



Annexe 22

Licence professionnelle « Bachelor Universitaire de Technologie »

RÉSEAUX ET TÉLÉCOMMUNICATIONS

Parcours :

- Cybersécurité
- Développement système et cloud
- Internet des objets et mobilité
- Pilotage de projets de réseaux
- Réseaux Opérateurs et Multimédia

Programme national

Sommaire

I. La formation B.U.T. Réseaux et Télécommunications et ses parcours	11
1. Objectifs de la formation	12
1.1. Le parcours : Cybersécurité	12
1.2. Le parcours : Développement système et cloud	13
1.3. Le parcours : Internet des objets et mobilité	13
1.4. Le parcours : Pilotage de projets de réseaux	13
1.5. Le parcours : Réseaux Opérateurs et Multimédia	13
II. Référentiel de compétences	15
1. Parcours : Cybersécurité	16
2. Parcours : Développement système et cloud	25
3. Parcours : Internet des objets et mobilité	34
4. Parcours : Pilotage de projets de réseaux	43
5. Parcours : Réseaux Opérateurs et Multimédia	52
III. Référentiel de formation	61
1. Cadre général	62
1. L'alternance	62
2. Les situations d'apprentissage et d'évaluation (SAÉ)	62
3. La démarche portfolio	62
4. Le projet personnel et professionnel	63
2. Structure générale des six semestres de formation	64
3. Référentiel de la première année du B.U.T. commun à tous les parcours	66
1. Semestre 1	66
1.1. Tableau croisé	66
1.2. Fiches Situations d'apprentissage et d'évaluation (SAÉ)	68
1.2.1. SAÉ 1.01 : Se sensibiliser à l'hygiène informatique et à la cybersécurité	68
1.2.2. SAÉ 1.02 : S'initier aux réseaux informatiques	69
1.2.3. SAÉ 1.03 : Découvrir un dispositif de transmission	70
1.2.4. SAÉ 1.04 : Se présenter sur Internet	71
1.2.5. SAÉ 1.05 : Traiter des données	72
1.2.6. PORTFOLIO : Démarche portfolio	73
1.3. Fiches Ressources	74
1.3.1. Ressource R1.01 : Initiation aux réseaux informatiques	74
1.3.2. Ressource R1.02 : Principes et architecture des réseaux	75
1.3.3. Ressource R1.03 : Réseaux locaux et équipements actifs	76
1.3.4. Ressource R1.04 : Fondamentaux des systèmes électroniques	77
1.3.5. Ressource R1.05 : Supports de transmission pour les réseaux	78
1.3.6. Ressource R1.06 : Architecture des systèmes numériques et informatiques	79
1.3.7. Ressource R1.07 : Fondamentaux de la programmation	80

1.3.8.	Ressource R1.08 : Bases des systèmes d'exploitation	81
1.3.9.	Ressource R1.09 : Introduction aux technologies Web	82
1.3.10.	Ressource R1.10 : Anglais technique 1	83
1.3.11.	Ressource R1.11 : Expression-Culture-Communication Professionnelles : Introduction à la communication et au savoir-être professionnels	84
1.3.12.	Ressource R1.12 : Projet Personnel et Professionnel	86
1.3.13.	Ressource R1.13 : Mathématiques du signal	88
1.3.14.	Ressource R1.14 : Mathématiques des transmissions	89
1.3.15.	Ressource R1.15 : Gestion de projet 1 : Maîtriser les bases de l'organisation du travail	90
2.	Semestre 2	91
2.1.	Tableau croisé	91
2.2.	Fiches Situations d'apprentissage et d'évaluation (SAÉ)	93
2.2.1.	SAÉ 2.01 : Construire un réseau informatique pour une petite structure	93
2.2.2.	SAÉ 2.02 : Mesurer et caractériser un signal ou un système	94
2.2.3.	SAÉ 2.03 : Mettre en place une solution informatique pour l'entreprise	95
2.2.4.	SAÉ 2.04 : Projet intégratif	96
2.2.5.	PORTFOLIO : Démarche portfolio	98
2.3.	Fiches Ressources	99
2.3.1.	Ressource R2.01 : Technologies de l'Internet	99
2.3.2.	Ressource R2.02 : Administration système et fondamentaux de la virtualisation	100
2.3.3.	Ressource R2.03 : Bases des services réseaux	101
2.3.4.	Ressource R2.04 : Initiation à la téléphonie d'entreprise	102
2.3.5.	Ressource R2.05 : Signaux et Systèmes pour les transmissions	103
2.3.6.	Ressource R2.06 : Numérisation de l'information	104
2.3.7.	Ressource R2.07 : Sources de données	105
2.3.8.	Ressource R2.08 : Analyse et traitement de données structurées	106
2.3.9.	Ressource R2.09 : Initiation au développement Web	107
2.3.10.	Ressource R2.10 : Anglais technique 2	108
2.3.11.	Ressource R2.11 : Expression-Culture-Communication Professionnelles : Renforcement des techniques de communication	109
2.3.12.	Ressource R2.12 : Projet Personnel et Professionnel	111
2.3.13.	Ressource R2.13 : Mathématiques des systèmes numériques	113
2.3.14.	Ressource R2.14 : Analyse des signaux	114
4.	Parcours : Cybersécurité	115
1.	Semestre 3	115
1.1.	Tableau croisé	115
1.2.	Fiches Situations d'apprentissage et d'évaluation (SAÉ)	117
1.2.1.	SAÉ 3.01 : Mettre en oeuvre un système de transmission	117
1.2.2.	SAÉ 3.02 : Développer des applications communicantes	118
1.2.3.	SAÉ 3.Cyber.03 : Concevoir un réseau informatique sécurisé multi-sites	119
1.2.4.	SAÉ 3.Cyber.04 : Découvrir le pentesting	121
1.2.5.	PORTFOLIO : Démarche portfolio	122
1.3.	Fiches Ressources	123
1.3.1.	Ressource R3.01 : Réseaux de campus	123
1.3.2.	Ressource R3.02 : Réseaux opérateurs	124
1.3.3.	Ressource R3.03 : Services réseaux avancés	125
1.3.4.	Ressource R3.04 : Services d'annuaires	126
1.3.5.	Ressource R3.05 : Chaînes de transmissions numériques	127
1.3.6.	Ressource R3.06 : Fibres optiques et propagation	128
1.3.7.	Ressource R3.07 : Réseaux d'accès	129
1.3.8.	Ressource R3.08 : Consolidation de la programmation	130
1.3.9.	Ressource R3.09 : Programmation événementielle	131
1.3.10.	Ressource R3.10 : Gestion d'un système de bases de données	132
1.3.11.	Ressource R3.11 : Anglais professionnel 1	133
1.3.12.	Ressource R3.12 : Expression-Culture-Communication professionnelles : Savoir collaborer	134
1.3.13.	Ressource R3.13 : Projet Personnel et Professionnel	135

1.3.14.	Ressource R3.14 : Analyse de Fourier	137
1.3.15.	Ressource R3.15 : Gestion de projet 2 : Utiliser les méthodes de gestion de projet	138
1.3.16.	Ressource R3.Cyber.16 : Méthodologie du pentesting	139
2.	Semestre 4	140
2.1.	Tableau croisé	140
2.2.	Fiches Situations d'apprentissage et d'évaluation (SAÉ)	142
2.2.1.	SAÉ 4.Cyber.01 : Sécuriser un système d'information	142
2.2.2.	STAGE.Cyber : Stage	143
2.2.3.	PORTFOLIO : Démarche portfolio	145
2.3.	Fiches Ressources	146
2.3.1.	Ressource R4.01 : Infrastructures de sécurité	146
2.3.2.	Ressource R4.02 : Transmissions avancées	147
2.3.3.	Ressource R4.03 : Physique des télécoms	148
2.3.4.	Ressource R4.04 : Réseaux cellulaires	149
2.3.5.	Ressource R4.05 : Automatisation des tâches d'administration	150
2.3.6.	Ressource R4.06 : Anglais professionnel 2	151
2.3.7.	Ressource R4.07 : Expression-Culture-Communication professionnelles : Préparer l'insertion professionnelle	152
2.3.8.	Ressource R4.08 : Projet Personnel et Professionnel	153
2.3.9.	Ressource R4.Cyber.09 : Sécurité des réseaux LAN	155
2.3.10.	Ressource R4.Cyber.10 : Cryptographie	156
2.3.11.	Ressource R4.Cyber.11 : Sécurisation de services réseaux	157
3.	Semestre 5	158
3.1.	Tableau croisé	158
3.2.	Fiches Situations d'apprentissage et d'évaluation (SAÉ)	160
3.2.1.	SAÉ 5.01 : Concevoir, réaliser et présenter une solution technique	160
3.2.2.	SAÉ 5.02 : Piloter un projet informatique	162
3.2.3.	SAÉ 5.Cyber.03 : Assurer la sécurisation et la supervision avancées d'un système d'information	164
3.2.4.	PORTFOLIO : Démarche portfolio	165
3.3.	Fiches Ressources	166
3.3.1.	Ressource R5.01 : WiFi avancé	166
3.3.2.	Ressource R5.02 : Supervision des réseaux	167
3.3.3.	Ressource R5.03 : Ingénierie de systèmes télécoms	168
3.3.4.	Ressource R5.04 : Cycle de vie d'un projet informatique	169
3.3.5.	Ressource R5.05 : Anglais : Insertion professionnelle 1	171
3.3.6.	Ressource R5.06 : Expression-Culture-Communication professionnelles : S'intégrer dans une organisation	172
3.3.7.	Ressource R5.07 : Projet Personnel et Professionnel	173
3.3.8.	Ressource R5.08 : Gestion de projets 3 : Mener un projet professionnel	175
3.3.9.	Ressource R5.Cyber.09 : Architectures sécurisées	177
3.3.10.	Ressource R5.Cyber.10 : Audits de sécurité	178
3.3.11.	Ressource R5.Cyber.11 : Supervision de la sécurité	179
3.3.12.	Ressource R5.Cyber.12 : Normes, standards et analyse de risques	180
4.	Semestre 6	181
4.1.	Tableau croisé	181
4.2.	Fiches Situations d'apprentissage et d'évaluation (SAÉ)	183
4.2.1.	SAÉ 6.Cyber.01 : Réagir face à une cyber-attaque	183
4.2.2.	STAGE.Cyber : Stage	184
4.2.3.	PORTFOLIO : Démarche portfolio	186
4.3.	Fiches Ressources	187
4.3.1.	Ressource R6.01 : Anglais : Insertion professionnelle 2	187
4.3.2.	Ressource R6.02 : Expression-Culture-Communication professionnelles : Communiquer en tant que futur cadre intermédiaire	188
4.3.3.	Ressource R6.03 : Connaissance de l'entreprise	189
4.3.4.	Ressource R6.Cyber.04 : Réponse à incident	190
5. Parcours : Développement système et cloud		191

Première partie

La formation B.U.T. Réseaux et Télécommunications et ses parcours

Ce document présente le programme national du B.U.T. Réseaux et Télécommunications et complète l'annexe 1 de l'arrêté relatif aux programmes nationaux de la licence professionnelle – bachelor universitaire de technologie.

1. Objectifs de la formation

La formation de Bachelor Universitaire de Technologie en Réseaux et Télécommunications (B.U.T R&T) répond à la demande toujours croissante de compétences dans les secteurs des technologies de l'information et de la communication. Les réseaux informatiques sont au cœur de nombreuses activités dont l'importance pour la vie sociale et économique est chaque jour plus présente : télétravail, communications mobiles, réseaux à très haut débit, transport et accès à l'information. Ces technologies, en pleine évolution, impliquent des objets communicants de plus en plus répandus tant chez les particuliers que dans les entreprises (Internet des objets). Elles génèrent d'importants flux de données et posent de nouveaux problèmes de cybersécurité. La plupart des entreprises déportent tout ou partie de leurs données et traitements vers des data centers et mobilisent des solutions cloud. Le déploiement d'infrastructures et de services réseaux ou le suivi de leur évolution sont au cœur de projets d'envergure à gérer et piloter. Le B.U.T R&T forme en trois ans des professionnels en réseaux et télécommunications, cadres intermédiaires de leur entreprise ou de leur organisation, capables de comprendre, de mettre en œuvre, de configurer et de maintenir des équipements et systèmes d'informations, tout en assurant leur sécurité physique et logicielle. En plus des compétences scientifiques et techniques, le B.U.T R&T met l'accent sur les savoir-être, l'éthique, la capacité à travailler en équipe dans un environnement international et la compréhension des enjeux des technologies modernes.

Les fonctions du diplômé de B.U.T Réseaux & Télécommunications

La formation dispensée dans les départements de la spécialité "Réseaux et Télécommunications" permet au ou à la future diplômée d'exercer différentes activités professionnelles :

- conception, installation, administration d'infrastructures et de services réseaux informatiques et de solutions cloud ;
- déploiement et administration de solutions de télécommunications fixes ou mobiles et de systèmes de communications (VoIP, téléconférence, visio-conférence, vidéo-surveillance, chat ...);
- analyse, suivi, coordination des projets et leur valorisation ; déploiement et maintenance d'un système d'information et de solutions logicielles, développement d'outils informatiques.

Cinq parcours de spécialité

La formation repose sur un socle commun de compétences dans les domaines réseaux, informatiques et télécommunications. Ce socle, représentant 80% de la formation, couvre l'administration des réseaux IP (Internet), la connexion des entreprises et des usagers, la création d'outils et d'applications informatiques pour les réseaux et télécommunications. Il est complété par une spécialisation sous forme de compétences complémentaires sur la 2ème et la 3ème année. Cette spécialisation est à choisir parmi cinq orientations professionnelles en R&T :

- Cybersécurité,
- Développement système et cloud,
- Internet des objets et mobilité,
- Pilotage de projets réseaux,
- Réseaux opérateurs et multimédia.

Ces 5 parcours se déroulent sur les 2 dernières années avec un objectif d'insertion professionnelle en fin de cursus ce qui n'exclut pas pour autant les poursuites d'études.

1.1. Le parcours : Cybersécurité

Le parcours Cybersécurité (Cyber) forme des professionnels R&T dans l'analyse des risques d'attaques menaçant les systèmes d'informations d'une entreprise (réseaux, serveurs, postes de travail ...). Ainsi, il est en mesure de définir la politique de sécurité de l'entreprise visant à fixer le cadre d'utilisation des ressources numériques, à sensibiliser et former les utilisateurs. Il est également en capacité d'appliquer au sein de l'entreprise la loi notamment RGPD et les préconisations de l'Etat (ANSSI) imposées par le contexte actuel.

Ce parcours regroupe l'ensemble des métiers liés à la sécurité des systèmes d'information, de l'installation d'équipements de sécurité à leur surveillance. Le spécialiste en Cybersécurité est capable d'administrer un système d'informations sécurisé, de le superviser, de détecter et de parer aux attaques informatiques.

Les diplômés exercent les métiers de Technicien en cybersécurité, Technicien des réseaux d'entreprises, Technicien réseaux sécurisés, Technicien d'infrastructures sécurisées, Coordinateur cybersécurité des systèmes d'information, Administrateur de solutions de sécurité, Auditeur de sécurité technique, Opérateur analyste SOC (Security Operation Center), Intégrateur de solutions de sécurité, Administrateur Data Center.

1.2. Le parcours : Développement système et cloud

Le parcours Développement Système et Cloud (DevCloud) forme des professionnels R&T à deux situations professionnelles complémentaires : il est à même de comprendre, déployer, tester une infrastructure ou une application informatique en collaboration avec les architectes et administrateurs réseaux ou les développeurs d'applications. Il met également en place et maintient un environnement Cloud adapté aux besoins métiers tout en automatisant la production.

Ce parcours regroupe l'ensemble des métiers liés aux solutions Cloud (DevCloud, DevOps) en mettant en œuvre, en maintenant et en configurant ces solutions adaptées aux entreprises. Le spécialiste en développement système et cloud est capable d'administrer, de configurer et de maintenir l'ensemble des solutions Cloud de l'entreprise.

Les diplômés exercent les métiers de Technicien réseaux cloud, Administrateur cloud, Intégrateur cloud, intégrateur DevOps, Administrateur Réseaux Programmables, Administrateur Système et Réseaux (DevOps, NetDevOps), Technicien sécurité des systèmes cloud (DevSecOps), Administrateur de serveurs et de réseaux virtualisés.

1.3. Le parcours : Internet des objets et mobilité

Le parcours Internet des Objets et Mobilité (IOM) forme des professionnels R&T à la maîtrise des technologies de communication entre objets mobiles et communicants : téléphones, ordinateurs, véhicules, capteurs de toute nature. Le secteur de l'Internet des objets est en plein développement avec de nombreux métiers dans des domaines tels que l'agriculture de précision, l'Industrie 4.0, les systèmes de transport intelligents, et la e-Santé. De nouvelles technologies et normes sont conçues pour ce domaine (LoRa, Sigfox, NB-IoT, IEEE 802.15.4, etc.). Les différentes générations des réseaux mobiles (3G, 4G, 5G, xG) ainsi que les solutions de communication sans fil (WiFi, Bluetooth) continuent à générer de nombreux emplois de cadres intermédiaires et sont de plus en plus utilisées pour l'Internet des objets.

Ce parcours regroupe l'ensemble des métiers autour des objets mobiles et communicants en incluant les technologies de communications. Le spécialiste en internet des objets et mobilités est capable de maîtriser les technologies de communication entre objets mobiles et communicants : téléphones, véhicules, capteurs de toute nature.

Les diplômés exercent les métiers de Technicien de maintenance exploitation, Technicien de maintenance réseaux mobiles, Technicien télécom, Technicien support réseau mobile, Administrateur en IOT, Administrateur réseaux et internet des objets, Consultant Internet des Objets ...

1.4. Le parcours : Pilotage de projets de réseaux

Le parcours Pilotage de Projets Réseaux (PilPro) forme des professionnels R&T aux technologies des réseaux informatiques et de télécommunications afin de faire dialoguer les différents acteurs d'un projet ou d'un contrat. Il a la capacité d'analyser et de piloter les demandes internes et externes des organisations, quelles que soient leurs tailles. Il analyse et réalise les composantes des contrats, dans le respect des normes techniques et réglementaires de son activité.

Ce parcours regroupe l'ensemble des métiers autour des technologies des réseaux informatiques et de télécommunications afin de dialoguer avec les différents acteurs d'un projet ou d'un contrat. Le spécialiste en pilotage de projets réseaux assure le pilotage et la direction d'activités réseaux et télécoms. Il est capable d'analyser, de suivre, de coordonner puis de piloter les demandes internes et externes des entreprises, organismes privés ou publics, dans le respect des normes techniques et réglementaires de son activité.

Les diplômés exercent les métiers de Responsable d'affaires clients, Conducteur de travaux (cuivre, fibre ou mobile), Technicien avant-vente, Technicien de production, Coordinateur de projet R&T, Chargé d'études télécoms, Pilote d'activités réseaux et télécoms, Pilote de production réseaux, Architecte réseau complexe ...

1.5. Le parcours : Réseaux Opérateurs et Multimédia

Le parcours Réseaux Opérateurs et Multimédia (ROM) forme des professionnels R&T aux métiers des opérateurs de télécommunication fixe et mobile qui fournissent l'accès au réseau pour les entreprises ou les particuliers (fibres optiques, cœur de

réseaux ...) et aux métiers d'intégrateur de solutions de communication pour l'entreprise (téléphonie sur IP, visio-conférence, vidéo-protection). Il a la capacité de configurer et de maintenir le réseau de données d'une entreprise. Il gère, sécurise et supervise ses services voix et données.

Ce parcours regroupe les métiers l'ensemble des métiers liés aux opérateurs de télécommunication fixe et mobile, et intégrateurs de solutions de communication pour l'entreprise. Le spécialiste en Réseaux Opérateurs et Multimédia est capable d'installer, de maintenir des systèmes réseaux allant des serveurs au systèmes voix, données et vidéo.

Les diplômés exercent les métiers de Technicien d'intervention client boucle locale, Technicien support réseaux fixes, Chargé de support technique, Technicien service client SAV, Superviseur ADSL/FTTH, Technicien production et d'intégration de solutions complexes, Technicien déploiement de la fibre optique, Pilote de production, Chargé d'ingénierie réseau structurant, Technicien d'intervention VoIP, Administrateur Réseau VoIP, Administrateur réseau et sécurité, administrateur réseaux et télécommunications, administrateur voix ...

