INFRES_7_2_DL Architecture et Sécurité du Système d'information	INFRES	S7

Pourquoi cette UE ?

Ce module forme les élèves aux fondements de la sécurité des systèmes informatiques, en lien direct avec les pratiques DevOps. La cryptographie leur permet de comprendre les mécanismes de confidentialité et d'intégrité. La gestion des certificats leur donne les compétences pour sécuriser les communications et les accès. L'infrastructure as code complète l'approche en automatisant le déploiement d'environnements sécurisés, traçables et reproductibles. Ce module renforce l'autonomie et la rigueur des élèves face aux exigences de la production.

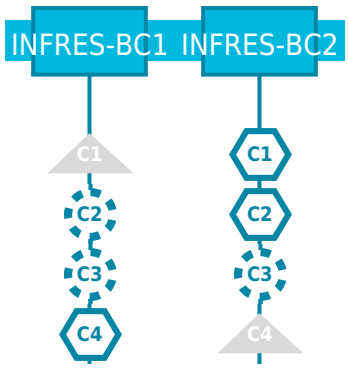
Eléménts constitutifs de l'UE

	coefficient
INFRES_7_2_DL-1 Sécurité applicative	1
INFRES_7_2_DL-2 Infrastructure as code	1

Volume d'heures d'enseignement encadré	Volume d'heures de travail personnel	Nombre d'ECTS
49	11	3

Alignement curriculaire

Parmi les compétences visées par la formation, lesquelles sont développées dans cette UE ?



INFRES_7_2_DL Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_DL-1 Sécurité applicative	**S7**

Contexte et enjeux de l'enseignement

Ce cours s’inscrit dans un univers numérique où les applications sont devenues la porte d’entrée privilégiée des cyberattaques. Avec la généralisation du web, du cloud et du mobile, elles manipulent des données sensibles et soutiennent des services critiques, ce qui en fait des cibles majeures. Les enjeux sont de montrer que la sécurité ne se limite pas aux infrastructures, mais doit être intégrée dès la conception logicielle (approche « security by design »). Le cours met en avant les principales vulnérabilités (injections, fuites de données, mauvaises gestions des accès), les bonnes pratiques de développement sécurisé et l’importance des tests réguliers. Il vise à sensibiliser à la responsabilité des concepteurs et développeurs dans la protection des utilisateurs et des organisations, et à poser les fondations pour des systèmes numériques fiables, robustes et conformes aux normes de sécurité.

Prise en compte des dimensions socio-environnementales

Prérequis

Utilisation basique du système Linux.

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	
Cours intégré (cours + TD)	17
TD	
TP	12
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	1
Travail personnel	11

Objectifs pédagogiques

(à la fin de cet enseignement, l'étudiant sera capable de ...)

Etre capable d’écrire un code sécurisé

Activités

(CM, TD, TP, projet, sortie terrain, etc.)

Le cours est constitué de 28 heures de cours en salle machine, et d’une étude de cas de 2 heures.
Chaque point abordé sur le plan théorique est mis en pratique par les apprentis, individuellement ou par binômes.

Évaluations et retours faits aux élèves

(évaluations qui comptent pour la note ou qui permettent à l'étudiant de se situer, corrigés, feedback personnalisé...)

Evaluation : Etude de cas de 2h
Retour sur l’évaluation fait à l’élève : Copies corrigées consultables sur demande

INFRES_7_2_DL Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_DL-1 Sécurité applicative	**S7**

Plan de cours

- Introduction
- Définitions importantes
- Études de cas
- Quelques types d’attaques et défaillances connues
- Contres mesures | Mitigations et Techniques de programmation

Ressources et références

Deprecated: htmlspecialchars(): Passing null to parameter #1 ($string) of type string is deprecated in **C:\Developpement\syllabus\public_html\views\syllabus_template.php** on line **297**

INFRES_7_2_DL Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_DL-2 Infrastructure as code	**S7**

Contexte et enjeux de l'enseignement

L’infrastructure as code (IaC) transforme la gestion des systèmes d’information en la rendant programmable, reproductible et versionnable. Dans un contexte d’automatisation croissante des déploiements, les infrastructures doivent être définies, modifiées et déployées de manière fiable, rapide et sécurisée. IaC permet de réduire les erreurs humaines, d’assurer la cohérence entre environnements et de favoriser l’agilité des équipes techniques. Cet enseignement vise à doter l’élève ingénieur des fondements méthodologiques et techniques nécessaires pour concevoir, maintenir et sécuriser des infrastructures automatisées, au service de systèmes complexes et distribués.

Prise en compte des dimensions socio-environnementales

ODD9 - Industrie, innovation et infrastructure

Prérequis

Containérisation

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	
Cours intégré (cours + TD)	10
TD	
TP	9
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	
Travail personnel	

Objectifs pédagogiques

(à la fin de cet enseignement, l'étudiant sera capable de ...)

- configurer un parc de machines virtuelles à l’aide de l’outil Ansible,
- Assimiler les notions fondamentales de cet outil : control host, targets, commandes ad hoc, modules Ansible, idempotence, playbooks, facts, rôles, etc.

Activités

(CM, TD, TP, projet, sortie terrain, etc.)

- TD : 6 séances de 3h30
- Installation d’un cluster de machines virtuelles
- Exposé théorique des notions
- Nombreux ateliers pratiques pour l’assimilation par la pratique
- Exercices pour chacune des notions

Évaluations et retours faits aux élèves

(évaluations qui comptent pour la note ou qui permettent à l'étudiant de se situer, corrigés, feedback personnalisé...)

Exercices en cours (contrôle continu)

INFRES_7_2_DL Architecture et Sécurité du Système d'information	INFRES
INFRES_7_2_DL-2 Infrastructure as code	**S7**

Plan de cours

Ressources et références

https://blog.microlinux.fr/formation-ansible/