

Pourquoi cette UE ?

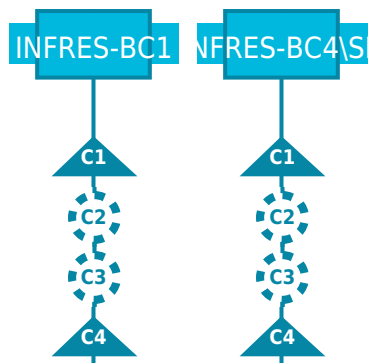
Ce module combine trois dimensions clés des systèmes actuels : le cloud, pour comprendre les nouveaux modèles de déploiement et de gestion des ressources ; l'automatisation réseau, pour assurer agilité et fiabilité ; et le forensics, pour analyser et répondre aux incidents. Ensemble, ils donnent aux élèves une vision complète : concevoir, administrer et sécuriser des infrastructures modernes tout en sachant investiguer en cas d'attaque.

Éléments constitutifs de l'UE

		coefficient
INFRES_9_5_SR-1 Solutions Clouds		2
INFRES_9_5_SR-2 Automatisation systèmes et réseaux		3
INFRES_9_5_SR-3 Forensics et preuves numériques		2
Volume d'heures d'enseignement encadré	Volume d'heures de travail personnel	Nombre d'ECTS
66	10	3

Alignement curriculaire

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



BC1	L'UE ne contribue pas à ce bloc de compétences
BC1	L'UE contribue à ce bloc de compétences
C1	Compétence non adressée dans cette UE
C1	Compétence mise en œuvre dans cette UE
C1	Compétence enseignée dans cette UE
C1	Compétence évaluée dans cette UE
C1	Compétence enseignée et évaluée dans cette UE

INFRES_9_5_SR Architecture et Sécurité du Système d'information	INFRES
INFRES_9_5_SR-1 Solutions Clouds	S9

Contexte et enjeux de l'enseignement

Les solutions cloud publiques transforment en profondeur l'architecture et la gestion des systèmes d'information. Elles permettent l'accès à des ressources informatiques à la demande, en optimisant la scalabilité, la résilience et les coûts. Dans un contexte industriel en mutation rapide, la maîtrise des offres cloud (IaaS, PaaS, SaaS) devient un atout stratégique pour les ingénieurs. L'adoption du cloud pose néanmoins des défis en matière de souveraineté, de sécurité, de portabilité des données et de gouvernance. Cet enseignement vise à donner aux élèves les clés pour comprendre, évaluer et intégrer les solutions cloud publiques dans des contextes professionnels complexes.

Prise en compte des dimensions socio-environnementales

ODD9 - Industrie, innovation et infrastructure

Prérequis

Infrastructure As Code Containérisation

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	
Cours intégré (cours + TD)	11
TD	
TP	8
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	1
Travail personnel	

Objectifs pédagogiques

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

- Expliquer les principes fondamentaux des architectures cloud publiques.
- Comparer les offres des principaux fournisseurs de services cloud.
- Déployer une infrastructure simple sur un cloud public.
- Appliquer les bonnes pratiques de sécurité et de conformité.
- Évaluer les coûts et la performance d'une solution cloud.

Activités

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

Cours
TP sur Microsoft Azure

Évaluations et retours faits aux élèves

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

QCM
TP évalué

INFRES_9_5_SR Architecture et Sécurité du Système d'information	INFRES
INFRES_9_5_SR-1 Solutions Clouds	S9

Plan de cours

- Introduction aux solutions cloud publiques : définitions, modèles de services (IaaS, PaaS, SaaS), modèles de déploiement (public, privé, hybride), évolutions du cloud computing, positionnement des grands acteurs (AWS, Azure, GCP).
- Fondamentaux techniques et architecture : virtualisation, conteneurisation, orchestration, stockage distribué, réseaux virtuels, scalabilité automatique, résilience.
- Mise en œuvre d’une infrastructure cloud : déploiement de machines virtuelles, configuration réseau, stockage persistant, supervision, introduction à l’infrastructure as code (Terraform, CloudFormation).
- Sécurité, conformité et gouvernance : gestion des identités et des accès (IAM), chiffrement, journalisation, politiques de sécurité, certifications, conformité réglementaire (RGPD, ISO 27001).
- Optimisation, coûts et perspectives : modèles de tarification, gestion budgétaire, outils de surveillance des coûts, éco-conception numérique, perspectives d’évolution (serverless, edge computing, IA dans le cloud).

Ressources et références

Support de cours disponible sur Campus.

INFRES_9_5_SR Architecture et Sécurité du Système d'information	INFRES
INFRES_9_5_SR-2 Automatisation systèmes et réseaux	S9

Contexte et enjeux de l'enseignement

L'automatisation des réseaux est devenue un pilier stratégique pour répondre aux exigences de scalabilité, de fiabilité et de sécurité des infrastructures modernes. Face à la complexité croissante des architectures, les solutions manuelles sont inadaptées, sources d'erreurs et coûteuses en temps. L'automatisation permet d'orchestrer dynamiquement la configuration, la supervision et la correction d'incidents. Elle repose sur des outils, des protocoles et des langages standardisés (API, modèles de données, scripts) qui favorisent l'agilité opérationnelle et la cohérence à grande échelle. Cet enseignement vise à doter les élèves d'une compréhension approfondie de ces mécanismes et des compétences pratiques pour les mettre en œuvre dans un cadre industriel.