Deuxième partie

Référentiel de compétences

1. Parcours : Cybersécurité

Référentiel de compétences

Référentiel de compétences du B.U.T. Réseaux et Télécommunications

Parcours Cybersécurité

Les compétences et les composantes essentielles

B.U.T. Réseaux et Télécommunications

Parcours Cybersécurité

Une compétence est un « savoir-agir complexe, prenant appui sur la mobilisation et la combinaison efficaces d'une variété de ressources à l'intérieur d'une famille de situations » (Tardif, 2006). Les ressources désignent ici les savoirs, savoir-faire et savoir-être dont dispose un individu et qui lui permettent de mettre en œuvre la compétence.

Administre	Administre les réseaux et l'Internet	<ul style="list-style-type: none">- CE1.01 en choisissant les solutions et technologies réseaux adaptées- CE1.02 en respectant les principes fondamentaux de la sécurité informatique- CE1.03 en utilisant une approche rigoureuse pour la résolution des dysfonctionnements- CE1.04 en respectant les règles métiers- CE1.05 en assurant une veille technologique
Connecter	Connecter les entreprises et les usagers	<ul style="list-style-type: none">- CE2.01 en communiquant avec le client et les différents acteurs impliqués, parfois en anglais- CE2.02 en faisant preuve d'une démarche scientifique- CE2.03 en choisissant les solutions et technologies adaptées- CE2.04 en proposant des solutions respectueuses de l'environnement
Programmer	Créer des outils et applications informatiques pour les R&T	<ul style="list-style-type: none">- CE3.01 en étant à l'écoute des besoins du client- CE3.02 en documentant le travail réalisé- CE3.03 en utilisant les outils numériques à bon escient- CE3.04 en choisissant les outils de développement adaptés- CE3.05 en intégrant les problématiques de sécurité
Sécuriser	Administre un système d'information sécurisé	<ul style="list-style-type: none">- CE4.01 en visant un juste compromis entre exigences de sécurité et contraintes d'utilisation- CE4.02 en respectant les normes et le cadre juridique- CE4.03 en intégrant les dernières technologies- CE4.04 en travaillant en équipe- CE4.05 en sensibilisant efficacement des utilisateurs
Surveiller	Surveiller un système d'information sécurisé	<ul style="list-style-type: none">- CE5.01 en assurant une veille permanente- CE5.02 en réalisant les mises à jour critiques- CE5.03 en automatisant des tâches- CE5.04 en s'intégrant dans une équipe- CE5.05 en surveillant le comportement du réseau- CE5.06 en veillant au respect des contrats et à la conformité des obligations du système d'information

Les situations professionnelles

B.U.T. Réseaux et Télécommunications

Parcours Cybersécurité

Les situations professionnelles se réfèrent aux **contextes** dans lesquels les compétences sont mises en jeu. Ces situations varient selon la compétence ciblée.

Administre	Situations professionnelles	<ul style="list-style-type: none">Conception et administration de l'infrastructure du réseau informatique d'une entrepriseInstallation et administration des services réseau informatique d'une entrepriseDéploiement et administration des solutions fixes pour les clients d'un opérateur de télécommunication
Connecter	Situations professionnelles	<ul style="list-style-type: none">Déploiement des supports et systèmes de transmissionMise en service et administration des équipements d'accès fixe ou mobile d'un opérateur de télécommunicationsDéploiement et administration des accès sans fil pour l'entrepriseDéploiement des systèmes de communications
Programmer	Situations professionnelles	<ul style="list-style-type: none">Conception, déploiement et maintenance du système d'information d'une entrepriseAutomatisation du déploiement et de la maintenance des outils logicielsDéveloppement d'outils informatiques à usage interne d'une équipe
Sécuriser	Situations professionnelles	<ul style="list-style-type: none">Analyse de l'existant et étude des besoins de sécurité d'une petite structureÉvolution et mise en conformité du système d'information d'une entreprise
Surveiller	Situations professionnelles	<ul style="list-style-type: none">Surveillance et analyse du système d'informationAudit de sécuritéGestion d'un incident de sécurité

Les niveaux de développement des compétences

B.U.T. Réseaux et Télécommunications
Parcours Cybersécurité

Administre	Connexion	Programmer	Sécuriser	Surveiller
Niveau 1 Assister l'administrateur du réseau	Niveau 1 Découvrir les transmissions et la ToIP	Niveau 1 S'intégrer dans un service informatique		
Niveau 2 Administrer un réseau	Niveau 2 Maîtriser les différentes composantes des solutions de connexion des entreprises et des usagers	Niveau 2 Développer une application R&T	Niveau 1 Sensibiliser aux vulnérabilités d'un système d'information et aux remédiations possibles	Niveau 1 Prendre en main les outils de surveillance et de test du système d'information
Niveau 3 Concevoir un réseau	Niveau 3 Déployer une solution de connexion ou de communication sur IP	Niveau 3 Piloter un projet de développement d'une application R&T	Niveau 2 Mettre en œuvre un système d'information sécurisé pour une petite structure	Niveau 2 Mettre en œuvre le système de surveillance d'incidents de sécurité

Compétence Administrer

B.U.T. Réseaux et Télécommunications

Parcours Cybersécurité

Administrer	Administrer les réseaux et l'Internet	- CE1.01 en choisissant les solutions et technologies réseaux adaptées - CE1.02 en respectant les principes fondamentaux de la sécurité informatique - CE1.03 en utilisant une approche rigoureuse pour la résolution des dysfonctionnements - CE1.04 en respectant les règles métiers - CE1.05 en assurant une veille technologique
Situations professionnelles	Conception et administration de l'infrastructure du réseau informatique d'une entreprise Installation et administration des services réseau informatique d'une entreprise Déploiement et administration des solutions fixes pour les clients d'un opérateur de télécommunication	
Niveaux		Apprentissages critiques
Niveau 1 Assister l'administrateur du réseau		<ul style="list-style-type: none">- AC11.01 Maîtriser les lois fondamentales de l'électricité afin d'intervenir sur des équipements de réseaux et télécommunications- AC11.02 Comprendre l'architecture et les fondements des systèmes numériques, les principes du codage de l'information, des communications et de l'Internet- AC11.03 Configurer les fonctions de base du réseau local- AC11.04 Maîtriser les rôles et les principes fondamentaux des systèmes d'exploitation afin d'interagir avec ceux-ci pour la configuration et l'administration des réseaux et services fournis- AC11.05 Identifier les dysfonctionnements du réseau local et savoir les signaler- AC11.06 Installer un poste client, expliquer la procédure mise en place
Niveau 2 Administrer un réseau		<ul style="list-style-type: none">- AC21.01 Configurer et dépanner le routage dynamique dans un réseau- AC21.02 Configurer et expliquer une politique simple de QoS et les fonctions de base de la sécurité d'un réseau- AC21.03 Déployer des postes clients et des solutions virtualisées adaptées à une situation donnée- AC21.04 Déployer des services réseaux avancés- AC21.05 Identifier les réseaux opérateurs et l'architecture d'Internet- AC21.06 Travailler en équipe pour développer ses compétences professionnelles
Niveau 3 Concevoir un réseau		<ul style="list-style-type: none">- AC31.01 Concevoir un projet de réseau informatique d'une entreprise en intégrant les problématiques de haute disponibilité, de QoS, de sécurité et de supervision- AC31.02 Réaliser la documentation technique de ce projet- AC31.03 Réaliser une maquette de démonstration du projet- AC31.04 Défendre/argumenter un projet- AC31.05 Communiquer avec les acteurs du projet- AC31.06 Gérer le projet et les différentes étapes de sa mise en œuvre en respectant les délais

Compétence Connecter

B.U.T. Réseaux et Télécommunications

Parcours Cybersécurité

Connecter	Connecter les entreprises et les usagers	<ul style="list-style-type: none">- CE2.01 en communiquant avec le client et les différents acteurs impliqués, parfois en anglais- CE2.02 en faisant preuve d'une démarche scientifique- CE2.03 en choisissant les solutions et technologies adaptées- CE2.04 en proposant des solutions respectueuses de l'environnement
Situations professionnelles	<ul style="list-style-type: none">Déploiement des supports et systèmes de transmissionMise en service et administration des équipements d'accès fixe ou mobile d'un opérateur de télécommunicationsDéploiement et administration des accès sans fil pour l'entrepriseDéploiement des systèmes de communications	
Niveaux	Apprentissages critiques	
Niveau 1 Découvrir les transmissions et la ToIP	<ul style="list-style-type: none">- AC12.01 Mesurer, analyser et commenter les signaux- AC12.02 Caractériser des systèmes de transmissions élémentaires et découvrir la modélisation mathématique de leur fonctionnement- AC12.03 Déployer des supports de transmission- AC12.04 Connecter les systèmes de ToIP- AC12.05 Communiquer avec un tiers (client, collaborateur...) et adapter son discours et sa langue à son interlocuteur	
Niveau 2 Maîtriser les différentes composantes des solutions de connexion des entreprises et des usagers	<ul style="list-style-type: none">- AC22.01 Déployer et caractériser des systèmes de transmissions complexes- AC22.02 Mettre en place un accès distant sécurisé- AC22.03 Mettre en place une connexion multi-site via un réseau opérateur- AC22.04 Déployer des réseaux d'accès des opérateurs- AC22.05 Capacité à questionner un cahier des charges RT	
Niveau 3 Déployer une solution de connexion ou de communication sur IP	<ul style="list-style-type: none">- AC32.01 Déployer un système de communication pour l'entreprise- AC32.02 Déployer un réseau d'accès sans fil pour le réseau d'entreprise en intégrant les enjeux de la sécurité- AC32.03 Déployer un réseau d'accès fixe ou mobile pour un opérateur de télécommunications en intégrant la sécurité- AC32.04 Permettre aux collaborateurs de se connecter de manière sécurisée au système d'information de l'entreprise- AC32.05 Collaborer en mode projet en français et en anglais	

Compétence Programmer

B.U.T. Réseaux et Télécommunications

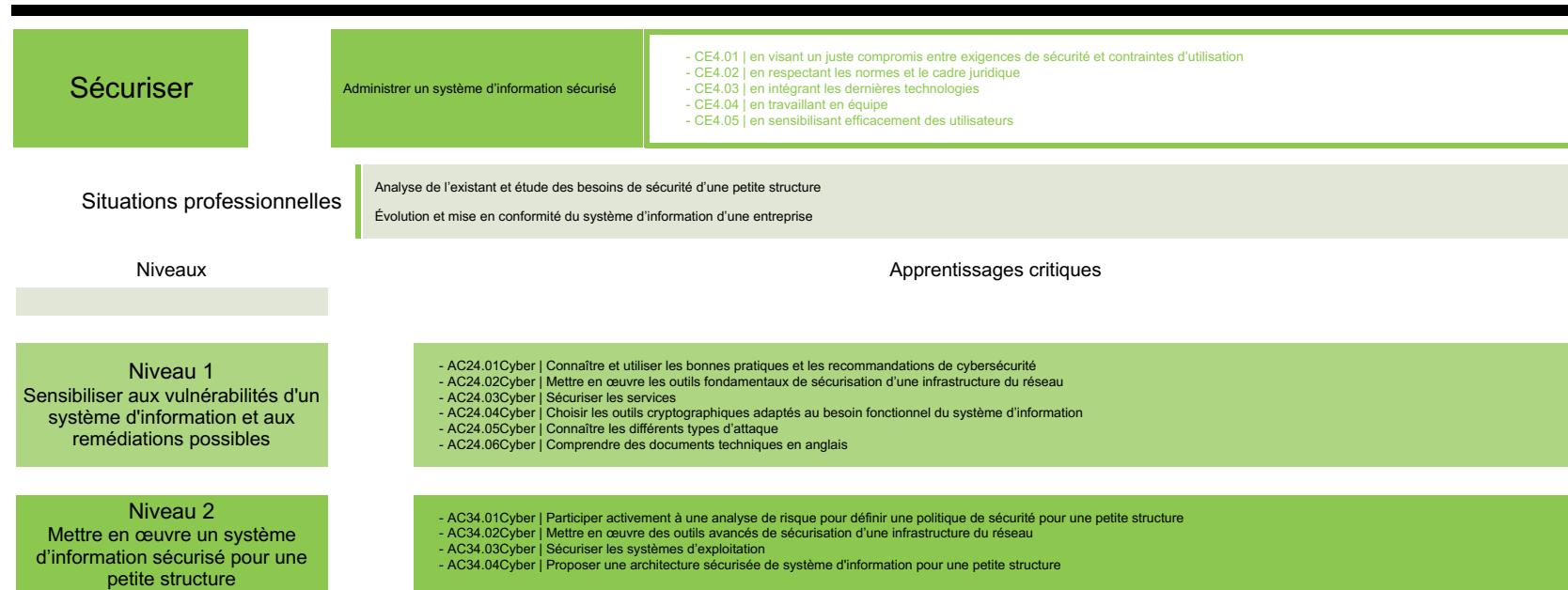
Parcours Cybersécurité

Programmer	Créer des outils et applications informatiques pour les R&T	<ul style="list-style-type: none">- CE3.01 en étant à l'écoute des besoins du client- CE3.02 en documentant le travail réalisé- CE3.03 en utilisant les outils numériques à bon escient- CE3.04 en choisissant les outils de développement adaptés- CE3.05 en intégrant les problématiques de sécurité
<p>Situations professionnelles</p> <p>Conception, déploiement et maintenance du système d'information d'une entreprise</p> <p>Automatisation du déploiement et de la maintenance des outils logiciels</p> <p>Développement d'outils informatiques à usage interne d'une équipe</p>		
Niveaux		Apprentissages critiques
Niveau 1 S'intégrer dans un service informatique	<ul style="list-style-type: none">- AC13.01 Utiliser un système informatique et ses outils- AC13.02 Lire, exécuter, corriger et modifier un programme- AC13.03 Traduire un algorithme, dans un langage et pour un environnement donné- AC13.04 Connaitre l'architecture et les technologies d'un site Web- AC13.05 Choisir les mécanismes de gestion de données adaptés au développement de l'outil et argumenter ses choix- AC13.06 S'intégrer dans un environnement propice au développement et au travail collaboratif	
Niveau 2 Développer une application R&T	<ul style="list-style-type: none">- AC23.01 Automatiser l'administration système avec des scripts- AC23.02 Développer une application à partir d'un cahier des charges donné, pour le Web ou les périphériques mobiles- AC23.03 Utiliser un protocole réseau pour programmer une application client/serveur- AC23.04 Installer, administrer un système de gestion de données- AC23.05 Accéder à un ensemble de données depuis une application et/ou un site web	
Niveau 3 Piloter un projet de développement d'une application R&T	<ul style="list-style-type: none">- AC33.01 Élaborer les spécifications techniques et le cahier des charges d'une application informatique- AC33.02 Mettre en place un environnement de travail collaboratif- AC33.03 Participer à la formation des utilisateurs- AC33.04 Déployer et maintenir une solution informatique- AC33.05 S'informer sur les évolutions et les nouveautés technologiques- AC33.06 Sécuriser l'environnement numérique d'une application	

Compétence Sécuriser

B.U.T. Réseaux et Télécommunications

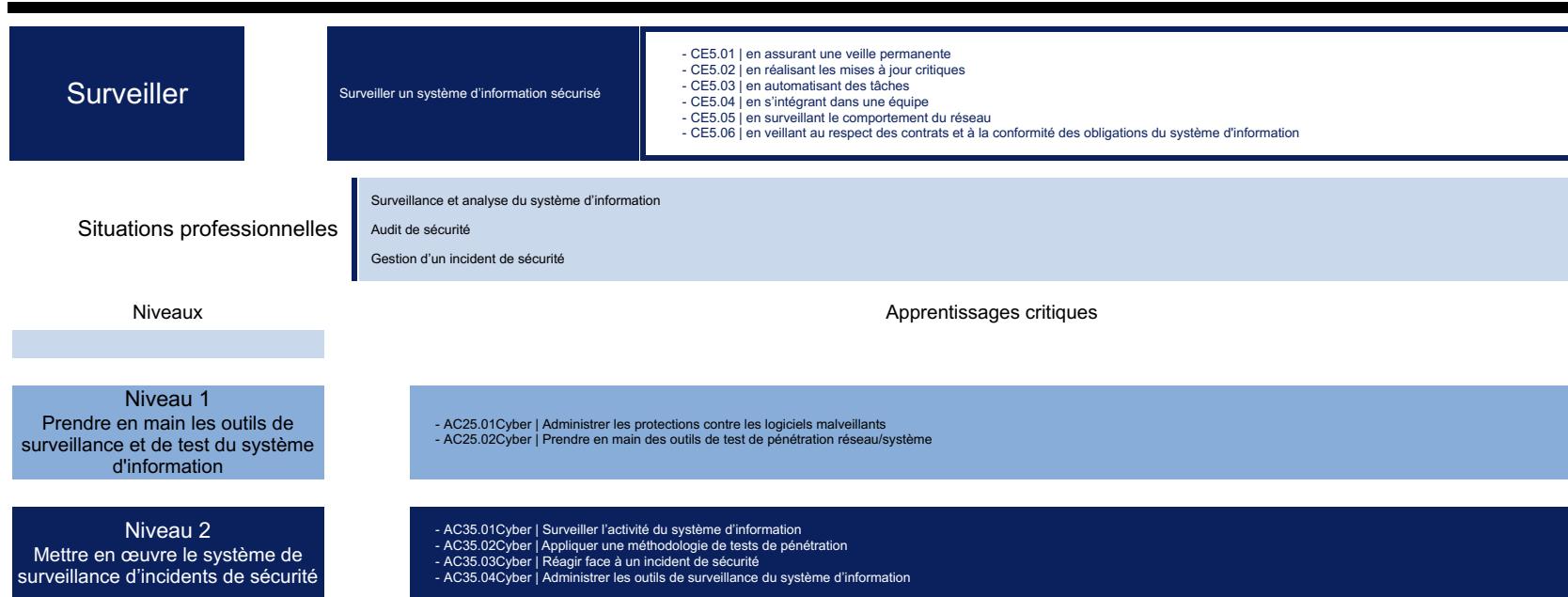
Parcours Cybersécurité



Compétence Surveiller

B.U.T. Réseaux et Télécommunications

Parcours Cybersécurité



Chapitre 4.

Parcours : Cybersécurité

1. Semestre 3

1.1. Tableau croisé

Ce tableau explicite les correspondances entre les compétences, les apprentissages critiques, les SAÉ et les ressources programmés dans le semestre.

Les SAÉ et les ressources ainsi identifiées pour chaque UE participent à son obtention, et en ce sens doivent faire l'objet d'une évaluation, à l'exception de la démarche portfolio des semestres impairs.

Ce tableau détaille par ailleurs la répartition du volume horaire global des heures d'enseignement encadré de chaque semestre, à savoir :

- le volume horaire alloué à l'ensemble des SAÉ ;
- le volume de chaque ressource définie nationalement dont les heures TP ;
- le volume horaire, dont les heures TP, relevant d'une partie de l'adaptation locale et pouvant être affecté de manière non exclusive soit aux SAÉ, soit aux ressources définies nationalement ou localement.

1.2. Fiches Situations d'apprentissage et d'évaluation (SAÉ)

1.2.1. SAÉ 3.01 : Mettre en oeuvre un système de transmission

Compétence ciblée :

- Connecter les entreprises et les usagers

Objectifs et problématique professionnelle :

Le professionnel R&T propose et met en oeuvre des solutions répondant aux besoins d'un système de transmission selon un cahier des charges.

Descriptif générique :

A partir d'un cahier des charges spécifiant les besoins d'un système de transmission pour un opérateur ou une entreprise (connexion entre bâtiments par exemple), le professionnel R&T participe à l'étude des différentes solutions techniques, au choix de la solution technique retenue, à son installation et sa mise en oeuvre.

Il est ainsi amené à :

- proposer des solutions en les justifiant d'un point de vue théorique et pratique ;
- dimensionner les équipements ;
- mettre en place la solution retenue ;
- prendre en main les appareils d'analyses et de mesures ;
- caractériser les performances du système de transmission.

Apprentissages critiques :

- AC22.01 | Déployer et caractériser des systèmes de transmissions complexes
- AC22.03 | Mettre en place une connexion multi-site via un réseau opérateur
- AC22.04 | Déployer des réseaux d'accès des opérateurs
- AC22.05 | Capacité à questionner un cahier des charges RT

Ressources mobilisées et combinées :

- R3.05 | Chaînes de transmissions numériques
- R3.06 | Fibres optiques et propagation
- R3.07 | Réseaux d'accès
- R3.11 | Anglais professionnel 1
- R3.12 | Expression-Culture-Communication professionnelles : Savoir collaborer
- R3.13 | Projet Personnel et Professionnel
- R3.14 | Analyse de Fourier
- R3.15 | Gestion de projet 2 : Utiliser les méthodes de gestion de projet

Volume horaire :

Volume horaire : à définir localement par chaque IUT

1.2.2. SAÉ 3.02 : Développer des applications communicantes

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

Objectifs et problématique professionnelle :

Le professionnel R&T est amené à installer, adapter et développer des outils logiciels permettant l'échange d'informations au sein de l'entreprise. Il met en place une solution adaptée qui respecte les besoins et les contraintes techniques imposées par l'entreprise. Il utilise dans ce but différents protocoles de communication, différents moyens d'authentification et de sauvegarde des données sécurisées. Il commente le code produit et génère la documentation technique en français ou en anglais. Il doit aussi présenter sa solution en argumentant les choix opérés avant la validation.

