 2 - Cybersécurité

Sécurisation SSH

CIEL_IR - Séquence Pédagogique 1

Module Cyber - Objectifs

- Rappel de la triade des problématiques de cybersécurité :

- Confidentialité
- Intégrité
- Disponibilité
- Traçabilité

Module Cyber - Compétences et connaissances visées

BTS CIEL ***Option A : Informatique et réseaux*** *(i) Étude et conception de réseaux informatiques* *(ii) Exploitation et maintenance de réseaux informatiques* *(iii) Valorisation de la donnée et cybersécurité*		C01 – COMMUNIQUER…	C02 – ORGANISER…	C03 – GÉRER UN PROJET	C04 – ANALYSER…	C05 – CONCEVOIR…	C06 – VALIDER…	C07 (non mobilisée)	C08 – CODER…	C09 – INSTALLER…	C10 – EXPLOITER…	C11 – MAINTENIR…
(i)	R1 : Accompagnement du client	X			X	X						
	R2 : Installation et qualification				X	X	X		X	X	X	
(ii)	R3 : Exploitation et maintien en condition opérationnelle		X				X		X	X	X	X
	R4 : Gestion de projet et d'équipe	X	X	X								
	R5 : Maintenance des réseaux informatiques		X		X		X			X	X	X
(iii)	D1 : Élaboration et appropriation d'un cahier des charges	X		X	X	X						
	D2 : Développement et validation de solutions logicielles					X	X		X			
	D3 : Gestion d'incidents	X			X						X	X
	D4 : Valorisation de la donnée			X	X				X			
	D5 : Audit de l'installation ou du système	X		X							X	
Unités certificatives :												
U4					X	X						
U5			X				X			X		X
U6		X		X					X		X	

Module Cyber – Compétences et connaissances visées

Compétence	Connaissance
C02 – Organiser (U5)	• Exploitation et maintien en conditions opérationnelle (2) • Différents acteurs du projet (2) • Contraintes en terme de sécurisation (2)
C06 – Valider un système informatique (U5)	• Réseaux informatiques (4) • Sécurisation des réseaux (3) • Tests unitaire et d'intégration (3) • Fiche de recette (3)
C09 – Installer (U5)	• SSH (4) • Système d'exploitation UNIX, virtualisation (3)

Module Cyber - Organisation

Stratégie pédagogique

- Une approche immersive et concrète dans le coeur d'une problématique de cybersécurité.
- Démarrer des modules déjà réalisés par les enseignants en BTS SN IR
- L'enseignant pourra bien sûr décider, selon son expérience et ses habitudes, de pousser l'apprentissage du réseau et du système Unix et décaler un peu la suite de la séquence cybersécurité.
- Intégrer la finalité de la triade (**Confidentialité, Intégrité, Disponibilité**) sur toutes les étapes.

Organisation

- Logiciel Tableur, VirtualBox, VM Debian Linux

Volume horaire indicatif de la séquence

- 7 semaines de cours (1H/semaine)
- 7 semaines de TP (5 heures/semaine)

Module Cyber - Objectifs

- Fondamentaux de réseau et système UNIX
- Fondamentaux de cryptoanalyse
- Etude détaillée du protocole SSH
- Démarche d'audit et de validation

Module Cyber – Déroulé de la séquence

Ces premiers modules sont des parties déjà existantes dans le BTS SN IR

Module 01 :

- Introduction au réseau, couches OSI, adressage IPv4

Module 02 :

- Installation simplifiée d'une VM sous Debian .

- Notion d'administration Unix (se déplacer et se repérer dans une arborescence, lire et éditer un fichier, gestion des droits Unix)

Module 03 : Droits POSIX

- Introduction aux droits POSIX

- Mise en pratique en contexte multi utilisateurs

Module 04 : Introduction Virtualisation et réseau

- Installation d'une VM Linux personnalisée **(avoir sa VM cliente)**

- Communication entre VM (VM serveur fournie)

Module Cyber – Déroulé de la séquence

Module 05: Cryptoanalyse et SSH

- **Notions de cryptographie** : clefs publiques, clefs privées
- **TP** Chiffrement symétrique et asymétrique
  Mise en place d'une authentification par clé

Module 06: Cybersécurité

- **La Triade : Confidentialité , Intégrité , Disponibilité**
- **TP** Tunnels SSH dynamique
  Vulnérabilité SSH Man in The Middle (VM d'attaque fournie)

Module 07: Démarche d'audit et de validation

- **Introduction à la méthodologie d'audit**
- **TP** Validation et mise en conformité de l'installation SSH

Selon le document officiel de l'ANSSI :
"Note technique de Recommandations pour un usage sécurisé d'(Open)SSH "

Module Cyber – Co-construction

Enseignant

- Intégrer et faire intégrer la triade (Confidentialité , Intégrité, Disponibilité) sur toutes les étapes
- Lancer les étudiants dans une démarche d'apprentissage des compétence d'analyse et de communication
- Gérer le cadre de mise en œuvre d'une vulnérabilité par les étudiants
- Réaliser ses premières évaluations U5

Étudiants

- Mettre en œuvre des règles d'hygiène informatique dès le début
- Installer sa VM de travail personnelle et construire son architecture
- Exercer un esprit critique et travailler la validation
- S'approprier la documentation de référence