Prise en compte des dimensions socio-environnementales

ODD9 - Industrie, innovation et infrastructure

Prérequis

Infrastructure As Code Containérisation

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	
Cours intégré (cours + TD)	21
TD	
TP	
Projets	8
Travail en autonomie encadré	
Contrôles et soutenances	1
Travail personnel	10

Objectifs pédagogiques	Activités	Évaluations et retours faits aux élèves
<p>(à la fin de cet enseignement, l'étudiant sera capable de ...)</p> <ul style="list-style-type: none"> - Expliquer les enjeux et principes de l’automatisation réseau. - Concevoir des scripts pour automatiser des tâches réseau. - Manipuler des API réseau et des outils d’orchestration. - Déployer une infrastructure réseau automatisée. - Diagnostiquer et corriger des défaillances dans un système automatisé. 	<p>(CM, TD, TP, projet, sortie terrain, etc.)</p> <p>Cours TP de mise en place d'une infrastructure automatisée</p>	<p>(évaluations qui comptent pour la note ou qui permettent à l'étudiant de se situer, corrigés, feedback personnalisé...)</p> <p>QCM TP évalué</p>

INFRES_9_5_SR Architecture et Sécurité du Système d'information	INFRES
INFRES_9_5_SR-2 Automatisation systèmes et réseaux	S9

Plan de cours

- Introduction à l'automatisation des réseaux : Définitions, enjeux économiques et techniques, limites de la gestion manuelle. Panorama des cas d'usage et évolution du rôle des ingénieurs réseau dans les architectures modernes.
- Outils et langages de l'automatisation : Présentation de Python pour le scripting réseau, utilisation de Netmiko, NAPALM, Ansible, YANG, JSON, RESTCONF. Construction d'un environnement de test reproductible.
- Modélisation et interfaces programmables : Structures de données pour la description des configurations (YAML, JSON), API REST, gRPC, interfaces SDN. Méthodes pour l'interrogation et la modification dynamique des équipements.
- Automatisation du cycle de vie des infrastructures : Provisioning, déploiement, supervision, reconfiguration automatique, gestion des erreurs. Scénarios d'automatisation avec Ansible et Terraform.
- Atelier projet et études de cas : Mise en œuvre complète d'une infrastructure automatisée sur simulateur ou équipement réel. Analyse de scénarios de défaillance, résilience, sécurité, auditabilité des configurations.

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_9_5_SR Architecture et Sécurité du Système d'information	INFRES
INFRES_9_5_SR-3 Forensics et preuves numériques	S9

Contexte et enjeux de l'enseignement

Ce cours s'inscrit dans un contexte de multiplication des cyberattaques, de la cybercriminalité et des obligations légales en matière de protection et de traçabilité des données. Il vise à former les élèves aux méthodes d'investigation numérique permettant d'identifier, collecter, analyser et préserver des preuves exploitables devant un tribunal ou dans un cadre disciplinaire. Les enjeux sont doubles : techniques, avec la maîtrise d'outils et de procédures garantissant l'intégrité et la fiabilité des éléments collectés ; et juridiques, avec la compréhension des normes et règles encadrant l'admissibilité des preuves. Ce cours contribue à développer une posture rigoureuse face aux incidents de sécurité, en préparant les élèves à agir efficacement lors d'enquêtes, tout en respectant les contraintes légales et éthiques.

Prise en compte des dimensions socio-environnementales



Prérequis

Cours de sécurité des réseaux Cours de droit informatique
Cours Ethical Hacking

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	
Cours intégré (cours + TD)	15
TD	
TP	
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	1
Travail personnel	

Objectifs pédagogiques

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

- Comprendre les principes du forensics et de la preuve numérique
- Apprendre à identifier, collecter et préserver des preuves sans altération
- Maîtriser les outils et méthodes d'analyse d'incidents
- Connaître le cadre légal et les règles d'admissibilité des preuves
- Développer une rigueur méthodologique et éthique dans les investigations

Activités

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

Cours
TP

Évaluations et retours faits aux élèves

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

TP évalué
QCM

INFRES_9_5_SR Architecture et Sécurité du Système d'information	INFRES
INFRES_9_5_SR-3 Forensics et preuves numériques	S9

Plan de cours

- Introduction au forensics et à la preuve numérique
- Définitions, enjeux et domaines d'application
- Typologie des incidents et rôle des enquêtes numériques
- Cadre légal et éthique
- Principes juridiques encadrant la collecte de preuves
- Règles d'admissibilité et respect de la vie privée
- Responsabilités de l'enquêteur numérique
- Méthodologie d'investigation
- Chaîne de conservation (chain of custody)
- Processus : identification, collecte, préservation, analyse, présentation
- Acquisition et préservation des preuves
- Outils et techniques de copie forensique (imagerie disque, mémoire, réseaux)
- Gestion des supports physiques et virtuels
- Documentation et traçabilité des opérations
- Analyse des systèmes et des données
- Analyse des systèmes de fichiers, logs et métadonnées
- Investigation mémoire et réseau
- Détection de traces de compromission et de malwares
- Rédaction et présentation des résultats
- Structurer un rapport clair, précis et exploitable juridiquement
- Présentation orale des conclusions dans un contexte d'enquête
- Études de cas et mises en pratique

Ressources et références

Support de cours disponible sur Campus.