Descriptif générique :

Partant de l'analyse d'un cahier des charges fourni, le professionnel R&T développe une application communicante permettant l'échange et la sauvegarde de données (position GPS, données d'emploi du temps, ...). La réalisation de ce projet contient les étapes suivantes :

- Analyser le cahier des charges fourni et répondre à celui-ci en mentionnant les technologies à utiliser et éventuellement leur impact environnemental et économique ;
- Développer une application client/serveur (le serveur pouvant être fourni ou développé) ;
- Authentifier les utilisateurs ;
- Sauvegarder les données échangées ;
- Concevoir une interface graphique, une application mobile ou une interface Web.

Mots-clés : Protocoles (TCP, UDP, HTTP, HTTPS), Objets (socket, websocket, socket-io), Sérialisation (base de données SQL ou no-SQL, fichier binaire ou fichier texte, ...).

Apprentissages critiques :

- AC21.06 | Travailler en équipe pour développer ses compétences professionnelles
- AC22.05 | Capacité à questionner un cahier des charges RT
- AC23.02 | Développer une application à partir d'un cahier des charges donné, pour le Web ou les périphériques mobiles
- AC23.03 | Utiliser un protocole réseau pour programmer une application client/serveur
- AC23.04 | Installer, administrer un système de gestion de données
- AC23.05 | Accéder à un ensemble de données depuis une application et/ou un site web

Ressources mobilisées et combinées :

- R3.08 | Consolidation de la programmation
- R3.09 | Programmation événementielle
- R3.10 | Gestion d'un système de bases de données
- R3.11 | Anglais professionnel 1
- R3.12 | Expression-Culture-Communication professionnelles : Savoir collaborer
- R3.13 | Projet Personnel et Professionnel
- R3.15 | Gestion de projet 2 : Utiliser les méthodes de gestion de projet

Volume horaire :

Volume horaire : à définir localement par chaque IUT

1.2.3. SAÉ 3.Cyber.03 : Concevoir un réseau informatique sécurisé multi-sites

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé
- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers

Objectifs et problématique professionnelle :

Le professionnel R&T spécialisé en Cybersécurité doit mettre en œuvre une infrastructure multi-sites sécurisée et justifier les solutions apportées à partir d'un cahier des charges spécifiant les besoins du réseau d'une entreprise. Il prête une attention particulière aux vulnérabilités potentielles et connues des équipements réseaux et du système d'information installés.

Descriptif générique :

A partir d'un cahier des charges spécifiant les besoins du réseau d'une entreprise, le professionnel Cyber doit mettre en œuvre une infrastructure multi-sites en justifiant les solutions apportées notamment en termes de cybersécurité. Cette infrastructure repose :

- sur les concepts fondamentaux du réseau :
 - routage, filtrage inter-VLAN ;
 - redondance (STP, routage dynamique, VRRP) ;
 - tunnel (VPN, VPN opérateurs) ;
 - services avancés ;
 - Wi-Fi.
- sur la mise en place et la configuration des équipements ;
- sur le test des fonctionnalités et les performances de l'infrastructure (QoS, MLS3) ;
- sur les besoins spécifiques en terme de cybersécurité, en utilisant les outils mis en place dans le cadre de la SAÉ3.Cyber.04 "Découvrir le pentesting" notamment les tests de pénétration et les techniques de durcissement et de remédiation permettant de renforcer la robustesse du réseau informatique ;
- sur une documentation détaillée de l'infrastructure mise en œuvre et de son niveau de sécurité.

Apprentissages critiques :

- AC21.01 | Configurer et dépanner le routage dynamique dans un réseau
- AC21.02 | Configurer et expliquer une politique simple de QoS et les fonctions de base de la sécurité d'un réseau
- AC21.03 | Déployer des postes clients et des solutions virtualisées adaptées à une situation donnée
- AC21.04 | Déployer des services réseaux avancés
- AC21.05 | Identifier les réseaux opérateurs et l'architecture d'Internet
- AC21.06 | Travailler en équipe pour développer ses compétences professionnelles
- AC22.02 | Mettre en place un accès distant sécurisé
- AC22.03 | Mettre en place une connexion multi-site via un réseau opérateur
- AC24.02Cyber | Mettre en œuvre les outils fondamentaux de sécurisation d'une infrastructure du réseau
- AC24.03Cyber | Sécuriser les services
- AC24.06Cyber | Comprendre des documents techniques en anglais
- AC25.01Cyber | Administre les protections contre les logiciels malveillants

Ressources mobilisées et combinées :

- R3.01 | Réseaux de campus
- R3.02 | Réseaux opérateurs
- R3.03 | Services réseaux avancés
- R3.04 | Services d'annuaires
- R3.11 | Anglais professionnel 1
- R3.12 | Expression-Culture-Communication professionnelles : Savoir collaborer
- R3.13 | Projet Personnel et Professionnel
- R3.15 | Gestion de projet 2 : Utiliser les méthodes de gestion de projet
- R3.Cyber.16 | Méthodologie du pentesting

Volume horaire :

Volume horaire : à définir localement par chaque IUT

1.2.4. SAÉ 3.Cyber.04 : Découvrir le pentesting

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé

Objectifs et problématique professionnelle :

Le professionnel R&T spécialisé dans la Cybersécurité doit collecter et exploiter le maximum d'éléments sur son système d'information, cible potentielle d'attaques, afin d'en assurer la sécurité. Il utilise tous les moyens à sa disposition (techniques, ingénierie sociale, recherche internet, ...), tout en respectant une approche "éthique" en accord avec la réglementation (RGPD par exemple) et la charte informatique de l'entreprise.

Descriptif générique :

Le professionnel Cyber réalise trois phases :

- la cartographie (reconnaissance) du système d'information en utilisant des outils et des opérations tels que :
 - base de données whois ;
 - étude du DNS de la zone correspondante ;
 - recherches sur Internet ;
 - ingénierie sociale ;
 - analyse du site web ;
 - scan de ports de serveurs, ...
- la recherche des vulnérabilités dans les données recueillies à l'aide d'outils spécialisés (metasploit, shodan, ...).
- la finalisation de l'analyse en suivant par exemple les 7 phases définies dans la "Cyber Kill Chain" : reconnaissance, armement, livraison, exploitation, installation, commandement et contrôle, actions sur l'objectif.

Apprentissages critiques :

- AC24.01Cyber | Connaître et utiliser les bonnes pratiques et les recommandations de cybersécurité
- AC24.05Cyber | Connaître les différents types d'attaque
- AC24.06Cyber | Comprendre des documents techniques en anglais
- AC25.01Cyber | Administrer les protections contre les logiciels malveillants
- AC25.02Cyber | Prendre en main des outils de test de pénétration réseau/système

Ressources mobilisées et combinées :

- R3.11 | Anglais professionnel 1
- R3.12 | Expression-Culture-Communication professionnelles : Savoir collaborer
- R3.13 | Projet Personnel et Professionnel
- R3.15 | Gestion de projet 2 : Utiliser les méthodes de gestion de projet
- R3.Cyber.16 | Méthodologie du pentesting

Volume horaire :

Volume horaire : à définir localement par chaque IUT

1.2.5. PORTFOLIO : Démarche portfolio

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé
- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

Objectifs et problématique professionnelle :

Au semestre 3, la démarche portfolio consistera en un point étape intermédiaire qui permettra à l'étudiant de se positionner, sans être évalué, dans le processus d'acquisition des niveaux de compétences de la seconde année du B.U.T. et relativement au parcours suivi.

Descriptif générique :

L'équipe pédagogique devra accompagner l'étudiant dans la compréhension et l'appropriation effectives du référentiel de compétences et de ses éléments constitutifs tels que les composantes essentielles en tant qu'elles constituent des critères qualité. Seront également exposées les différentes possibilités de démonstration et d'évaluation de l'acquisition des niveaux de compétences ciblés en deuxième année par la mobilisation notamment d'éléments de preuve issus de toutes les SAÉ. L'enjeu est de permettre à l'étudiant d'engager une démarche d'auto-positionnement et d'auto-évaluation tout en intégrant la spécificité du parcours suivi.

Ressources mobilisées et combinées :

- R3.11 | Anglais professionnel 1
- R3.12 | Expression-Culture-Communication professionnelles : Savoir collaborer
- R3.13 | Projet Personnel et Professionnel
- R3.15 | Gestion de projet 2 : Utiliser les méthodes de gestion de projet

Volume horaire :

Volume horaire : à définir localement par chaque IUT

1.3. Fiches Ressources

1.3.1. Ressource R3.01 : Réseaux de campus

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 3.Cyber.03 | Concevoir un réseau informatique sécurisé multi-sites

Descriptif :

Contexte et ancrage professionnel :

Dans le cadre de cette ressource, les étudiants vont revoir les notions essentielles abordées en 1ère année sur le routage, les VLANs et le routage inter-VLAN et découvriront les rudiments des réseaux sans fil.

Des connaissances complémentaires leur seront également apportées sur le routage dynamique et les ACL.

Contenus :

Les étudiants devront être capables de déployer et configurer les fonctionnalités élémentaires d'un réseau de campus.

L'utilisation de logiciels d'analyses de trames (WireShark, TCPDUMP...) pour les TP, devrait être systématisée.

Révisions et compléments du S1 et du S2 :

- Protocoles de routage dynamique.
- Introduction à la QoS
- OSPF avancé redistribution de routes.
- WIFI (bornes lourdes et/ou légères)
- VLAN/Routage inter VLAN/ACL pour filtrage inter-VLAN,
- Authentification centralisée (initiation à l'utilisation de PAM sur un fichier à plat et/ou gestion sous Windows).

Apprentissages critiques ciblés :

- AC21.01 | Configurer et dépanner le routage dynamique dans un réseau
- AC21.02 | Configurer et expliquer une politique simple de QoS et les fonctions de base de la sécurité d'un réseau
- AC22.05 | Capacité à questionner un cahier des charges RT

Mots clés :

Routage – Routage dynamique – OSPF – BGP – WIFI – VLAN – Routage inter-VLAN – ACL – Authentification centralisée

Volume horaire :

Volume horaire défini nationalement : 20 heures dont 11 heures de TP

1.3.2. Ressource R3.02 : Réseaux opérateurs

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 3.Cyber.03 | Concevoir un réseau informatique sécurisé multi-sites

Descriptif :

Contexte et ancrage professionnel :

Les étudiants devront être capables de décrire la structuration d'un réseau d'opérateur du réseau d'accès au cœur de réseau ainsi que les différentes technologies des réseaux WAN.

Contenus :

Pour cela, les concepts suivants seront détaillés :

- Présentation générale des Réseaux opérateurs de transmission : SDH, WDM/OTN, Carrier-Ethernet,
- Transit peering, BGP
- Mécanisme de transport MPLS, VPN L2 et VPN L3

Prolongements possibles :

Déploiement de réseaux Ethernet commutés très haut débit

Apprentissages critiques ciblés :

- AC21.05 | Identifier les réseaux opérateurs et l'architecture d'Internet
- AC22.03 | Mettre en place une connexion multi-site via un réseau opérateur

Mots clés :

Réseaux opérateurs – MPLS – BGP – VRF – SDH – Carrier Ethernet – WDM – OTN

Volume horaire :

Volume horaire défini nationalement : 18 heures dont 11 heures de TP

1.3.3. Ressource R3.03 : Services réseaux avancés

Compétence ciblée :

- Administrer les réseaux et l'Internet

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 3.Cyber.03 | Concevoir un réseau informatique sécurisé multi-sites

Descriptif :

Contexte et ancrage professionnel :

Les professionnels R&T doivent être capables d'installer et configurer le serveur DNS d'une zone ainsi que le serveur de courrier correspondant.

Contenus :

L'architecture globale du système de nommage internet ainsi que le fonctionnement de la messagerie électronique seront étudiés. Les interactions entre les deux services seront détaillées.

Des clients de tests (nslookup, dig, host, mutt, ...) seront utilisés.

Dans le cadre des travaux pratiques, il pourra s'agir de :

- Installer et configurer un serveur DNS
- Installer un utilitaire client DNS (nslookup, dig, host, ...)
- Installer et configurer un serveur SMTP
- Installer et configurer un serveur IMAP et/ou POP
- Installer et configurer un client IMAP et/ou POP

Apprentissages critiques ciblés :

- AC21.03 | Déployer des postes clients et des solutions virtualisées adaptées à une situation donnée
- AC21.04 | Déployer des services réseaux avancés

Mots clés :

DNS – Messagerie électronique – Mail – SMTP – POP – IMAP

Volume horaire :

Volume horaire défini nationalement : 15 heures dont 11 heures de TP

1.3.4. Ressource R3.04 : Services d'annuaires

Compétence ciblée :

- Administrer les réseaux et l'Internet

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 3.Cyber.03 | Concevoir un réseau informatique sécurisé multi-sites

Descriptif :

Contexte et ancrage professionnel :

Les étudiants seront capables d'installer, configurer et interroger un annuaire d'entreprise.

Contenus :

Les concepts généraux des annuaires ainsi que leur interconnexion seront présentés dans le cadre de ce cours. Des exemples d'utilisation courante pourront être détaillés.

Les manipulations suivantes peuvent être envisagées dans le cadre de séances de Travaux Pratiques :

- Notion d'annuaire LDAP et/ou Active Directory
- Notion d'authentification centralisée
- Mise en œuvre d'un annuaire
- Interrogation d'un annuaire
- Exploitation de cet annuaire

Préconisations de mise en oeuvre :

les problématiques suivantes peuvent être abordés :

- Conception d'un annuaire
- Sécurisation d'un annuaire (droits d'accès)

Apprentissages critiques ciblés :

- AC21.03 | Déployer des postes clients et des solutions virtualisées adaptées à une situation donnée
- AC21.04 | Déployer des services réseaux avancés

Mots clés :

Annuaire – LDAP – Active directory – DIT

Volume horaire :

Volume horaire défini nationalement : 8 heures dont 5 heures de TP

1.3.5. Ressource R3.05 : Chaînes de transmissions numériques

Compétence ciblée :

- Connecter les entreprises et les usagers

SAÉ au sein desquelles la ressource peut être mobilisée et combinée :

- SAÉ 3.01 | Mettre en oeuvre un système de transmission

Descriptif :

Contexte et ancrage professionnel :

L'étudiant devra être capable de maîtriser les éléments fondamentaux d'une chaîne de transmission analogique et numérique.

Contenus :

- Bases des transmissions radio : notion de translation de fréquence :
 - AM
 - aspect temporels et fréquentiels
- Notion de symboles :
 - Débit, rapidité de modulation, ...
- Modulations en bande de base : PAM
 - aspect temporels et fréquentiels
 - différents types de modulation en bande de base
- Caractérisation d'une modulation :
 - diagramme de l'oeil
 - diagramme de constellation
 - SNR, Valence
 - BER
- Modulations numériques sur fréquence porteuse :
 - ASK
 - FSK
 - PSK
 - QAM et modulation IQ
- Architecture d'un système de transmission.

Apprentissage critique ciblé :

- AC22.01 | Déployer et caractériser des systèmes de transmissions complexes

Mots clés :

Modulation – Spectre – Bande de base – ASK – FSK – PSK – QAM – IQ – Diagramme de l'œil – Constellation – Système de transmission – Émetteur – Canal – Récepteur

Volume horaire :

Volume horaire défini nationalement : 36 heures dont 17 heures de TP

1.3.6. Ressource R3.06 : Fibres optiques et propagation

Compétence ciblée :

- Connecter les entreprises et les usagers

SAÉ au sein desquelles la ressource peut être mobilisée et combinée :

- SAÉ 3.01 | Mettre en oeuvre un système de transmission

Descriptif :

Contexte et ancrage professionnel :

L'étudiant devra être capable de décrire, caractériser et déployer des supports, à base de fibres optiques ou de câbles, nécessaires à la transmission.

Contenus :

- Propagation sur câble
- Adaptation d'impédance
- Fibres optiques : Propagation, Liaison optique, Photométrie et Réflectométrie
- Bilans de liaison

Préconisations de mise en oeuvre :

- Ondes stationnaires - diaphonie.
- Fibres optiques : Optique géométrique pour les fibres, Fibres monomodes et multimodes, Budget optique, Bande passeante de modulation, WDM

Apprentissage critique ciblé :

- AC22.01 | Déployer et caractériser des systèmes de transmissions complexes

Mots clés :

Fibre optique – Monomode – Multimode – Liaison optique – Budget optique – Photométrie – Réflectométrie – Propagation – Adaptation d'impédance – TOS – Atténuation – Bilan de liaison – Dispersion

Volume horaire :

Volume horaire défini nationalement : 18 heures dont 9 heures de TP

1.3.7. Ressource R3.07 : Réseaux d'accès

Compétence ciblée :

- Connecter les entreprises et les usagers

SAÉ au sein desquelles la ressource peut être mobilisée et combinée :

- SAÉ 3.01 | Mettre en oeuvre un système de transmission

Descriptif :

Contexte et ancrage professionnel :

L'étudiant devra être capable de décrire l'architecture d'un réseau d'accès (cuivre, fibre).

Contenus :

- Architecture globale d'un réseau d'opérateur, Panorama des réseaux d'accès
- Réseau d'accès xDSL :
 - Architecture de la boucle locale cuivre
 - Principe de l'OFDM
 - DSLAM
- Réseau d'accès Fibre :
 - Architecture de la boucle locale optique
 - FTTx
 - OLT
 - technologie active ou passive (GPON, XGPON,...)
 - WDM

Prolongements possibles :

Fonctions de gestion des abonnés (BAS, BNG, accès PPPOE, IPOE)

Prérequis :

- R3.05 | Chaînes de transmissions numériques
- R3.06 | Fibres optiques et propagation

Apprentissages critiques ciblés :

- AC22.01 | Déployer et caractériser des systèmes de transmissions complexes
- AC22.04 | Déployer des réseaux d'accès des opérateurs

Mots clés :

XDSL – DSLAM – OFDM – FTTx – PON – OLT – WDM – Réseaux opérateurs – Réseaux accès – Boucle locale – Triple play

Volume horaire :

Volume horaire défini nationalement : 18 heures dont 9 heures de TP

1.3.8. Ressource R3.08 : Consolidation de la programmation

Compétence ciblée :

- Créer des outils et applications informatiques pour les R&T

SAÉ au sein desquelles la ressource peut être mobilisée et combinée :

- SAÉ 3.02 | Développer des applications communicantes

Descriptif :

Contexte et ancrage professionnel :

Cette ressource approfondit les bases de la programmation. Elle permet un traitement automatisé en utilisant des structures de données plus performantes.

Contenus :

L'étudiant abordera les notions suivantes :

- Principes fondamentaux de la programmation orientée objet :
 - Classes/Objets/attributs/méthodes/constructeurs
 - Notion d'héritage, agrégation
 - Format et description de données (affichage, expr. textuelle pour un json/yaml/xml, date avec timezone, retour sur l'encodage)
 - Sérialisation des objets (texte versus binaire)
 - Gestion des erreurs/exceptions

Prolongements possibles :

- les interfaces, classes abstraites, polymorphisme
- Structures de données avancées comme par exemple listes, files, piles, arbres, ...

Apprentissages critiques ciblés :

- AC23.02 | Développer une application à partir d'un cahier des charges donné, pour le Web ou les périphériques mobiles
- AC23.05 | Accéder à un ensemble de données depuis une application et/ou un site web

Mots clés :

POO – Classes – Objet – Algorithmes – Sérialisation – Encodage – Exceptions

Volume horaire :

Volume horaire défini nationalement : 17 heures dont 11 heures de TP

1.3.9. Ressource R3.09 : Programmation événementielle

Compétence ciblée :

- Créer des outils et applications informatiques pour les R&T

SAÉ au sein desquelles la ressource peut être mobilisée et combinée :

- SAÉ 3.02 | Développer des applications communicantes

Descriptif :

Contexte et ancrage professionnel :

L'étudiant sera capable d'utiliser les techniques de programmation en réaction à des événements abordés du point de vue interface homme machine, réseau et système.

Contenus :

Seront abordés :

- la notion de programmation synchrone vs asynchrone,
- les principes de la programmation réseau,
- la gestion des processus : Thread ...

