Gestion centralisée de logs

Description de la séquence

Niveau pédagogique → **BTS CIEL IR 1ère année**

Thème de la séquence → **Gestion Centralisée de logs**

Positionnement → **BTS 1ère année - Semestre 1**

7 semaines de la rentrée de septembre à la Toussaint

Prérequis → **Aucun**

Contextualisation

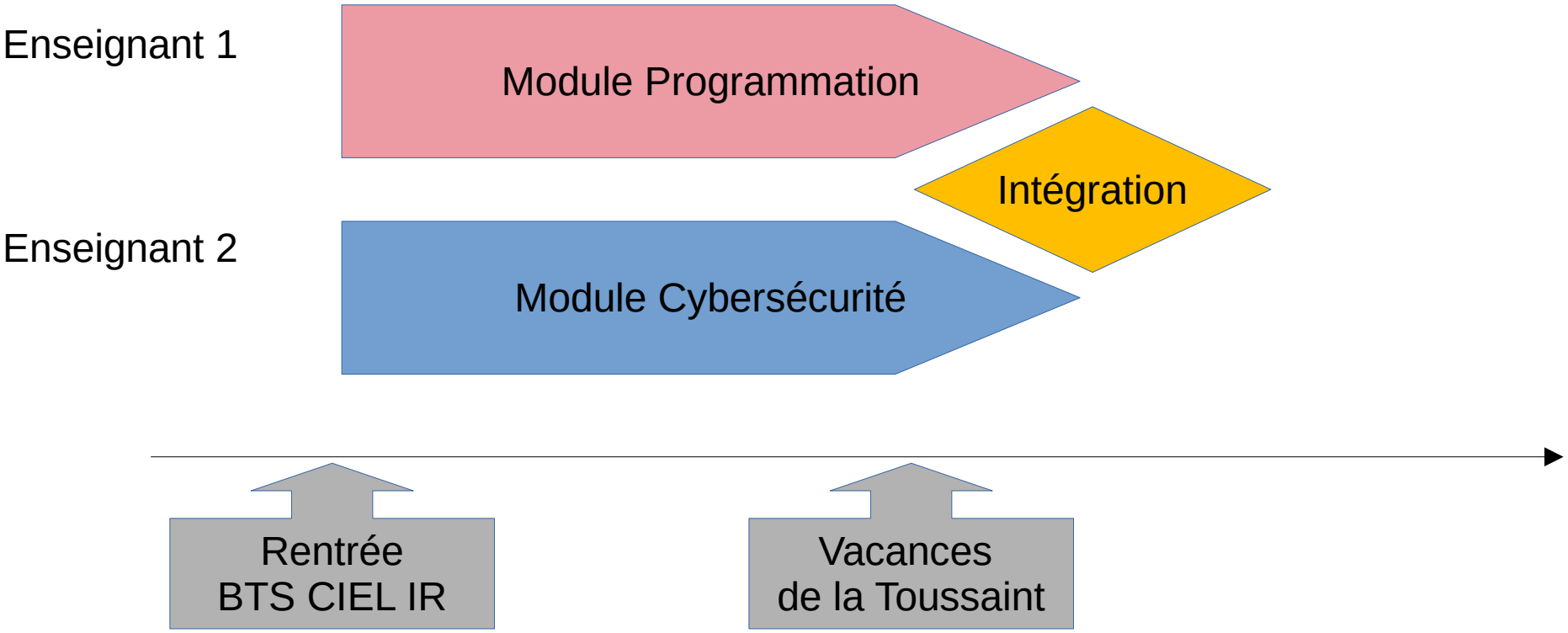
L’entreprise XYZ développe des solutions SAAS pour ses clients

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
- Sensibiliser et faire adhérer chaque collaborateur aux contraintes de sécurité

2 séquences en parallèle (pour 2 enseignants) 1 thème commun



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

- Poser que la cybersécurité n'est pas de l'intrusion mais que c'est établir un état normal de protection.
- Intégrer la finalité de la triade (**Confidentialité, Intégrité, Disponibilité**) sur toutes les étapes.
- 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.

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 – Documents et évaluation

Documents élèves

Fiches d'activités

Les élèves ont des consignes sous forme de fiche activité qui permettent d'avoir sous les yeux les commandes avec leurs options en attendant d'être autonomes dans les documentations techniques.

Exercices

Les travaux pratiques de MITM se font sur des machines virtuelles hors réseau Lycée.

Cours

Les cours formaliseront les notions abordées dans les activités

Évaluations

Évaluation de chaque TP (livrable attendu, compte rendu de TP) dans le cadre de U5

Évaluation sommative des objectifs dans le cadre de U5 (documents d'audit et de recette)

Evaluation formative dans le cadre de U6 pour les compétences communiquer et analyser.

Module Cyber – Déroulé de la séquence

Module 1 :

- Introduction au réseau, couches OSI, adressage IPv4

Module 2 :

- 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)

Ces deux premiers modules sont des parties déjà existantes dans le BTS SN IR , elles n’ont pas de spécificités CIEL

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 **(sécurisation VM serveur)**

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

Module Cyber - Evaluations

Évaluation

- Évaluation de chaque itération (livrables attendus)
- Évaluation hebdomadaire auto-formative (QCM)
- Évaluation sommative des objectifs (Documents d’audit/installation/recette)

U5 :

- **C02 Organiser**
- **C06 Valider**
- **C09 Installer**

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 compétences 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