Ces notions peuvent être approfondies à partir d'un ou plusieurs des exemples suivants :

- Interface homme machine : applications graphiques, web ou smartphone,
- Boucle d'événements,
- Socket, websocket,
- Timer,
- Programmation asynchrone.

Prérequis :

- R3.08 | Consolidation de la programmation

Apprentissages critiques ciblés :

- AC23.02 | Développer une application à partir d'un cahier des charges donné, pour le Web ou les périphériques mobiles
- AC23.03 | Utiliser un protocole réseau pour programmer une application client/serveur

Mots clés :

Événement – Callback – Socket – Datagramme – Synchrone – Asynchrone – IHM – Processus

Volume horaire :

Volume horaire défini nationalement : 11 heures dont 9 heures de TP

1.3.10. Ressource R3.10 : Gestion d'un système de bases de données

Compétences ciblées :

- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein desquelles la ressource peut être mobilisée et combinée :

- SAÉ 3.02 | Développer des applications communicantes

Descriptif :

Contexte et ancrage professionnel :

Le professionnel RT peut être amené à installer et administrer un système de gestion de bases de données à l'instar d'un service réseau à part entière.

Contenus :

La ressource lui permet d'acquérir les notions suivantes :

- L'installation et la configuration d'un système de gestion de base de données,
- La gestion des comptes utilisateurs du service et leur accès à l'interface d'administration
- La gestion des droits d'accès aux données par les utilisateurs,
- La sécurité des données et des connexions au service,
- La sauvegarde et la restauration.

La ressource peut aussi aborder les stratégies et méthodes de conception (qu'il s'agisse du schéma de la BDD ou de la structure du réseau pour y intégrer un service de BDD).

Apprentissages critiques ciblés :

- AC22.02 | Mettre en place un accès distant sécurisé
- AC23.04 | Installer, administrer un système de gestion de données

Mots clés :

SBGD – Sécurité – Données

Volume horaire :

Volume horaire défini nationalement : 7 heures dont 4 heures de TP

1.3.11. Ressource R3.11 : Anglais professionnel 1

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 3.01 | Mettre en oeuvre un système de transmission
- SAÉ 3.02 | Développer des applications communicantes
- SAÉ 3.Cyber.03 | Concevoir un réseau informatique sécurisé multi-sites
- SAÉ 3.Cyber.04 | Découvrir le pentesting
- PORTFOLIO | Portfolio

Descriptif :

Contexte et ancrage professionnel :

Cette ressource apporte le socle de connaissances langagières pour les compétences de cœur de métier « Administrer les réseaux et l'Internet » et « Connecter les entreprises et les usagers ». Elle contribue aussi à la compétence « Créer des outils et applications informatiques pour les R&T » à travers des mises en situations, jeux de rôle, dialogues qui permettent la prise de parole en continu et en interaction, en développant les compétences de compréhension dans un contexte professionnel technique.

Contenus :

- Communiquer avec un client/collaborateur à l'oral et/ou à l' écrit. Exemples : courriel, conversation téléphonique, visio-conférence, réunion, débat/argumentation, exposé technique, rapport d'activité, documentation technique
- Présenter son parcours et ses souhaits professionnels à l'oral et à l'écrit (lien avec le portfolio), comme par exemple au travers de : CV, lettre de motivation, entretien, profil réseau professionnel...
- Découvrir le monde de l'entreprise et les métiers R&T
- Faire un exposé technique
- Développer le vocabulaire technique des domaines cibles
- Renforcer ses compétences linguistiques et phonologiques

Anglais de spécialité adapté aux parcours.

Préconisations de mise en oeuvre :

- Télécollaboration, télétandem, EMILE
- Mobilité à l'étranger (séjour linguistique, stage, semestre)
- Les ressources d'anglais seront utiles et à mettre en oeuvre dans le PPP et portfolio notamment sur le volet internationale

Apprentissages critiques ciblés :

- AC21.02 | Configurer et expliquer une politique simple de QoS et les fonctions de base de la sécurité d'un réseau
- AC21.06 | Travailler en équipe pour développer ses compétences professionnelles
- AC22.05 | Capacité à questionner un cahier des charges RT
- AC23.02 | Développer une application à partir d'un cahier des charges donné, pour le Web ou les périphériques mobiles

Mots clés :

Communication écrite et orale professionnelle – Anglais technique de spécialité

Volume horaire :

Volume horaire défini nationalement : 20 heures dont 10 heures de TP

1.3.12. Ressource R3.12 : Expression-Culture-Communication professionnelles : Savoir collaborer

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 3.01 | Mettre en oeuvre un système de transmission
- SAÉ 3.02 | Développer des applications communicantes
- SAÉ 3.Cyber.03 | Concevoir un réseau informatique sécurisé multi-sites
- SAÉ 3.Cyber.04 | Découvrir le pentesting
- PORTFOLIO | Portfolio

Descriptif :

Contexte et ancrage professionnel :

Un objectif de cette ressource est de viser l'insertion professionnelle et plus directement liée au stage et à la recherche de stage. Pour les étudiants déjà en poste (apprentissage, formation continue, ...), la ressource permettra de travailler l'intégration dans l'entreprise et la communication au sein de celle-ci.

Contenus :

En tout premier lieu et pour les étudiants concernés, la recherche de stage est l'élément fondamental de ce semestre avec les activités suivantes :

- Analyse du type de candidature : spontanée ou en réponse à une offre ;
- Rédaction et mise en forme du CV et de la lettre de motivation ;
- Rédaction de l'e-mail de motivation (format court) ;
- Préparation aux entretiens ;
- Simulation d'entretiens tant en présentiel, qu'à distance ou même téléphoniques.

Les étudiants doivent s'intégrer dans leur milieu professionnel avec par exemple tout ou une partie des contenus suivants :

- Communiquer en entreprise : c'est quoi ? Pourquoi ? Comment ?
- S'exprimer formellement, remédiation (Projet Voltaire, Ecri+, ...);
- Préparer une réunion, rédiger un e-mail d'invitation ;
- Pouvoir argumenter à partir de données objectives ;
- Vulgariser un contenu scientifique ou technique ;
- Apprendre à gérer ses émotions dans un cadre professionnel ;
- Apprendre à contextualiser : connaissance de l'histoire des télécoms, de l'évolution de la sécurité des systèmes d'information, histoire de l'informatique (sous forme d'exposé, de fiche de lecture d'un ouvrage scientifique, technique, littéraire, documentaire), ... ;
- Comprendre les usages sociaux et politiques (au sens large) de l'Internet ;
- Utiliser à bon escient les données, les droits d'auteur, le droit à l'image, ...

Apprentissages critiques ciblés :

- AC21.06 | Travailler en équipe pour développer ses compétences professionnelles
- AC22.05 | Capacité à questionner un cahier des charges RT
- AC23.02 | Développer une application à partir d'un cahier des charges donné, pour le Web ou les périphériques mobiles

Mots clés :

Insertion professionnelle – Vulgarisation – Contextualisation – Culture générale – Culture scientifique et technologique – Stage – CV – Lettre de motivation – Entretien

Volume horaire :

Volume horaire défini nationalement : 20 heures dont 10 heures de TP

1.3.13. Ressource R3.13 : Projet Personnel et Professionnel

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé
- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 3.01 | Mettre en oeuvre un système de transmission
- SAÉ 3.02 | Développer des applications communicantes
- SAÉ 3.Cyber.03 | Concevoir un réseau informatique sécurisé multi-sites
- SAÉ 3.Cyber.04 | Découvrir le pentesting
- PORTFOLIO | Portfolio

Descriptif :

[1] Définir son profil, en partant de ses appétences, de ses envies et asseoir son choix professionnel notamment au travers de son parcours

- Connaissance de soi tout au long de la sa formation
- Modalités d'admissions (école et entreprise)
- Initiation à la veille informationnelle sur un secteur d'activité, une entreprise, les innovations, les technologies...
- Quels sont les différents métiers possibles avec les parcours proposés

[2] Construire un(des) projet(s) professionnel(s) en définissant une stratégie personnelle pour le/les réaliser

- Identifier les métiers associés au(x) projet(s) professionnel(s)
- Construire son parcours de formation en adéquation avec son/ses projet(s) professionnel(s) (spécialité et modalité en alternance ou initiale, réorientation, internationale, poursuite d'études, insertion professionnelle)
- Découvrir la pluralité des parcours pour accéder à un métier : Poursuite d'études et passerelles en B.U.T.2 et B.U.T.3 (tant au national qu'à l'international), VAE, formation tout au long de la vie, entrepreneuriat

[3] Analyser les métiers envisagés : postes, types d'organisation, secteur, environnement professionnel.

- Les secteurs professionnels
- Les métiers représentatifs du secteur
- Quels sont les métiers possibles avec le parcours choisi

[4] Mettre en place une démarche de recherche de stage et d'alternance et les outils associés

- Formaliser les acquis personnels et professionnels de l'expérience du stage [connaissance de soi, choix de domaine et de métier/découverte du monde l'entreprise, réadaptation des stratégies de travail dans la perspective de la 3e année)
- Accompagnement à la recherche de stage, alternance et job étudiant (en lien avec formation)
- Développer une posture professionnelle adaptée
- Technique de recherche de stage ou d'alternance : rechercher une offre, l'analyser, élaborer un CV & LM adaptés. Se préparer à l'entretien. Développer une méthodologie de suivi de ses démarches
- Gérer son identité numérique et e-réputation

Le Projet Personnel et Professionnel du semestre 3 fait logiquement suite à celui du semestre 2 pour engager les démarches d'insertion professionnelle (stage) : le profil personnel et professionnel construit par chaque étudiant est désormais mis à jour et exploité afin de fournir les CV et lettre de motivation attendus, et de préparer l'entretien de motivation. Dans cette perspective de préparation à l'insertion professionnelle, l'étudiant découvre les codes et usages de l'offre de stage ou d'emploi, confronte son profil à l'offre professionnelle dans son domaine et se positionne en fonction des entreprises et des missions possibles.

Contenus :

- Mettre à jour son profil personnel et professionnel (job d'été ; regard augmenté en maturité, connaissances et compétences)
- Mobiliser les techniques d'insertion professionnelle dans le cadre d'une recherche de stage ou d'un contrat d'alternance

- Rechercher une ou plusieurs offres de stage ou d'emploi et les comprendre : décryptage des termes et expressions, acronymes d'usage...
- Analyser et commenter les offres : caractérisation de l'émetteur, implicites, déduction de compétences techniques ou transversales, capacité à synthétiser les missions proposées...
- Se positionner par rapport à une offre : degré de maîtrise des compétences citées, adéquation personnelle avec les modalités d'organisation du travail, adéquation de l'expérience visée avec le projet personnel et professionnel de l'étudiant...
- Être capable d'argumenter de manière précise et justifiée afin de valoriser son profil personnel et professionnel en rapport avec une offre choisie

Prolongements possibles :

- Construction des outils d'insertion professionnelle en ECCP (construction du CV et de la lettre de motivation, techniques de l'entretien)
- Construction ou amélioration de son réseau professionnel, de sa visibilité numérique, de son portfolio en tant que présentation destinée à une entreprise

Apprentissages critiques ciblés :

- AC21.01 | Configurer et dépanner le routage dynamique dans un réseau
- AC21.02 | Configurer et expliquer une politique simple de QoS et les fonctions de base de la sécurité d'un réseau
- AC21.03 | Déployer des postes clients et des solutions virtualisées adaptées à une situation donnée
- AC21.04 | Déployer des services réseaux avancés
- AC21.05 | Identifier les réseaux opérateurs et l'architecture d'Internet
- AC21.06 | Travailler en équipe pour développer ses compétences professionnelles
- AC22.01 | Déployer et caractériser des systèmes de transmissions complexes
- AC22.02 | Mettre en place un accès distant sécurisé
- AC22.03 | Mettre en place une connexion multi-site via un réseau opérateur
- AC22.04 | Déployer des réseaux d'accès des opérateurs
- AC22.05 | Capacité à questionner un cahier des charges RT
- AC23.01 | Automatiser l'administration système avec des scripts
- AC23.02 | Développer une application à partir d'un cahier des charges donné, pour le Web ou les périphériques mobiles
- AC23.03 | Utiliser un protocole réseau pour programmer une application client/serveur
- AC23.04 | Installer, administrer un système de gestion de données
- AC23.05 | Accéder à un ensemble de données depuis une application et/ou un site web
- AC24.01Cyber | Connaître et utiliser les bonnes pratiques et les recommandations de cybersécurité
- AC24.02Cyber | Mettre en œuvre les outils fondamentaux de sécurisation d'une infrastructure du réseau
- AC24.03Cyber | Sécuriser les services
- AC24.04Cyber | Choisir les outils cryptographiques adaptés au besoin fonctionnel du système d'information
- AC24.05Cyber | Connaître les différents types d'attaque
- AC24.06Cyber | Comprendre des documents techniques en anglais
- AC25.01Cyber | Administrer les protections contre les logiciels malveillants
- AC25.02Cyber | Prendre en main des outils de test de pénétration réseau/système

Mots clés :

Insertion professionnelle – Stage – Profil personnel et professionnel

Volume horaire :

Volume horaire défini nationalement : 8 heures dont 4 heures de TP

1.3.14. Ressource R3.14 : Analyse de Fourier

Compétences ciblées :

- Connecter les entreprises et les usagers

SAÉ au sein desquelles la ressource peut être mobilisée et combinée :

- SAÉ 3.01 | Mettre en oeuvre un système de transmission

Descriptif :

Contexte et ancrage professionnel :

Les systèmes de transmission doivent être adaptés aux supports de transmission, en particulier à leur bande passante. Un filtrage, une transposition de fréquence voire un échantillonnage du signal source sont généralement mis en œuvre. La maîtrise des outils d'analyse fréquentielle est donc nécessaire.

On veillera à montrer l'intérêt des concepts présentés pour modéliser les systèmes électroniques et on choisira de préférence des exercices en lien avec l'électronique et les télécommunications.

Contenus :

- Séries de Fourier (réelles et complexes)
 - introduction aux séries et aux séries de fonctions
 - harmoniques
 - spectre de puissance
 - Parseval
- Transformée de Fourier
 - propriétés : linéarité, dilatation, dérivation, retard, multiplication par une exponentielle complexe
 - TF usuelles (porte, triangle, exponentielle décroissante, gaussienne)
 - densité spectrale d'énergie
 - Parseval
 - distribution de Dirac
 - TF des signaux périodiques
- Convolution et applications
 - produit de convolution
 - filtrage
 - transposition de fréquence
 - échantillonnage
 - peigne de Dirac
 - théorème d'échantillonnage

Préconisations de mise en oeuvre :

Transformée de Fourier discrète, FFT

Apprentissages critiques ciblés :

- AC22.01 | Déployer et caractériser des systèmes de transmissions complexes
- AC22.05 | Capacité à questionner un cahier des charges RT

Mots clés :

Fréquence – Analyse fréquentielle – Filtrage – Échantillonnage

Volume horaire :

Volume horaire défini nationalement : 19 heures

1.3.15. Ressource R3.15 : Gestion de projet 2 : Utiliser les méthodes de gestion de projet

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 3.01 | Mettre en oeuvre un système de transmission
- SAÉ 3.02 | Développer des applications communicantes
- SAÉ 3.Cyber.03 | Concevoir un réseau informatique sécurisé multi-sites
- SAÉ 3.Cyber.04 | Découvrir le pentesting
- PORTFOLIO | Portfolio

Descriptif :

Contexte et ancrage professionnel :

Le professionnel R&T peut être impliqué dans différents projets l'amenant à travailler en équipe. Pour être opérationnel sur ce plan, l'étudiant doit être capable de s'aider d'outils logiciels d'organisation du travail et de travail collaboratif. Il s'agit d'un moyen, et non d'une fin. La mise en place et la gestion d'un projet sont amenées de manière plus précise et plus technique en 2e année de B.U.T.

Contenus :

- Savoir lire/décoder et construire un cahier des charges simple via l'analyse des besoins/d'une commande.
- Se projeter, conceptualiser, définir et hiérarchiser les tâches à réaliser à l'aide d'outils adaptés (cartes mentales, infographies, etc.).
- Adapter finement une solution à un contexte défini (objectifs, contraintes liées au contexte, aux ressources humaines/matérielles).
- Être capable de faire preuve de créativité pour se lancer dans un projet ou trouver des solutions innovantes (intrapreneuriat).
- Valider une idée projet.
- Prendre sa place dans une équipe en connaissant les différents rôles d'une équipe projet.
- Apprendre à organiser son travail et celui de l'équipe à partir d'outils de planification de types Gantt ou PERT (qui fait quoi, quand, comment ?).
- Organiser des réunions de projet (avec prise de notes, compte rendu, actions à réaliser).
- Actualiser/faire évoluer l'organisation du travail en s'initiant à des méthodes de types agilité/Scrum/réitération/production immédiate.
- Apprendre à faire un bilan régulier sur l'avancée d'un projet à un client ou un référent : points bloquants, solutions apportées, Lean management/amélioration continue (appliquer la critique constructive dans l'intérêt du projet ; analyse).
- Prendre en compte des coûts approximatifs et les justifier.
- Être conscient de son éco-responsabilité et intégrer la notion de développement durable (bonnes pratiques, choix des matériels, valeur écologique/responsable apportée au projet, manière de développer/coder).

L'utilisation des ressources de gestion de projets dans les SAÉ est l'objet d'une attention particulière.

Apprentissages critiques ciblés :

- AC21.06 | Travailler en équipe pour développer ses compétences professionnelles
- AC22.05 | Capacité à questionner un cahier des charges RT
- AC23.02 | Développer une application à partir d'un cahier des charges donné, pour le Web ou les périphériques mobiles

Mots clés :

Organisation – Planification – Créativité – Adaptabilité – Découverte des méthodes de management de projet

Volume horaire :

Volume horaire défini nationalement : 8 heures dont 2 heures de TP

1.3.16. Ressource R3.Cyber.16 : Méthodologie du pentesting

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 3.Cyber.03 | Concevoir un réseau informatique sécurisé multi-sites
- SAÉ 3.Cyber.04 | Découvrir le pentesting

Descriptif :

Contexte et ancrage professionnel :

Les étudiants apprendront à connaître et à utiliser l'ensemble des outils et sites permettant :

- d'obtenir des informations sur une cible désignée (Whois, DNS, nmap, ...) afin de produire une cartographie de son SI,
- de mettre en évidence certaines vulnérabilités (avec les outils par exemple Hydra, Metasploit, openVAS, ...), tout ceci dans un esprit de hacking éthique, dans le respect de la réglementation en vigueur et dans un environnement d'exécution privé.

S'il est possible de rester dans un tel contexte, les étudiants pourront aller jusqu'à l'exploitation des vulnérabilités ainsi mises en évidence.

Contenus :

Cette ressource pourra comporter :

- une introduction à la cybersécurité (rappel de la SAÉ1.01 "Se sensibiliser à l'hygiène informatique et à la cybersécurité") ;
- Reconnaissance passive : utilisation des informations accessibles publiquement (base whois, interrogation du DNS, recherches sur Internet, cert-fr, cve-details, ...);
- Reconnaissance active : utilisation d'outils ou techniques pour approfondir la collecte d'informations (scan de ports, ingénierie sociale, écoute de réseau, ...);
- Recherche de vulnérabilités (analyse des versions de services, attaque de mots de passe par dictionnaire, Hydra, Metasploit, OpenVAS, OWASP, scapy, ...).

Apprentissages critiques ciblés :

- AC24.01Cyber | Connaître et utiliser les bonnes pratiques et les recommandations de cybersécurité
- AC24.05Cyber | Connaître les différents types d'attaque
- AC24.06Cyber | Comprendre des documents techniques en anglais
- AC25.01Cyber | Administrer les protections contre les logiciels malveillants
- AC25.02Cyber | Prendre en main des outils de test de pénétration réseau/système

Mots clés :

Cybersécurité – Ethical hacking – Pentesting – Reconnaissance – Ingénierie sociale scan de port – Écoute de réseau – Vulnérabilité – Exploitation de vulnérabilité

Volume horaire :

Volume horaire défini nationalement : 19 heures dont 11 heures de TP

2. Semestre 4

2.1. Tableau croisé

Ce tableau explicite les correspondances entre les compétences, les apprentissages critiques, les SAÉ et les ressources programmés dans le semestre.

Les SAÉ et les ressources ainsi identifiées pour chaque UE participent à son obtention, et en ce sens doivent faire l'objet d'une évaluation, à l'exception de la démarche portfolio des semestres impairs.

Ce tableau détaille par ailleurs la répartition du volume horaire global des heures d'enseignement encadré de chaque semestre, à savoir :

- le volume horaire alloué à l'ensemble des SAÉ ;
- le volume de chaque ressource définie nationalement dont les heures TP ;
- le volume horaire, dont les heures TP, relevant d'une partie de l'adaptation locale et pouvant être affecté de manière non exclusive soit aux SAÉ, soit aux ressources définies nationalement ou localement.

			AC															
			SAÉ 4 Cyber 01 Sécuriser un système d'information															
			STAGE Cyber Stage															
			PORTFOLIO Portfolio															
Administre	AC21.01		X	X														
	AC21.02		X	X	X													
	AC21.03		X	X														
	AC21.04		X	X	X													
	AC21.05		X	X														
	AC21.06		X	X							X	X	X					
Connecter	AC22.01		X	X		X	X	X						X				
	AC22.02		X	X	X									X				
	AC22.03		X	X	X									X				
	AC22.04		X	X				X						X				
	AC22.05		X	X							X	X	X					
Programmer	AC23.01		X	X					X					X				
	AC23.02		X	X						X	X	X						
	AC23.03		X	X								X						
	AC23.04		X	X								X						
	AC23.05		X	X								X						
Sécuriser	AC24.01Cyber		X	X	X							X	X					
	AC24.02Cyber		X	X	X							X	X					
	AC24.03Cyber		X	X	X							X		X				
	AC24.04Cyber		X	X	X							X		X				
	AC24.05Cyber		X	X	X							X	X					
	AC24.06Cyber		X	X	X							X	X	X				
Surveiller	AC25.01Cyber		X	X	X							X						
	AC25.02Cyber		X	X	X							X	X	X				
Volume total					18	15	18	20	18	11	11	5	9	8	11	144		
Dont TP					12	6	8	9	9	5	5	0	4	4	6	68		
Adaptation Locale (SAÉ)					39											39		
Adaptation Locale (Ressources ou SAÉ)																57		
TP Adaptation locale																45		

2.2. Fiches Situations d'apprentissage et d'évaluation (SAÉ)

2.2.1. SAÉ 4.Cyber.01 : Sécuriser un système d'information

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé

Objectifs et problématique professionnelle :

Le professionnel R&T spécialisé dans la Cybersécurité se doit de sécuriser un réseau multi-sites tant au niveau des équipements que des services.

Descriptif générique :

Afin de procéder à la sécurisation des équipements et des services, le professionnel Cyber se doit de :

- sécuriser l'infrastructure locale existante et ce de manière ascendante notamment en commençant par les éléments actifs de couches supérieures à 3, pour finir par les différents services proposés (DNS, Web, ...);
- ajouter des équipements spécialisés ;
- utiliser des outils cryptographiques judicieusement choisis pour sécuriser les services (authentification, certificats, ...);
- se référer aux recommandations de l'ANSSI pour sécuriser un système d'information.

Cette SAÉ fait suite à la SAÉ3.03Cyber "Concevoir un réseau informatique sécurisé multi-sites" qui a débouché sur la conception d'un réseau multi-sites.

Apprentissages critiques :

- AC24.01Cyber | Connaître et utiliser les bonnes pratiques et les recommandations de cybersécurité
- AC24.02Cyber | Mettre en œuvre les outils fondamentaux de sécurisation d'une infrastructure du réseau
- AC24.03Cyber | Sécuriser les services
- AC24.04Cyber | Choisir les outils cryptographiques adaptés au besoin fonctionnel du système d'information
- AC24.05Cyber | Connaître les différents types d'attaque
- AC24.06Cyber | Comprendre des documents techniques en anglais
- AC25.01Cyber | Administre les protections contre les logiciels malveillants
- AC25.02Cyber | Prendre en main des outils de test de pénétration réseau/système

Ressources mobilisées et combinées :

- R4.06 | Anglais professionnel 2
- R4.07 | Expression-Culture-Communication professionnelles : Préparer l'insertion professionnelle
- R4.08 | Projet Personnel et Professionnel
- R4.Cyber.09 | Sécurité des réseaux LAN
- R4.Cyber.10 | Cryptographie
- R4.Cyber.11 | Sécurisation de services réseaux

Volume horaire :

Volume horaire : à définir localement par chaque IUT

2.2.2. STAGE.Cyber : Stage

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé
- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

Objectifs et problématique professionnelle :

Le B.U.T. R&T a pour objectif de former des techniciens supérieurs polyvalents dotés de fortes compétences technologiques dans les domaines des réseaux informatiques, des télécommunications et de l'informatique.

L'entreprise doit être en capacité de proposer des mises en situations significatives liées aux compétences de déploiement, d'installation ou de maintien en conditions opérationnelles sur :

- des infrastructures réseaux sécurisées ;
- des infrastructures de télécommunications ;
- des réseaux d'objets connectés ;
- des solutions logicielles sur des systèmes Cloud ;
- de pilotage de projet réseaux ou télécommunications.

Les activités développées devront être en adéquation, si possible, avec le projet professionnel et le choix de parcours de l'étudiant. Il devra en outre développer, appliquer, et consolider ses savoirs-faire et ses savoirs-être :

- s'intégrer dans l'entreprise : découvrir les aspects organisationnels, les codes de l'entreprise, l'interaction avec ses collègues, responsables ;
- développer ses connaissances des outils, des méthodes de travail, de la gestion et de la réalisation des missions confiées ;
- développer son autonomie, son esprit d'initiative ;
- rendre compte à l'écrit et à l'oral de son activité, de ses missions en conduisant une réflexion structurée et rigoureuse.

Apprentissages critiques :

- AC21.01 | Configurer et dépanner le routage dynamique dans un réseau
- AC21.02 | Configurer et expliquer une politique simple de QoS et les fonctions de base de la sécurité d'un réseau
- AC21.03 | Déployer des postes clients et des solutions virtualisées adaptées à une situation donnée
- AC21.04 | Déployer des services réseaux avancés
- AC21.05 | Identifier les réseaux opérateurs et l'architecture d'Internet
- AC21.06 | Travailler en équipe pour développer ses compétences professionnelles
- AC22.01 | Déployer et caractériser des systèmes de transmissions complexes
- AC22.02 | Mettre en place un accès distant sécurisé
- AC22.03 | Mettre en place une connexion multi-site via un réseau opérateur
- AC22.04 | Déployer des réseaux d'accès des opérateurs
- AC22.05 | Capacité à questionner un cahier des charges RT
- AC23.01 | Automatiser l'administration système avec des scripts
- AC23.02 | Développer une application à partir d'un cahier des charges donné, pour le Web ou les périphériques mobiles
- AC23.03 | Utiliser un protocole réseau pour programmer une application client/serveur
- AC23.04 | Installer, administrer un système de gestion de données
- AC23.05 | Accéder à un ensemble de données depuis une application et/ou un site web
- AC24.01Cyber | Connaître et utiliser les bonnes pratiques et les recommandations de cybersécurité
- AC24.02Cyber | Mettre en œuvre les outils fondamentaux de sécurisation d'une infrastructure du réseau
- AC24.03Cyber | Sécuriser les services
- AC24.04Cyber | Choisir les outils cryptographiques adaptés au besoin fonctionnel du système d'information
- AC24.05Cyber | Connaître les différents types d'attaque
- AC24.06Cyber | Comprendre des documents techniques en anglais
- AC25.01Cyber | Administrer les protections contre les logiciels malveillants
- AC25.02Cyber | Prendre en main des outils de test de pénétration réseau/système

Ressources mobilisées et combinées :

- R4.01 | Infrastructures de sécurité
- R4.02 | Transmissions avancées
- R4.03 | Physique des télécoms
- R4.04 | Réseaux cellulaires
- R4.05 | Automatisation des tâches d'administration
- R4.06 | Anglais professionnel 2
- R4.07 | Expression-Culture-Communication professionnelles : Préparer l'insertion professionnelle
- R4.08 | Projet Personnel et Professionnel
- R4.Cyber.09 | Sécurité des réseaux LAN
- R4.Cyber.10 | Cryptographie
- R4.Cyber.11 | Sécurisation de services réseaux

2.2.3. PORTFOLIO : Démarche portfolio

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé
- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

Objectifs et problématique professionnelle :

Au semestre 4, la démarche portfolio permettra d'évaluer l'étudiant dans son processus d'acquisition des niveaux de compétences de la deuxième année du B.U.T., et dans sa capacité à en faire la démonstration par la mobilisation d'éléments de preuve argumentés et sélectionnés. L'étudiant devra donc engager une posture réflexive et de distanciation critique en cohérence avec le parcours suivi et le degré de complexité des niveaux de compétences ciblés, tout en s'appuyant sur l'ensemble des mises en situation proposées dans le cadre des SAÉ de deuxième année.

Descriptif générique :

Prenant n'importe quelle forme, littérale, analogique ou numérique, la démarche portfolio pourra être menée dans le cadre d'ateliers au cours desquels l'étudiant retracera la trajectoire individuelle qui a été la sienne durant la seconde année du B.U.T. au prisme du référentiel de compétences et du parcours suivi, tout en adoptant une posture propice à une analyse distanciée et intégrative de l'ensemble des SAÉ.

Ressources mobilisées et combinées :

- R4.06 | Anglais professionnel 2
- R4.07 | Expression-Culture-Communication professionnelles : Préparer l'insertion professionnelle
- R4.08 | Projet Personnel et Professionnel

Volume horaire :

Volume horaire : à définir localement par chaque IUT

2.3. Fiches Ressources

2.3.1. Ressource R4.01 : Infrastructures de sécurité

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- STAGE.Cyber | Stage

Descriptif :

Contexte et ancrage professionnel :

Les étudiants devront être capables de déployer et configurer une architecture de réseau sécurisé. Ils devront également choisir les bons outils de cryptologie adaptés à chaque fonctionnalité recherchée.

Contenus :

- Équipements dédiés à la sécurité
- Bases de cryptographie asymétrique (chiffrement asymétrique, certificats, signature, pki, ...)
- Services et applications sécurisées (SSL, HTTPS, ...)
- Architecture réseau sécurisée (DMZ, proxy, reverse-proxy, ...)
- Approfondissement des mécanismes de filtrage et de contrôle d'accès (Proxy-Firewall, NAT, ACL...)
- Tunnels VPN

Penser à systématiser l'utilisation de logiciels d'analyse de trames (WireShark, TCPDUMP, ...) pour les TP.

Apprentissages critiques ciblés :

- AC21.02 | Configurer et expliquer une politique simple de QoS et les fonctions de base de la sécurité d'un réseau
- AC21.04 | Déployer des services réseaux avancés
- AC22.02 | Mettre en place un accès distant sécurisé
- AC22.03 | Mettre en place une connexion multi-site via un réseau opérateur

Mots clés :

Cybersécurité – Cryptologie – Certificat – Signature – Pki – VPN – DMZ – Proxy – Services sécurisés – ACL – Firewall

Volume horaire :

Volume horaire défini nationalement : 18 heures dont 12 heures de TP

2.3.2. Ressource R4.02 : Transmissions avancées

Compétence ciblée :

- Connecter les entreprises et les usagers

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- STAGE.Cyber | Stage

Descriptif :

Contexte et ancrage professionnel :

L'étudiant devra être capable de maîtriser les éléments d'une chaîne de transmission avancée.

Contenus :

- Propagation à trajets multiples et interférences inter symboles
- Modulation à étalement de spectre, OFDM et multiplexages associés CDMA et OFDMA
- MIMO
- Correction d'erreurs et mesures de taux d'erreurs
- Veille technologique (conférence, webinaire, ...)

Apprentissage critique ciblé :

- AC22.01 | Déployer et caractériser des systèmes de transmissions complexes

Mots clés :

OFDM – CDMA – MIMO – IES – TEB/BER – FEC

Volume horaire :

Volume horaire défini nationalement : 15 heures dont 6 heures de TP

2.3.3. Ressource R4.03 : Physique des télécoms

Compétence ciblée :

- Connecter les entreprises et les usagers

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- STAGE.Cyber | Stage

Descriptif :

Contexte et ancrage professionnel :

L'étudiant devra être capable de caractériser, mesurer et analyser et déployer des dispositifs radio ou optiques indispensables aux transmissions modernes.

Contenus :

- Propagation des ondes, Onde incidente, transmise et réfléchie, Modes de propagation, Dispositifs optiques/photoniques : émetteurs et amplificateurs optiques
- Diagramme rayonnement, gain d'antenne, types d'antennes
- Guides d'ondes, adaptation d'impédance, abaque de Smith
- Bilan de liaison

Apprentissage critique ciblé :

- AC22.01 | Déployer et caractériser des systèmes de transmissions complexes

Mots clés :

Propagation des ondes – Modes – Ondes stationnaires – ROS/TOS – Diagramme de rayonnement – Gain de puissance – Bilan de liaison – Optique – Photonique

Volume horaire :

Volume horaire défini nationalement : 18 heures dont 8 heures de TP

2.3.4. Ressource R4.04 : Réseaux cellulaires

Compétence ciblée :

- Connecter les entreprises et les usagers

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- STAGE.Cyber | Stage

Descriptif :

Contexte et ancrage professionnel :

L'étudiant devra être capable d'analyser, de mesurer ou de déployer des réseaux cellulaires

Contenus :

- Réseaux d'opérateurs pour mobiles
- Connaître l'architecture des réseaux mobiles actuels (2G-5G, xG), notions de cœur de réseau
- Connaître les débits et les services offerts par les réseaux
- Connaître les bases de la couche radio et les procédures d'accès au réseau.
- Connaître les critères d'évaluation de la qualité de service dans un réseau cellulaire (couverture/cartographie, choix des protocoles, services,...)

Prérequis :

- R4.02 | Transmissions avancées
- R4.03 | Physique des télécoms

Apprentissages critiques ciblés :

- AC22.01 | Déployer et caractériser des systèmes de transmissions complexes
- AC22.04 | Déployer des réseaux d'accès des opérateurs

Mots clés :

2G – 3G – 4G – 5G – Réseaux mobiles – Réseaux cellulaires – Couche radio – Cartographie – LTE – LTE Advanced – NR (new radio) – Hand Over – NodeB

Volume horaire :

Volume horaire défini nationalement : 20 heures dont 9 heures de TP

2.3.5. Ressource R4.05 : Automatisation des tâches d'administration

Compétence ciblée :

- Créer des outils et applications informatiques pour les R&T

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- STAGE.Cyber | Stage

Descriptif :

Contexte et ancrage professionnel :

Afin d'améliorer l'administration d'un parc informatique ou la surveillance des infrastructures réseaux, le professionnel R&T est amené à développer des scripts permettant le relevé et le traitement automatique des paramètres.

Contenus :

Seront abordés :

- L'automatisation,
- La gestion de configuration,
- La recherche d'information système et la gestion de la base des registres,
- L'ordonnancement des tâches,
- La gestion des erreurs et la manipulation des journaux d'événement,
- La création de scripts avancés,
- La sécurité et la signature des scripts,
- La gestion des mémoires et des entrées/sorties,
- L'application des expressions régulières pour l'automatisation.

Ces notions seront abordées autant du point de vue Linux que Windows en utilisant potentiellement les environnements technologiques Powershell ou shell.

Ces notions pourront être appliquées à la gestion de conteneurs. Il sera possible d'introduire ici l'usage des outils d'automatisation tels que Ansible et de poursuivre la prise en main de l'environnement Git.

Apprentissage critique ciblé :

- AC23.01 | Automatiser l'administration système avec des scripts

Mots clés :

Automatisation – Scripts – Expressions régulières – Journaux d'événements – Administration système

Volume horaire :

Volume horaire défini nationalement : 18 heures dont 9 heures de TP

2.3.6. Ressource R4.06 : Anglais professionnel 2

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 4.Cyber.01 | Sécuriser un système d'information
- STAGE.Cyber | Stage
- PORTFOLIO | Portfolio

Descriptif :

Contexte et ancrage professionnel :

Cette ressource apporte le socle de connaissances langagières pour les compétences de cœur de métier « Administrer les réseaux et l'Internet » et « Connecter les entreprises et les usagers ». Elle contribue aussi à la compétence « Créer des outils et applications informatiques pour les R&T » à travers des mises en situations, jeux de rôle, dialogues qui permettent la prise de parole en continu et en interaction, en développant les compétences de compréhension dans un contexte professionnel technique.

Contenus :

- Participer à/conduire une réunion
- Faire un compte-rendu
- Rechercher, comprendre, synthétiser, vulgariser et présenter des données techniques à l'écrit et à l'oral,
- Approfondir son vocabulaire de spécialité
- Renforcer ses compétences linguistiques et phonologiques
- Comprendre et rédiger une documentation technique

Anglais de spécialité adapté aux parcours.

Préconisations de mise en œuvre :

- Télécollaboration, télétandem, EMILE
- Mobilité à l'étranger (séjour linguistique, stage, semestre)
- Les ressources d'anglais seront utiles et à mettre en œuvre dans le PPP et portfolio notamment sur le volet internationale
- Portfolio avec des traces dans une langue étrangère dont l'anglais

Apprentissages critiques ciblés :

- AC21.02 | Configurer et expliquer une politique simple de QoS et les fonctions de base de la sécurité d'un réseau
- AC21.06 | Travailler en équipe pour développer ses compétences professionnelles
- AC22.05 | Capacité à questionner un cahier des charges RT
- AC23.02 | Développer une application à partir d'un cahier des charges donné, pour le Web ou les périphériques mobiles

Mots clés :

Communication écrite et orale professionnelle – Anglais technique de spécialité

Volume horaire :

Volume horaire défini nationalement : 11 heures dont 5 heures de TP

2.3.7. Ressource R4.07 : Expression-Culture-Communication professionnelles : Préparer l'insertion professionnelle

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 4.Cyber.01 | Sécuriser un système d'information
- STAGE.Cyber | Stage
- PORTFOLIO | Portfolio

Descriptif :

Contexte et ancrage professionnel :

En amont de la première immersion professionnelle R&T, un objectif de cette ressource est l'acquisition d'outils permettant de collaborer efficacement au sein d'une organisation.

Préconisation de contenus :

- Lire et écrire un cahier des charges ;
- Lire un appel d'offres ;
- Expliquer à des néophytes ou à des clients une démarche technique ;
- Construire un support percutant au contenu immédiatement lisible ;
- Apprendre à négocier.

Dans la démarche de l'étudiant, tout ou une partie des thèmes suivants pourront être abordés :

- Prendre conscience des risques psycho-sociaux (manipulation, aliénation, exploitation...) ;
- Appréhender les situations de conflit ;
- Appréhender le changement ;
- Prendre en compte les évolutions sociales et environnementales ;
- Agir de manière éco-responsable : sensibilisation à une éthique numérique (choix d'une activité responsable, économie low-tech, etc.) ;
- Lutter contre la pollution numérique : Green IT, écologie, éco-conception, développement durable et transverse, recyclage systématique, utilisation de matériels durables, conscience critique de la surconsommation.
- Réfléchir aux enjeux économiques, géo-politiques et industriels du dérèglement climatique ;
- Utiliser du matériel et des logiciels équitables (open-source par exemple) ;
- Soigner son image numérique ;
- Développer une approche de la citoyenneté et de la responsabilité citoyenne : enjeux de la liberté d'expression en contexte de laïcité ;
- Appréhender les enjeux de l'intelligence artificielle, de la numérisation sociale (GAFAM, big data, ...).

Une partie des travaux pourra être consacrée à un entraînement au rapport écrit et à la soutenance orale sous forme de rédaction d'analyse, de résumé, de comptes-rendus, de présentations orales courtes (seul ou en groupe).

Apprentissages critiques ciblés :

- AC21.06 | Travailler en équipe pour développer ses compétences professionnelles
- AC22.05 | Capacité à questionner un cahier des charges RT
- AC23.02 | Développer une application à partir d'un cahier des charges donné, pour le Web ou les périphériques mobiles

Mots clés :

Gestion de conflits – Conduite du changement – Ethique numérique – Enjeux politiques et environnementaux – Approches communicationnelles et socio-culturelles

Volume horaire :

Volume horaire défini nationalement : 11 heures dont 5 heures de TP

2.3.8. Ressource R4.08 : Projet Personnel et Professionnel

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé
- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 4.Cyber.01 | Sécuriser un système d'information
- STAGE.Cyber | Stage
- PORTFOLIO | Portfolio

Descriptif :

[1] Définir son profil, en partant de ses appétences, de ses envies et asséoir son choix professionnel notamment au travers de son parcours

- Connaissance de soi tout au long de la sa formation
- Modalités d'admissions (école et entreprise)
- Initiation à la veille informationnelle sur un secteur d'activité, une entreprise, les innovations, les technologies...
- Quels sont les différents métiers possibles avec les parcours proposés

[2] Construire un(des) projet(s) professionnel(s) en définissant une stratégie personnelle pour le/les réaliser

- Identifier les métiers associés au(x) projet(s) professionnel(s)
- Construire son parcours de formation en adéquation avec son/ses projet(s) professionnel(s) (spécialité et modalité en alternance ou initiale, réorientation, internationale, poursuite d'études, insertion professionnelle)
- Découvrir la pluralité des parcours pour accéder à un métier : Poursuite d'études et passerelles en B.U.T.2 et B.U.T.3 (tant au national qu'à l'international), VAE, formation tout au long de la vie, entrepreneuriat
- [3] Analyser les métiers envisagés : postes, types d'organisation, secteur, environnement professionnel.
- Les secteurs professionnels
- Les métiers représentatifs du secteur
- Quels sont les métiers possibles avec le parcours choisi

[4] Mettre en place une démarche de recherche de stage et d'alternance et les outils associés

- Formaliser les acquis personnels et professionnels de l'expérience du stage [connaissance de soi, choix de domaine et de métier/découverte du monde l'entreprise, réadaptation des stratégies de travail dans la perspective de la 3e année)
- Accompagnement à la recherche de stage, alternance et job étudiant (en lien avec formation)
- Développer une posture professionnelle adaptée
- Technique de recherche de stage ou d'alternance : rechercher une offre, l'analyser, élaborer un CV & LM adaptés. Se préparer à l'entretien. Développer une méthodologie de suivi de ses démarches
- Gérer son identité numérique et e-réputation

A l'approche du premier stage professionnel, l'étudiant doit être capable d'envisager personnellement et professionnellement sa situation de collaborateur au sein d'une organisation.

Contenus :

- Approfondir l'approche des droits et devoirs des individus en matière de numérique (CNIL, RGPD, quadrature du Net...)
- Mieux comprendre les enjeux du monde professionnel (initiation : PME, grandes entreprises, multinationales, start-up, représentation syndicale, économie, développement durable, responsabilité sociétale des entreprises...)
- Comprendre l'articulation entre sa personnalité et les enjeux du monde socio-économique en prenant conscience de ses contraintes
- Être capable de s'intégrer correctement en entreprise, dans la visée du premier stage professionnel : quels avoir-être, qu'attend-on du collaborateur-stagiaire, comment se comporter, que prendre en compte ?

Prolongements possibles :

- Passerelles et choix de poursuites d'études

- Rapport et soutenance de stage
- Accentuation et valorisation des savoir-être et soft skills

Apprentissages critiques ciblés :

- AC21.01 | Configurer et dépanner le routage dynamique dans un réseau
- AC21.02 | Configurer et expliquer une politique simple de QoS et les fonctions de base de la sécurité d'un réseau
- AC21.03 | Déployer des postes clients et des solutions virtualisées adaptées à une situation donnée
- AC21.04 | Déployer des services réseaux avancés
- AC21.05 | Identifier les réseaux opérateurs et l'architecture d'Internet
- AC21.06 | Travailler en équipe pour développer ses compétences professionnelles
- AC22.01 | Déployer et caractériser des systèmes de transmissions complexes
- AC22.02 | Mettre en place un accès distant sécurisé
- AC22.03 | Mettre en place une connexion multi-site via un réseau opérateur
- AC22.04 | Déployer des réseaux d'accès des opérateurs
- AC22.05 | Capacité à questionner un cahier des charges RT
- AC23.01 | Automatiser l'administration système avec des scripts
- AC23.02 | Développer une application à partir d'un cahier des charges donné, pour le Web ou les périphériques mobiles
- AC23.03 | Utiliser un protocole réseau pour programmer une application client/serveur
- AC23.04 | Installer, administrer un système de gestion de données
- AC23.05 | Accéder à un ensemble de données depuis une application et/ou un site web
- AC24.01Cyber | Connaître et utiliser les bonnes pratiques et les recommandations de cybersécurité
- AC24.02Cyber | Mettre en œuvre les outils fondamentaux de sécurisation d'une infrastructure du réseau
- AC24.03Cyber | Sécuriser les services
- AC24.04Cyber | Choisir les outils cryptographiques adaptés au besoin fonctionnel du système d'information
- AC24.05Cyber | Connaître les différents types d'attaque
- AC24.06Cyber | Comprendre des documents techniques en anglais
- AC25.01Cyber | Administrer les protections contre les logiciels malveillants
- AC25.02Cyber | Prendre en main des outils de test de pénétration réseau/système

Mots clés :

Insertion professionnelle – Posture professionnelle – Orientation – Organisations

Volume horaire :

Volume horaire défini nationalement : 5 heures

2.3.9. Ressource R4.Cyber.09 : Sécurité des réseaux LAN

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 4.Cyber.01 | Sécuriser un système d'information
- STAGE.Cyber | Stage

Descriptif :

Contexte et ancrage professionnel :

Les étudiants devront déployer les services et fonctionnalités fondamentales des LAN et WLAN, en tester les limites, mettre en évidence leurs faiblesses et exploiter leurs vulnérabilités. Ils devront également savoir apporter des solutions à ces problèmes mis en évidence.

Contenus :

Cette ressource pourra comporter :

- Un rappel sur les protocoles ICMP, ARP, DHCP, STP, SLAAC, DNS, WPA PSK.
- Une mise en œuvre dans le cadre de prototypes et des expériences d'attaques connues avec des outils appropriés (IP/MAC/DNS spoofing, ARP poisoning, DHCP snooping, ICMP redirect, ...)
- Des solutions sur une partie des problèmes identifiés (segmentation VLAN, routage inter-VLAN, filtrage par ACL, fonctions de sécurisation de switchs, ...)

Apprentissages critiques ciblés :

- AC24.01Cyber | Connaître et utiliser les bonnes pratiques et les recommandations de cybersécurité
- AC24.02Cyber | Mettre en œuvre les outils fondamentaux de sécurisation d'une infrastructure du réseau
- AC24.05Cyber | Connaître les différents types d'attaque
- AC24.06Cyber | Comprendre des documents techniques en anglais
- AC25.02Cyber | Prendre en main des outils de test de pénétration réseau/système

Mots clés :

Sécurité des LAN – ARP spoofing – IP/MAC/DNS spoofing – ARP poisoning – DHCP snooping – ICMP redirect

Volume horaire :

Volume horaire défini nationalement : 9 heures dont 4 heures de TP

2.3.10. Ressource R4.Cyber.10 : Cryptographie

Compétence ciblée :

- Administrer un système d'information sécurisé

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 4.Cyber.01 | Sécuriser un système d'information
- STAGE.Cyber | Stage

Descriptif :

Contexte et ancrage professionnel :

Les étudiants devront être capables de choisir les outils cryptographiques adaptés à la résolution de chaque type de problème d'authentification, de confidentialité et d'intégrité. Ils devront précisément différencier chaque famille d'outils et en connaître les usages et limites.

La cryptologie pourra être abordée par une approche algorithmique et/ou mathématique en s'appuyant par exemple sur le langage Python et les librairies standardisées.

Contenus :

- Algorithmes de cryptographie,
- Fonctions de hachage,
- Architecture PKI.

Prérequis :

- R4.01 | Infrastructures de sécurité

Apprentissages critiques ciblés :

- AC24.04Cyber | Choisir les outils cryptographiques adaptés au besoin fonctionnel du système d'information
- AC24.06Cyber | Comprendre des documents techniques en anglais

Mots clés :

Clés – Chiffrement symétrique – Asymétrique – Intégrité – Confidentialité – Authentification – Authenticité – Signature – Certificat – Fonctions mathématiques et algorithmiques

Volume horaire :

Volume horaire défini nationalement : 8 heures dont 4 heures de TP

2.3.11. Ressource R4.Cyber.11 : Sécurisation de services réseaux

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 4.Cyber.01 | Sécuriser un système d'information
- STAGE.Cyber | Stage

Descriptif :

Contexte et ancrage professionnel :

Les étudiants devront être capables d'identifier les faiblesses des services usuels d'Internet (DNS, Web, ...) et de proposer des solutions sécurisées ce qui n'exclut pas la mise en œuvre de technologies complémentaires.

Contenus :

- Étudier les vulnérabilités des services réseaux (Web, DNS,).
- Sécuriser les services réseaux (sûreté, proxy,) : les solutions étudiées reposent la plupart du temps sur l'utilisation de la cryptographie.
- Assurer la continuité de services (haute disponibilité, redondance, répartition de charge...).

Prérequis :

- R4.01 | Infrastructures de sécurité

Apprentissages critiques ciblés :

- AC24.03Cyber | Sécuriser les services
- AC24.06Cyber | Comprendre des documents techniques en anglais
- AC25.02Cyber | Prendre en main des outils de test de pénétration réseau/système

Mots clés :

TLS – DNSSEC – HTTPS – Proxy – Load Balancing

Volume horaire :

Volume horaire défini nationalement : 11 heures dont 6 heures de TP

3. Semestre 5

3.1. Tableau croisé

Ce tableau explicite les correspondances entre les compétences, les apprentissages critiques, les SAÉ et les ressources programmés dans le semestre.

Les SAÉ et les ressources ainsi identifiées pour chaque UE participent à son obtention, et en ce sens doivent faire l'objet d'une évaluation, à l'exception de la démarche portfolio des semestres impairs.

Ce tableau détaille par ailleurs la répartition du volume horaire global des heures d'enseignement encadré de chaque semestre, à savoir :

- le volume horaire alloué à l'ensemble des SAÉ ;
- le volume de chaque ressource définie nationalement dont les heures TP ;
- le volume horaire, dont les heures TP, relevant d'une partie de l'adaptation locale et pouvant être affecté de manière non exclusive soit aux SAÉ, soit aux ressources définies nationalement ou localement.

3.2. Fiches Situations d'apprentissage et d'évaluation (SAÉ)

3.2.1. SAÉ 5.01 : Concevoir, réaliser et présenter une solution technique

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

Objectifs et problématique professionnelle :

Le professionnel R&T, en charge d'un projet technique, doit assurer l'ensemble des étapes du projet en concevant, réalisant et en présentant une solution technique mariant les différentes technologies réseaux, télécommunications et informatiques. Il assure également la coordination entre les techniciens faisant partie du projet.

Descriptif générique :

Le professionnel R&T est en charge de projets et d'architectures variées dont il coordonne la conception, la maintenance et l'évolution. Il s'assure de la formation des utilisateurs et de la documentation (procédures, ...). Il présente régulièrement les évolutions de son architecture à sa hiérarchie éventuellement en langue étrangère.

Il doit faire preuve de recul quant aux solutions techniques utilisées. Il assure la veille technologique tout en facilitant les échanges et en organisant les interventions de son équipe technique (gestion de projet, méthodologie de répartition de tâches, jalons, etc.). Cette coordination doit être également pensée dans le cadre du travail collaboratif à distance (site web collaboratif, espace de stockage partagé, outils de suivi de versions, etc.) en gardant à l'esprit la sécurisation des outils (authentification, gestion d'accès et des droits, protection des données, etc.).

Il doit également se placer comme un acteur averti du développement durable, de la transition énergétique et des réglementations en vigueur (entreprise, RGPD, ARCEP, etc.).

Apprentissages critiques :

- AC31.01 | Concevoir un projet de réseau informatique d'une entreprise en intégrant les problématiques de haute disponibilité, de QoS, de sécurité et de supervision
- AC31.02 | Réaliser la documentation technique de ce projet
- AC31.03 | Réaliser une maquette de démonstration du projet
- AC31.04 | Défendre/argumenter un projet
- AC31.05 | Communiquer avec les acteurs du projet
- AC31.06 | Gérer le projet et les différentes étapes de sa mise en œuvre en respectant les délais
- AC32.01 | Déployer un système de communication pour l'entreprise
- AC32.02 | Déployer un réseau d'accès sans fil pour le réseau d'entreprise en intégrant les enjeux de la sécurité
- AC32.03 | Déployer un réseau d'accès fixe ou mobile pour un opérateur de télécommunications en intégrant la sécurité
- AC32.04 | Permettre aux collaborateurs de se connecter de manière sécurisée au système d'information de l'entreprise
- AC32.05 | Collaborer en mode projet en français et en anglais
- AC33.01 | Élaborer les spécifications techniques et le cahier des charges d'une application informatique
- AC33.02 | Mettre en place un environnement de travail collaboratif
- AC33.03 | Participer à la formation des utilisateurs
- AC33.04 | Déployer et maintenir une solution informatique
- AC33.05 | S'informer sur les évolutions et les nouveautés technologiques
- AC33.06 | Sécuriser l'environnement numérique d'une application

Ressources mobilisées et combinées :

- R5.01 | WiFi avancé
- R5.02 | Supervision des réseaux
- R5.03 | Ingénierie de systèmes télécoms
- R5.04 | Cycle de vie d'un projet informatique
- R5.05 | Anglais : Insertion professionnelle 1
- R5.06 | Expression-Culture-Communication professionnelles : S'intégrer dans une organisation
- R5.07 | Projet Personnel et Professionnel
- R5.08 | Gestion de projets 3 : Mener un projet professionnel

Volume horaire :

Volume horaire : à définir localement par chaque IUT

3.2.2. SAÉ 5.02 : Piloter un projet informatique

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

Objectifs et problématique professionnelle :

Le professionnel R&T est intégré dans un service de technologies de l'information dans lequel il est amené à travailler sur la conception d'applications ou de projets informatiques au sein d'une équipe. Il doit mettre en œuvre un environnement de travail collaboratif et utiliser des méthodologies de gestion de projet informatique.

Descriptif générique :

Un projet informatique nécessite une répartition de tâches entre les différents membres de l'équipe dont le professionnel R&T fait partie et où il peut coordonner certaines des activités du projet. Il s'appuie sur différentes méthodes de gestion de projet (Agiles, SCRUM, ...) et d'outils collaboratifs. L'équipe assure le cycle de vie du projet informatique au travers des étapes suivantes :

- Analyser le besoin aboutissant au lancement d'un projet de développement :
 - Définir les objectifs
 - Rédiger le cahier des charges en spécifiant les attentes/contraintes fonctionnelles et techniques
 - Définir la stratégie de mise en production
 - Tenir compte des problèmes de sécurité
- Mettre en place un environnement de travail collaboratif
 - Utilisation des plateformes collaboratives dédiées au développement comme par exemple GitLab
 - Gestion des branches de développement et production
 - Création de clones
 - Gestion des tickets
 - Gestion des versions
- Découper le travail pour affecter les tâches entre les membres de l'équipe de développement.
 - Choisir les environnements de développement pour chaque partie du projet (par exemple virtualenv python, IDE tel que VSCode, Docker, ...)
 - Prévoir les procédures de tests unitaires et qualification tout au long de la phase de développement
- Produire les documentations
 - La documentation technique pour la maintenance et l'évolution de l'application
 - La documentation utilisateur en vue de la formation des usagers
- Mettre en production les différentes versions de l'application en tenant compte des aspects de sécurité (stockage des mots de passe, base de données de production,...).

Apprentissages critiques :

- AC31.02 | Réaliser la documentation technique de ce projet
- AC31.03 | Réaliser une maquette de démonstration du projet
- AC31.04 | Défendre/argumenter un projet
- AC31.05 | Communiquer avec les acteurs du projet
- AC31.06 | Gérer le projet et les différentes étapes de sa mise en œuvre en respectant les délais
- AC32.05 | Collaborer en mode projet en français et en anglais
- AC33.01 | Élaborer les spécifications techniques et le cahier des charges d'une application informatique
- AC33.02 | Mettre en place un environnement de travail collaboratif
- AC33.03 | Participer à la formation des utilisateurs
- AC33.04 | Déployer et maintenir une solution informatique
- AC33.05 | S'informer sur les évolutions et les nouveautés technologiques
- AC33.06 | Sécuriser l'environnement numérique d'une application

Ressources mobilisées et combinées :

- R5.04 | Cycle de vie d'un projet informatique
- R5.05 | Anglais : Insertion professionnelle 1
- R5.06 | Expression-Culture-Communication professionnelles : S'intégrer dans une organisation

- R5.07 | Projet Personnel et Professionnel
- R5.08 | Gestion de projets 3 : Mener un projet professionnel

Volume horaire :

Volume horaire : à définir localement par chaque IUT

3.2.3. SAÉ 5.Cyber.03 : Assurer la sécurisation et la supervision avancées d'un système d'information

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé

Objectifs et problématique professionnelle :

Le professionnel R&T en Cybersécurité doit être capable d'adapter la cybersurveillance au système d'information d'une entreprise. Il peut tester l'efficacité des dispositifs déployés au vu des alertes générées par un pentest.

Descriptif générique :

Le professionnel R&T réalise une analyse préalable des besoins de sécurité lui permettant de mettre en œuvre judicieusement tout ou partie des concepts plus avancés suivants :

- zones de sécurité hiérarchique (DMZ)
- filtrage avancés (FireWall statefull, NG, ...)
- accès distants et télétravail sécurisé et interconnexion de sites (VPN, ...)
- outils de surveillance :
 - IDS/IPS
 - logs
 - supervision
 - SIEM

Cette SAÉ peut faire suite à la SAÉ4.Cyber.01 "Sécuriser un système d'information".

Apprentissages critiques :

- AC34.01Cyber | Participer activement à une analyse de risque pour définir une politique de sécurité pour une petite structure
- AC34.02Cyber | Mettre en œuvre des outils avancés de sécurisation d'une infrastructure du réseau
- AC34.03Cyber | Sécuriser les systèmes d'exploitation
- AC34.04Cyber | Proposer une architecture sécurisée de système d'information pour une petite structure
- AC35.01Cyber | Surveiller l'activité du système d'information
- AC35.02Cyber | Appliquer une méthodologie de tests de pénétration
- AC35.03Cyber | Réagir face à un incident de sécurité
- AC35.04Cyber | Administre les outils de surveillance du système d'information

Ressources mobilisées et combinées :

- R5.05 | Anglais : Insertion professionnelle 1
- R5.06 | Expression-Culture-Communication professionnelles : S'intégrer dans une organisation
- R5.07 | Projet Personnel et Professionnel
- R5.08 | Gestion de projets 3 : Mener un projet professionnel
- R5.Cyber.09 | Architectures sécurisées
- R5.Cyber.10 | Audits de sécurité
- R5.Cyber.11 | Supervision de la sécurité
- R5.Cyber.12 | Normes, standards et analyse de risques

Volume horaire :

Volume horaire : à définir localement par chaque IUT

3.2.4. PORTFOLIO : Démarche portfolio

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé
- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

Objectifs et problématique professionnelle :

Au semestre 5, la démarche portfolio consistera en un point étape intermédiaire qui permettra à l'étudiant de se positionner, sans être évalué, dans le processus d'acquisition des niveaux de compétences de la troisième année du B.U.T. et relativement au parcours suivi.

Descriptif générique :

L'équipe pédagogique devra accompagner l'étudiant dans la compréhension et l'appropriation effectives du référentiel de compétences et de ses éléments constitutifs tels que les composantes essentielles en tant qu'elles constituent des critères qualité. Seront également exposées les différentes possibilités de démonstration et d'évaluation de l'acquisition des niveaux de compétences ciblés en troisième année par la mobilisation notamment d'éléments de preuve issus de toutes les SAÉ. L'enjeu est de permettre à l'étudiant d'engager une démarche d'auto-positionnement et d'auto-évaluation tout en intégrant la spécificité du parcours suivi.

Ressources mobilisées et combinées :

- R5.05 | Anglais : Insertion professionnelle 1
- R5.06 | Expression-Culture-Communication professionnelles : S'intégrer dans une organisation
- R5.07 | Projet Personnel et Professionnel
- R5.08 | Gestion de projets 3 : Mener un projet professionnel

Volume horaire :

Volume horaire : à définir localement par chaque IUT

3.3. Fiches Ressources

3.3.1. Ressource R5.01 : WiFi avancé

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers

SAÉ au sein desquelles la ressource peut être mobilisée et combinée :

- SAÉ 5.01 | Concevoir, réaliser et présenter une solution technique

Descriptif :

Contexte et ancrage professionnel :

Les étudiants seront capables de déployer et maintenir une infrastructure sans fil centralisée, ainsi que de mesurer la qualité de la couverture radio (puissance, canaux, débit, interférences, ...).

Contenus :

- Normes (rappels)
- Couche physique (antennes, spectre, ...)
- Couverture radio
- Gestion centralisée (contrôleur)
- Sécurité (Authentification, Chiffrement, ...)

Apprentissages critiques ciblés :

- AC31.01 | Concevoir un projet de réseau informatique d'une entreprise en intégrant les problématiques de haute disponibilité, de QoS, de sécurité et de supervision
- AC31.03 | Réaliser une maquette de démonstration du projet
- AC32.01 | Déployer un système de communication pour l'entreprise
- AC32.02 | Déployer un réseau d'accès sans fil pour le réseau d'entreprise en intégrant les enjeux de la sécurité
- AC32.04 | Permettre aux collaborateurs de se connecter de manière sécurisée au système d'information de l'entreprise

Mots clés :

WIFI – 80211 – Bornes – Contrôleur WIFI – Antennes – Sécurité – Spectre – Propagation “indoor”

Volume horaire :

Volume horaire défini nationalement : 18 heures dont 11 heures de TP

3.3.2. Ressource R5.02 : Supervision des réseaux

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein desquelles la ressource peut être mobilisée et combinée :

- SAÉ 5.01 | Concevoir, réaliser et présenter une solution technique

Descriptif :

Contexte et ancrage professionnel :

Les étudiants seront capables de déployer une solution de supervision du système d'information d'une entreprise. Les concepts fondamentaux suivants seront mis en oeuvre :

Contenus :

- Méthodologie de la supervision ,
- Architecture d'un système de supervision,
- Services et protocoles, outils de supervision, outils de métrologie,
- Gestion des logs,
- API de supervision,
- Développement de modules complémentaires (plug-in).

Penser à systématiser l'utilisation de WireShark pour les TP.

Apprentissages critiques ciblés :

- AC31.01 | Concevoir un projet de réseau informatique d'une entreprise en intégrant les problématiques de haute disponibilité, de QoS, de sécurité et de supervision
- AC33.04 | Déployer et maintenir une solution informatique
- AC33.06 | Sécuriser l'environnement numérique d'une application

Mots clés :

NTP – Logs – SNMP – SIEM – Tableau de bord – Nagios – Centreon – Netflow – API REST

Volume horaire :

Volume horaire défini nationalement : 18 heures dont 13 heures de TP

3.3.3. Ressource R5.03 : Ingénierie de systèmes télécoms

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers

SAÉ au sein desquelles la ressource peut être mobilisée et combinée :

- SAÉ 5.01 | Concevoir, réaliser et présenter une solution technique

Descriptif :

Contexte et ancrage professionnel :

L'étudiant devra être capable d'étudier, de caractériser et de mettre en œuvre un système de transmission.

Contenus :

- Étude et conception de différentes briques d'un ou plusieurs systèmes de transmission
- Mise en application d'un ou plusieurs systèmes de transmission
- Veille technologique
- Exemples de systèmes : Radio logicielle, Antennes, WiFi, MIMO, Faisceaux hertziens, FTTA – FTTx, LiFi, FiWi

Prérequis :

- R5.01 | WiFi avancé

Apprentissages critiques ciblés :

- AC31.03 | Réaliser une maquette de démonstration du projet
- AC32.01 | Déployer un système de communication pour l'entreprise

Mots clés :

Systèmes télécoms – Radio logicielle – SDR – Antennes – WiFi – MIMO – Faisceaux hertziens – FTTA – FTTx – LiFi – FiWi – Fibres optiques

Volume horaire :

Volume horaire défini nationalement : 17 heures dont 10 heures de TP

3.3.4. Ressource R5.04 : Cycle de vie d'un projet informatique

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 5.01 | Concevoir, réaliser et présenter une solution technique
- SAÉ 5.02 | Piloter un projet informatique

Descriptif :

Contexte et ancrage professionnel :

Le professionnel R&T peut être amené à gérer toutes les étapes d'un projet informatique depuis le cahier des charges jusqu'à la mise en production et la fourniture de documentation tant utilisateurs que technique. Cette ressource a donc pour objectif de faire appréhender toutes les étapes d'un projet informatique depuis l'expression d'un besoin jusqu'au produit fini.

Contenus :

Cette ressource aborde les notions suivantes :

- Analyse du besoin aboutissant au lancement d'un projet de développement :
 - Définition des objectifs,
 - Rédaction du cahier des charges en spécifiant les attentes/contraintes fonctionnelles et techniques,
 - Choix de la stratégie de mise en production,
 - Prise en compte des problèmes de sécurité.
- Mise en place d'un environnement de travail collaboratif :
 - Utilisation des plateformes collaboratives dédiées au développement (par ex. GitLab) à travers la gestion des branches de développement et production, la création de clones, la gestion des tickets, la gestion des versions,
 - Découpage du travail pour affecter les tâches entre les membres de l'équipe de développement.
- Choix des environnements de développement pour chaque partie du projet (par exemple virtualenv python, IDE, Docker, ...).
- Mise en place des procédures de tests unitaires et de qualification tout au long de la phase de développement.
- Production de documentations :
 - Documentation technique pour la maintenance et l'évolution de l'application,
 - Documentation utilisateur en vue de la formation des usagers,
 - Outils pour la génération de documentation : générateurs à partir du code (Sphinx, Javadoc, ...), langage pour la documentation (markdown, asciidoc, restructured text, ...)
- Mise en production des différentes versions de l'application en tenant compte des aspects de sécurité (stockage des mots de passe, base de données de production, ...).

Cette ressource s'appuiera sur la réalisation d'un projet informatique en groupe restreint dans la SAÉ5.02 "Piloter un projet informatique". Elle pourra mobiliser les concepts des méthodes Agile et Scrum vus dans la ressource R5.08 "Gestion de projets".

On pourra approfondir certains de ces contenus en s'appuyant sur ceux décrits dans la ressource R5.DevCloud.09 « Outils et méthodes DevOps ».

Prérequis :

- R5.08 | Gestion de projets 3 : Mener un projet professionnel

Apprentissages critiques ciblés :

- AC31.02 | Réaliser la documentation technique de ce projet
- AC31.03 | Réaliser une maquette de démonstration du projet
- AC31.04 | Défendre/argumenter un projet
- AC31.05 | Communiquer avec les acteurs du projet
- AC31.06 | Gérer le projet et les différentes étapes de sa mise en œuvre en respectant les délais
- AC33.01 | Élaborer les spécifications techniques et le cahier des charges d'une application informatique
- AC33.02 | Mettre en place un environnement de travail collaboratif

- AC33.03 | Participer à la formation des utilisateurs
- AC33.04 | Déployer et maintenir une solution informatique
- AC33.05 | S'informer sur les évolutions et les nouveautés technologiques
- AC33.06 | Sécuriser l'environnement numérique d'une application

Mots clés :

Versionning – Cahier des charges – Environnement de travail collaboratif – Gestion de projet – Git – IDE – Documentation – Sécurité – Déploiement – Partage – Cycle de vie – Méthode Agile

Volume horaire :

Volume horaire défini nationalement : 7 heures dont 4 heures de TP

3.3.5. Ressource R5.05 : Anglais : Insertion professionnelle 1

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 5.01 | Concevoir, réaliser et présenter une solution technique
- SAÉ 5.02 | Piloter un projet informatique
- SAÉ 5.Cyber.03 | Assurer la sécurisation et la supervision avancées d'un système d'information
- PORTFOLIO | Portfolio

Descriptif :

Contexte et ancrage professionnel :

Cette ressource apporte le socle de connaissances langagières pour les compétences de cœur de métier « Administrer les réseaux et l'Internet » et « Connecter les entreprises et les usagers ». Elle contribue aussi à la compétence « Créer des outils et applications informatiques pour les R&T » à travers des mises en situations, jeux de rôle, dialogues qui permettent la prise de parole en continu et en interaction, en développant les compétences de compréhension dans un contexte professionnel technique.

Contenus :

- Rendre compte à l'oral et/ou à l'écrit de son expérience professionnelle, ses compétences, ses qualités et ses points d'amélioration
- Se projeter dans un parcours universitaire ou professionnel post B.U.T. (lien avec le portfolio)
- Mettre en perspective les nouvelles technologies et en avoir une approche critique
- Consolider les techniques de communication professionnelle orale et écrite
- Renforcer les compétences linguistiques et phonologiques

Anglais de spécialité adapté aux parcours

Préconisations de mise en oeuvre :

- Télécollaboration, télétandem, EMILE
- Mobilité à l'étranger (séjour linguistique, stage, semestre)
- Les ressources d'anglais seront utiles et à mettre en oeuvre dans le PPP et portfolio notamment sur le volet internationale
- Préparation du stage de S6

Apprentissages critiques ciblés :

- AC31.02 | Réaliser la documentation technique de ce projet
- AC31.04 | Défendre/argumenter un projet
- AC31.05 | Communiquer avec les acteurs du projet
- AC32.05 | Collaborer en mode projet en français et en anglais
- AC33.01 | Élaborer les spécifications techniques et le cahier des charges d'une application informatique
- AC33.03 | Participer à la formation des utilisateurs
- AC33.05 | S'informer sur les évolutions et les nouveautés technologiques

Mots clés :

Communication orale et écrite – Anglais technique de spécialité

Volume horaire :

Volume horaire défini nationalement : 14 heures dont 7 heures de TP

3.3.6. Ressource R5.06 : Expression-Culture-Communication professionnelles : S'intégrer dans une organisation

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 5.01 | Concevoir, réaliser et présenter une solution technique
- SAÉ 5.02 | Piloter un projet informatique
- SAÉ 5.Cyber.03 | Assurer la sécurisation et la supervision avancées d'un système d'information
- PORTFOLIO | Portfolio

Descriptif :

Contexte et ancrage professionnel :

A la suite de la première immersion professionnelle R&T et en amont de la seconde, cette ressource vise notamment, grâce au recul développé par les étudiants au cours du précédent stage, à développer des outils d'intégration et de collaboration.

Contenus :

- Renforcement de l'expression formelle, remédiation (CCDMD.qc.ca/fr Canadien, Projet Voltaire, Ecri+, Dictée des IUT, concours d'écriture...);
- Renforcement de l'utilisation des outils bureautiques : fonctionnalités avancées ;
- Renforcement des capacités à produire un document clair et concis ;
- Renforcement des capacités à construire un support visuel de présentation orale ;
- Renforcement des capacités à présenter oralement, de manière claire et concise ;
- Compréhension de la multiplicité des langages et les biais cognitifs associés ;
- Compréhension de l'image, de la culture et de l'identité d'une entreprise ;
- Initiation à la gestion de l'humain, à différents types de management, à la prévention des conflits ;
- Conduite, animation de réunion ;
- Reprise et amélioration des documents d'insertion professionnelle (CV, lettre de motivation, profil LinkedIn, ...).

L'étudiant sera également force de proposition en faisant preuve de créativité, en animant un brainstorming pour dégager de nouvelles idées, directions, ...

Apprentissages critiques ciblés :

- AC31.02 | Réaliser la documentation technique de ce projet
- AC31.04 | Défendre/argumenter un projet
- AC31.05 | Communiquer avec les acteurs du projet
- AC31.06 | Gérer le projet et les différentes étapes de sa mise en œuvre en respectant les délais
- AC32.05 | Collaborer en mode projet en français et en anglais
- AC33.01 | Élaborer les spécifications techniques et le cahier des charges d'une application informatique
- AC33.02 | Mettre en place un environnement de travail collaboratif
- AC33.03 | Participer à la formation des utilisateurs
- AC33.05 | S'informer sur les évolutions et les nouveautés technologiques

Mots clés :

Communication écrite et orale – Relations humaines – Insertion professionnelle

Volume horaire :

Volume horaire défini nationalement : 22 heures dont 7 heures de TP

3.3.7. Ressource R5.07 : Projet Personnel et Professionnel

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé
- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 5.01 | Concevoir, réaliser et présenter une solution technique
- SAÉ 5.02 | Piloter un projet informatique
- SAÉ 5.Cyber.03 | Assurer la sécurisation et la supervision avancées d'un système d'information
- PORTFOLIO | Portfolio

Descriptif :

[1] Connaissance de soi et posture professionnelle (en lien avec années 1&2)

- Exploiter son stage afin de parfaire sa posture professionnelle
- Formaliser ses réseaux professionnels (profils, carte réseau, réseau professionnel...)
- Faire le bilan de ses compétences

[2] Formaliser son plan de carrière

- Développer une stratégie personnelle et professionnelle à court terme (pour une insertion professionnelle immédiate après le B.U.T. ou une poursuite d'études) et à plus long terme (VAE, CPF, FTLV, etc.)

[3] S'approprier le processus et s'adapter aux différents types de recrutement

- mettre à jour les outils de communication professionnelle (CV, LM, identité professionnelle numérique, etc.)
- se préparer aux différents types et formes de recrutement
- types : test, entretien collectif ou individuel, mise en situation, concours, etc.
- formes : recrutement d'école, de master, d'entreprise, etc.

En dernière année de BUT, l'étudiant est amené à construire une stratégie d'insertion. L'approfondissement des métiers R&T à bac+3, des poursuites d'études possibles, et l'exploitation du stage du 4e semestre contribuent à cet objectif.

Contenus :

- Analyser plusieurs situations professionnelles, notamment lorsqu'elles ont été rencontrées lors des stages de 2e année
- Compléter et valoriser son parcours (formation et expériences professionnelles, exploitation du stage de 2e année)
- Compléter et valoriser son projet personnel et professionnel
- Mieux définir la notion de cadre intermédiaire (réunion, encadrement de projet, communication interne et management, responsabilité, ...)
- Approfondir et mieux définir le projet métier (enquête métiers)
- Découvrir les possibilités de poursuites d'études et de Formation Tout au Long de la Vie (VAE, formation continue, ...)
- Développer une stratégie personnelle et professionnelle à court terme (insertion immédiate ou poursuite d'études)
- Améliorer, mettre à jour et exploiter son réseau professionnel
- Préparer le bilan de ses compétences techniques et transversales

Prolongements possibles :

- Recherche de stage
- Portfolio
- CV et lettre de motivation
- Préparation à l'entretien de recrutement

Apprentissages critiques ciblés :

- AC31.01 | Concevoir un projet de réseau informatique d'une entreprise en intégrant les problématiques de haute disponibilité, de QoS, de sécurité et de supervision
- AC31.02 | Réaliser la documentation technique de ce projet

- AC31.03 | Réaliser une maquette de démonstration du projet
- AC31.04 | Défendre/argumenter un projet
- AC31.05 | Communiquer avec les acteurs du projet
- AC31.06 | Gérer le projet et les différentes étapes de sa mise en œuvre en respectant les délais
- AC32.01 | Déployer un système de communication pour l'entreprise
- AC32.02 | Déployer un réseau d'accès sans fil pour le réseau d'entreprise en intégrant les enjeux de la sécurité
- AC32.03 | Déployer un réseau d'accès fixe ou mobile pour un opérateur de télécommunications en intégrant la sécurité
- AC32.04 | Permettre aux collaborateurs de se connecter de manière sécurisée au système d'information de l'entreprise
- AC32.05 | Collaborer en mode projet en français et en anglais
- AC33.01 | Élaborer les spécifications techniques et le cahier des charges d'une application informatique
- AC33.02 | Mettre en place un environnement de travail collaboratif
- AC33.03 | Participer à la formation des utilisateurs
- AC33.04 | Déployer et maintenir une solution informatique
- AC33.05 | S'informer sur les évolutions et les nouveautés technologiques
- AC33.06 | Sécuriser l'environnement numérique d'une application
- AC34.01Cyber | Participer activement à une analyse de risque pour définir une politique de sécurité pour une petite structure
- AC34.02Cyber | Mettre en œuvre des outils avancés de sécurisation d'une infrastructure du réseau
- AC34.03Cyber | Sécuriser les systèmes d'exploitation
- AC34.04Cyber | Proposer une architecture sécurisée de système d'information pour une petite structure
- AC35.01Cyber | Surveiller l'activité du système d'information
- AC35.02Cyber | Appliquer une méthodologie de tests de pénétration
- AC35.03Cyber | Réagir face à un incident de sécurité
- AC35.04Cyber | Administrer les outils de surveillance du système d'information

Mots clés :

Carrière – recrutement – connaissance de soi – outils de communication – réseau – bilan de compétences – Stage – Connais-sance de soi – Stratégie d'insertion – Plan de carrière

Volume horaire :

Volume horaire défini nationalement : 7 heures dont 3 heures de TP

3.3.8. Ressource R5.08 : Gestion de projets 3 : Mener un projet professionnel

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 5.01 | Concevoir, réaliser et présenter une solution technique
- SAÉ 5.02 | Piloter un projet informatique
- SAÉ 5.Cyber.03 | Assurer la sécurisation et la supervision avancées d'un système d'information
- PORTFOLIO | Portfolio

Descriptif :

Contexte et ancrage professionnel :

Le professionnel R&T peut être impliqué dans différents projets l'amenant à travailler en équipe. Pour être opérationnel sur ce plan, l'étudiant doit être capable d'élaborer des solutions adaptées à des contraintes explicites ou implicites, et mettre en œuvre une organisation complète et détaillée, en s'a aidant d'outils et de méthodes professionnels.

Contenus :

- Lire ou décoder un cahier des charges complexe
- Construire un cahier des charges complexe
- Conceptualiser de manière détaillée et exhaustive les tâches à réaliser à l'aide d'outils adaptés (cartes mentales, infographies, etc.)
- Mettre en place les conditions nécessaires à la créativité, l'intrapreneuriat, et mettre en place des méthodes de validation des idées
- Prendre sa place dans une équipe en connaissant les différents rôles d'une équipe projet et en étant capable d'y prendre différents rôles
- S'adapter à des profils professionnels différents qui interviennent dans un projet (manager, collaborateur, client)
- Maîtriser le Lean Management (l'amélioration continue) : réaliser un bilan régulier sur l'avancée d'un projet (points bloquants, solutions apportées...)
- Organiser, préparer et conduire des réunions de projet : planification, prise de notes, comptes rendus, actions à réaliser
- Comprendre et analyser, contextualiser finement un sujet, adapter une solution à un contexte particulier (objectifs projet, contraintes liées au contexte et ressources humaines/matérielles/budgétaires)
- Être capable d'anticiper les risques (matrice, criticité) et mettre en place des stratégies de réponse associées à des plans d'actions
- Maîtriser les bilans réguliers sur l'avancée d'un projet à un client ou un référent
- Découper un projet en tâches détaillées
- Estimer finement le temps nécessaire à l'élaboration de chaque tâche
- Construire un rétroplanning intégrant les aléas attendus d'un projet technique (fiable, réaliste, prudent...)
- Répartir finement les tâches dans l'équipe de travail ; être capable de basculer d'un rôle à l'autre, d'une tâche à l'autre
- Actualiser/faire évoluer l'organisation du travail en fonction des contraintes
- Actualiser/faire évoluer l'organisation du travail en mettant en oeuvre des méthodes de types Agile/Scrum/réitération/production immédiate
- Savoir construire, motiver et faire vivre une équipe (adéquation des compétences/membres/personnalités dans une équipe, veiller à la compatibilité ou à la complémentarité au sein d'une équipe projet)
- Intégrer l'éco-responsabilité, le développement durable (bonnes pratiques, choix des matériels, valeur écologique ou responsable apportée au projet, manière de développer ou coder)
- Prendre en compte des coûts approximatifs et gérer un budget

Le stage représente un cadre particulier d'application des ressources.

Apprentissages critiques ciblés :

- AC31.01 | Concevoir un projet de réseau informatique d'une entreprise en intégrant les problématiques de haute disponibilité, de QoS, de sécurité et de supervision
- AC31.02 | Réaliser la documentation technique de ce projet

- AC31.03 | Réaliser une maquette de démonstration du projet
- AC31.04 | Défendre/argumenter un projet
- AC31.05 | Communiquer avec les acteurs du projet
- AC31.06 | Gérer le projet et les différentes étapes de sa mise en œuvre en respectant les délais
- AC32.05 | Collaborer en mode projet en français et en anglais
- AC33.01 | Élaborer les spécifications techniques et le cahier des charges d'une application informatique
- AC33.02 | Mettre en place un environnement de travail collaboratif

Mots clés :

Agilité – Cahier des charges – Coûts – Éco-responsabilité – Lean management – Gantt

Volume horaire :

Volume horaire défini nationalement : 11 heures dont 4 heures de TP

3.3.9. Ressource R5.Cyber.09 : Architectures sécurisées

Compétence ciblée :

- Administrer un système d'information sécurisé

SAÉ au sein desquelles la ressource peut être mobilisée et combinée :

- SAÉ 5.Cyber.03 | Assurer la sécurisation et la supervision avancées d'un système d'information

Descriptif :

Contexte et ancrage professionnel :

Les étudiants seront capables d'ajouter à une architecture sécurisée existante des fonctionnalités de sécurisation avancée (filtrage avec état, filtrage applicatif, analyse comportementale, inspection de contenus, authentification forte, ...)

Contenus :

Certaines fonctionnalités de sécurité pourront être mises en œuvre au travers de systèmes de détection ou de prévention d'intrusions sur des environnements physiques et/ou virtuels.

Apprentissages critiques ciblés :

- AC34.02Cyber | Mettre en œuvre des outils avancés de sécurisation d'une infrastructure du réseau
- AC34.03Cyber | Sécuriser les systèmes d'exploitation
- AC34.04Cyber | Proposer une architecture sécurisée de système d'information pour une petite structure

Mots clés :

Firewall-NG – IDS – IPS – Authentication – AAA – SSO – MFA

Volume horaire :

Volume horaire défini nationalement : 30 heures dont 20 heures de TP

3.3.10. Ressource R5.Cyber.10 : Audits de sécurité

Compétence ciblée :

- Surveiller un système d'information sécurisé

SAÉ au sein desquelles la ressource peut être mobilisée et combinée :

- SAÉ 5.Cyber.03 | Assurer la sécurisation et la supervision avancées d'un système d'information

Descriptif :

Contexte et ancrage professionnel :

Les étudiants seront capables de déployer une approche professionnelle d'audit de sécurité sur un système d'information de type PME. En cela, ils devront retracer la topologie du réseau d'entreprise, les équipements utilisés (éléments actifs, serveurs, postes clients), les services installés et la sécurité mise en place.

Ils doivent alors éprouver la robustesse du système en place dans le but d'identifier d'éventuelles vulnérabilités.

Ils préconisent alors des modifications pour améliorer la sécurité du système d'information.

Préconisations de mise en œuvre et de contenus :

L'analyse fonctionnelle pourra être mise en situation (simulée) en TD.

L'analyse opérationnelle pourra être mise en place en TP grâce à l'utilisation d'outils fondamentaux d'analyse (nmap, masscan, OpenVAS, ...) puis de tests d'intrusion et d'attaque (Metasploit, Mitre Att@ck, ...).

Les tests d'analyse, d'intrusion et d'attaques pourront être mis en œuvre sur des environnements cloisonnés locaux ou en ligne (cyber-range, ...)

On pourra s'appuyer sur les formations et supports de cours de l'ANSSI (CFSSI) « Principes et organisation des audits en SSI ».

Prérequis :

- R5.Cyber.09 | Architectures sécurisées

Apprentissages critiques ciblés :

- AC35.01Cyber | Surveiller l'activité du système d'information
- AC35.02Cyber | Appliquer une méthodologie de tests de pénétration

Mots clés :

Audit – Sécurité – Vulnérabilités – Attaques – Menaces – Tests d'intrusion

Volume horaire :

Volume horaire défini nationalement : 23 heures dont 12 heures de TP

3.3.11. Ressource R5.Cyber.11 : Supervision de la sécurité

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé

SAÉ au sein desquelles la ressource peut être mobilisée et combinée :

- SAÉ 5.Cyber.03 | Assurer la sécurisation et la supervision avancées d'un système d'information

Descriptif :

Contexte et ancrage professionnel :

Les étudiants seront capables de définir précisément (et différencier) les notions de SOC, NOC et SIM, SEM et SIEM, ...

Ils seront capables de remonter et collecter les différents types de logs grâce à l'utilisation des agents correspondants (agents de types divers, beats, ...).

Contenus :

La ressource traite de :

- l'utilisation d'outils de normalisation de logs (logstash, ...), de modules SIEM afin de détecter des attaques en procédant à la corrélation d'événements de sécurité.
- l'utilisation d'outils spécialisés (Kibana, Grafana, Elastic...) pour générer des tableaux de bords clairs et contextualisés permettant de mettre en évidence toute anomalie et de générer automatiquement des alertes.

Les étudiants sauront émettre un avis précis (de niveau 1) sur ces alertes afin de prendre les décisions adaptées.

Apprentissages critiques ciblés :

- AC34.02Cyber | Mettre en œuvre des outils avancés de sécurisation d'une infrastructure du réseau
- AC34.03Cyber | Sécuriser les systèmes d'exploitation
- AC35.01Cyber | Surveiller l'activité du système d'information
- AC35.04Cyber | Administrer les outils de surveillance du système d'information

Mots clés :

SOC (Security Operation Center) – NOC (Network Operation Center) – SIEM (SIM + SEM) (Security Information and Event Management)

Volume horaire :

Volume horaire défini nationalement : 22 heures dont 13 heures de TP

3.3.12. Ressource R5.Cyber.12 : Normes, standards et analyse de risques

Compétence ciblée :

- Administrer un système d'information sécurisé

SAÉ au sein desquelles la ressource peut être mobilisée et combinée :

- SAÉ 5.Cyber.03 | Assurer la sécurisation et la supervision avancées d'un système d'information

Descriptif :

Contexte et ancrage professionnel :

Les étudiants seront capables de se conformer aux exigences de la réglementation en vigueur, concernant la manipulation, le stockage et plus généralement la sécurisation des données du SI dont ils ont la responsabilité.

Contenus :

Ils seront capables de participer activement à une analyse de risques menée au sein de leur entreprise. Ce faisant :

- Ils auront participé à une analyse de risques sur un périmètre réduit,
- Ils auront acquis le vocabulaire spécifique à la gestion du risque,
- Ils sauront décrire les différentes phases du processus de gestion du risque (appréciation du risque, traitement du risque, ...),
- Ils auront eu une introduction aux diverses normes du domaine (ISO 27001, ISO 27002, ... et surtout ISO 27005).

Prérequis :

- R5.Cyber.09 | Architectures sécurisées

Apprentissages critiques ciblés :

- AC34.01Cyber | Participer activement à une analyse de risque pour définir une politique de sécurité pour une petite structure
- AC34.04Cyber | Proposer une architecture sécurisée de système d'information pour une petite structure

Mots clés :

Risque – Menaces – Vulnérabilités – Disponibilité – Intégrité – Confidentialité – Traçabilité – DICT – Mode opératoire – Valeur métier – Biens essentiels – EBIOS – Analyse de risques – ISO 27005 – RGPD – LPM

Volume horaire :

Volume horaire défini nationalement : 15 heures dont 9 heures de TP

4. Semestre 6

4.1. Tableau croisé

Ce tableau explicite les correspondances entre les compétences, les apprentissages critiques, les SAÉ et les ressources programmés dans le semestre.

Les SAÉ et les ressources ainsi identifiées pour chaque UE participent à son obtention, et en ce sens doivent faire l'objet d'une évaluation, à l'exception de la démarche portfolio des semestres impairs.

Ce tableau détaille par ailleurs la répartition du volume horaire global des heures d'enseignement encadré de chaque semestre, à savoir :

- le volume horaire alloué à l'ensemble des SAÉ ;
- le volume de chaque ressource définie nationalement dont les heures TP ;
- le volume horaire, dont les heures TP, relevant d'une partie de l'adaptation locale et pouvant être affecté de manière non exclusive soit aux SAÉ, soit aux ressources définies nationalement ou localement.

	AC	SAÉ 6 Cyber.01 Réagir face à une cyber-attaque	STAGE Cyber Stage	PORTFOLIO Portfolio	R6.01 Anglais : Insertion professionnelle 2	R6.02 Expression-Culture-Communication professionnelles : Communiquer en	R6.03 Connaissance de l'entreprise	R6 Cyber.04 Réponse à incident
Administrer	AC31.01		X	X			X	
	AC31.02		X	X	X	X		
	AC31.03		X	X			X	
	AC31.04		X	X	X	X		
	AC31.05		X	X	X	X		
	AC31.06		X	X				
Connecter	AC32.01		X	X			X	
	AC32.02		X	X			X	
	AC32.03		X	X			X	
	AC32.04		X	X				
	AC32.05		X	X	X	X		
Programmer	AC33.01		X	X	X		X	
	AC33.02		X	X		X	X	
	AC33.03		X	X	X	X	X	
	AC33.04		X	X				
	AC33.05		X	X	X	X		
	AC33.06		X	X				
Sécuriser	AC34.01Cyber		X	X				
	AC34.02Cyber	X	X	X				
	AC34.03Cyber	X	X	X				
	AC34.04Cyber		X	X				
Surveiller	AC35.01Cyber	X	X	X				
	AC35.02Cyber		X	X				
	AC35.03Cyber	X	X	X				X
	AC35.04Cyber	X	X	X				
Volume total				8	11	11	18	48
Dont TP				4	4	2	9	19
Adaptation Locale (SAÉ)				15				15
Adaptation Locale (Ressources ou SAÉ)					17			17
TP Adaptation locale				15				15

4.2. Fiches Situations d'apprentissage et d'évaluation (SAÉ)

4.2.1. SAÉ 6.Cyber.01 : Réagir face à une cyber-attaque

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé

Objectifs et problématique professionnelle :

Le professionnel R&T spécialisé dans la Cybersécurité, lorsqu'il fait face à une cyber-attaque au sein de son entreprise, identifie les enjeux de l'attaque, reproduit la situation technique se jouant pendant l'attaque et applique le processus de réponse à incident.

Descriptif générique :

Le professionnel en Cybersécurité, à l'aide d'une infrastructure technologique, a pour mission lors d'une attaque de :

- identifier l'attaque ;
- stopper la propagation ;
- neutraliser l'attaque ;
- prélever et conserver les preuves ;
- pratiquer les premières investigations.

Cette SAÉ peut s'appuyer sur l'infrastructure technologique mise en place à la SAÉ5.03Cyber "Sécurisation avancée et supervision d'un système d'information".

Apprentissages critiques :

- AC34.02Cyber | Mettre en œuvre des outils avancés de sécurisation d'une infrastructure du réseau
- AC34.03Cyber | Sécuriser les systèmes d'exploitation
- AC35.01Cyber | Surveiller l'activité du système d'information
- AC35.03Cyber | Réagir face à un incident de sécurité
- AC35.04Cyber | Administrer les outils de surveillance du système d'information

Ressources mobilisées et combinées :

- R6.01 | Anglais : Insertion professionnelle 2
- R6.02 | Expression-Culture-Communication professionnelles : Communiquer en tant que futur cadre intermédiaire
- R6.Cyber.04 | Réponse à incident

Volume horaire :

Volume horaire : à définir localement par chaque IUT

4.2.2. STAGE.Cyber : Stage

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé
- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

Objectifs et problématique professionnelle :

Dans les domaines des Réseaux et des Télécommunications, le stage de fin d'études en 3ème année du B.U.T. R&T doit permettre à l'étudiant de valoriser l'ensemble de ses compétences au cours d'une expérience professionnelle significative dont les contenus et l'envergure doivent être conformes aux objectifs finaux des parcours, à savoir : « former des techniciens supérieurs et futurs cadres intermédiaires capables de comprendre, de mettre en œuvre, de configurer et de maintenir des équipements et systèmes d'information, tout en assurant leur sécurité physique et logicielle. »

Les mises en situations professionnelles doivent correspondre au parcours choisi et au projet professionnel et personnel de l'étudiant au travers de différentes missions dont voici une liste non exhaustive :

- analyser des risques d'attaques menaçant les systèmes d'informations d'une entreprise (réseaux, serveurs, postes de travail, ...)
- comprendre, déployer, tester une infrastructure ou une application informatique, mettre en place et maintenir un environnement Cloud adapté, ...
- fournir l'accès au réseau pour les entreprises ou les particuliers (fibres optiques, cœur de réseaux, ...), mise en place solutions multimédias de communication pour l'entreprise (téléphonie sur IP, visio-conférence, vidéo-protection), configurer et de maintenir le réseau de données d'une entreprise, ...
- analyser, piloter les demandes internes et externes de réseaux informatiques et de télécommunications des organisations quelles que soient leurs tailles en dialoguant avec les différents d'un projet ou d'un contrat, ...
- déployer, maintenir des technologies de communication (LoRa, Sigfox, NB-IoT, IEEE 802.15.4, WiFi, Bluetooth, 3G, 4G, 5G, xG). entre objets mobiles et communicants : téléphones, ordinateurs, véhicules, capteurs de toute nature.

Apprentissages critiques :

- AC31.01 | Concevoir un projet de réseau informatique d'une entreprise en intégrant les problématiques de haute disponibilité, de QoS, de sécurité et de supervision
- AC31.02 | Réaliser la documentation technique de ce projet
- AC31.03 | Réaliser une maquette de démonstration du projet
- AC31.04 | Défendre/argumenter un projet
- AC31.05 | Communiquer avec les acteurs du projet
- AC31.06 | Gérer le projet et les différentes étapes de sa mise en œuvre en respectant les délais
- AC32.01 | Déployer un système de communication pour l'entreprise
- AC32.02 | Déployer un réseau d'accès sans fil pour le réseau d'entreprise en intégrant les enjeux de la sécurité
- AC32.03 | Déployer un réseau d'accès fixe ou mobile pour un opérateur de télécommunications en intégrant la sécurité
- AC32.04 | Permettre aux collaborateurs de se connecter de manière sécurisée au système d'information de l'entreprise
- AC32.05 | Collaborer en mode projet en français et en anglais
- AC33.01 | Élaborer les spécifications techniques et le cahier des charges d'une application informatique
- AC33.02 | Mettre en place un environnement de travail collaboratif
- AC33.03 | Participer à la formation des utilisateurs
- AC33.04 | Déployer et maintenir une solution informatique
- AC33.05 | S'informer sur les évolutions et les nouveautés technologiques
- AC33.06 | Sécuriser l'environnement numérique d'une application
- AC34.01Cyber | Participer activement à une analyse de risque pour définir une politique de sécurité pour une petite structure
- AC34.02Cyber | Mettre en œuvre des outils avancés de sécurisation d'une infrastructure du réseau
- AC34.03Cyber | Sécuriser les systèmes d'exploitation
- AC34.04Cyber | Proposer une architecture sécurisée de système d'information pour une petite structure
- AC35.01Cyber | Surveiller l'activité du système d'information
- AC35.02Cyber | Appliquer une méthodologie de tests de pénétration

- AC35.03Cyber | Réagir face à un incident de sécurité
- AC35.04Cyber | Administrer les outils de surveillance du système d'information

Ressources mobilisées et combinées :

- R6.01 | Anglais : Insertion professionnelle 2
- R6.02 | Expression-Culture-Communication professionnelles : Communiquer en tant que futur cadre intermédiaire
- R6.03 | Connaissance de l'entreprise
- R6.Cyber.04 | Réponse à incident

4.2.3. PORTFOLIO : Démarche portfolio

Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé
- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

Objectifs et problématique professionnelle :

Au semestre 6, la démarche portfolio permettra d'évaluer l'étudiant dans son processus d'acquisition des niveaux de compétences de la troisième année du B.U.T., et dans sa capacité à en faire la démonstration par la mobilisation d'éléments de preuve argumentés et sélectionnés. L'étudiant devra donc engager une posture réflexive et de distanciation critique en cohérence avec le parcours suivi et le degré de complexité des niveaux de compétences ciblés, tout en s'appuyant sur l'ensemble des mises en situation proposées dans le cadre des SAÉ de troisième année.

Descriptif générique :

Prenant n'importe quelle forme, littérale, analogique ou numérique, la démarche portfolio pourra être menée dans le cadre d'ateliers au cours desquels l'étudiant retracera la trajectoire individuelle qui a été la sienne durant la troisième année du B.U.T. au prisme du référentiel de compétences et du parcours suivi, tout en adoptant une posture propice à une analyse distanciée et intégrative de l'ensemble des SAÉ.

Ressources mobilisées et combinées :

- R6.01 | Anglais : Insertion professionnelle 2
- R6.02 | Expression-Culture-Communication professionnelles : Communiquer en tant que futur cadre intermédiaire
- R6.03 | Connaissance de l'entreprise

Volume horaire :

Volume horaire : à définir localement par chaque IUT

4.3. Fiches Ressources

4.3.1. Ressource R6.01 : Anglais : Insertion professionnelle 2

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 6.Cyber.01 | Réagir face à une cyber-attaque
- STAGE.Cyber | Stage
- PORTFOLIO | Portfolio

Descriptif :

Contexte et ancrage professionnel :

Cette ressource apporte le socle de connaissances langagières pour les compétences de cœur de métier « Administrer les réseaux et l'Internet » et « Connecter les entreprises et les usagers ». Elle contribue aussi à la compétence « Créer des outils et applications informatiques pour les R&T » à travers des mises en situations, jeux de rôle, dialogues qui permettent la prise de parole en continu et en interaction, en développant les compétences de compréhension dans un contexte professionnel technique.

Contenus :

- Perfectionner ses compétences linguistiques et phonologiques
- Consolider les techniques de communication orale et écrite (argumenter, négocier, convaincre) ‘

Anglais de spécialité adapté aux parcours

Préconisations de mise en œuvre :

- Télécollaboration, télétandem, EMILE
- Mobilité à l'étranger (séjour linguistique, stage, semestre)
- Les ressources d'anglais seront utiles et à mettre en œuvre dans le PPP et portfolio notamment sur le volet internatio-nalisation

Apprentissages critiques ciblés :

- AC31.02 | Réaliser la documentation technique de ce projet
- AC31.04 | Défendre/argumenter un projet
- AC31.05 | Communiquer avec les acteurs du projet
- AC32.05 | Collaborer en mode projet en français et en anglais
- AC33.01 | Élaborer les spécifications techniques et le cahier des charges d'une application informatique
- AC33.03 | Participer à la formation des utilisateurs
- AC33.05 | S'informer sur les évolutions et les nouveautés technologiques

Mots clés :

Communication orale et écrite – Anglais technique de spécialité

Volume horaire :

Volume horaire défini nationalement : 8 heures dont 4 heures de TP

4.3.2. Ressource R6.02 : Expression-Culture-Communication professionnelles : Communiquer en tant que futur cadre intermédiaire

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 6.Cyber.01 | Réagir face à une cyber-attaque
- STAGE.Cyber | Stage
- PORTFOLIO | Portfolio

Descriptif :

Contexte et ancrage professionnel :

Le diplômé du B.U.T. R&T peut rapidement être amené à occuper des fonctions de cadre intermédiaire, dont la présente ressource explore quelques axes et outils.

Contenus :

- Consolider son expression formelle, remédiation (Projet Voltaire, Ecri+, ...);
- S'initier à l'activité de manager ;
- Savoir négocier par exemple dans le cadre de choix de matériel ou d'un budget ;
- Gérer des conflits ;
- Conduire le changement ;
- Décrypter les jeux de pouvoir.

Dans le cadre de l'animation de réunions, il doit pouvoir :

- réaliser un schéma clair, contextuel, parlant ;
- rédiger et énoncer une minute de lancement performante (pitch) ;
- rédiger et énoncer la minute de clôture pertinente.

En parallèle de ces éléments, il travaille également sur son insertion professionnelle ou sa poursuite d'études en :

- exploitant les réseaux sociaux professionnels (LinkedIn, ...) et les relations professionnelles qu'il a pu tisser lors de son stage ;
- développant l'entrepreneuriat et l'intrapreneuriat.

Ces contenus peuvent être complétés par des travaux autour des attendus de fin de formation (rapport écrit, soutenance orale, ...).

Apprentissages critiques ciblés :

- AC31.02 | Réaliser la documentation technique de ce projet
- AC31.04 | Défendre/argumenter un projet
- AC31.05 | Communiquer avec les acteurs du projet
- AC32.05 | Collaborer en mode projet en français et en anglais
- AC33.02 | Mettre en place un environnement de travail collaboratif
- AC33.03 | Participer à la formation des utilisateurs
- AC33.05 | S'informer sur les évolutions et les nouveautés technologiques

Mots clés :

Entreprenariat – Intrapreneuriat – Négociation – Prise de parole – Relation Client – Rapport – Soutenance

Volume horaire :

Volume horaire défini nationalement : 11 heures dont 4 heures de TP

4.3.3. Ressource R6.03 : Connaissance de l'entreprise

Compétences ciblées :

- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers
- Créer des outils et applications informatiques pour les R&T

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- STAGE.Cyber | Stage
- PORTFOLIO | Portfolio

Descriptif :

Contexte et ancrage professionnel :

Le technicien R&T salarié ou indépendant doit pouvoir évoluer en connaissant les grands axes du droit du travail afin de pouvoir s'insérer sereinement dans le monde professionnel, mais aussi en connaissant les aspects juridiques spécifiques liés aux R&T dans la mesure où ils imposent des contraintes dans la gestion des utilisateurs, dans la conception d'un système d'information ou de communication, d'une base de données, etc.

Contenus :

- Repérer les grandes fonctions dans l'entreprise et se situer dans son organisation (technique, managériale, commerciale, économique...)
- Connaitre l'environnement professionnel du salarié R&T (obligations et droits du salarié) : étude d'un contrat de travail, d'une fiche de paie, règlements communs, règlements intérieurs, conventions collectives, périodes d'essai, ruptures conventionnelles, prud'hommes...
- Appréhender l'environnement juridique propre aux R&T : étude de cas réels et concrets, responsabilité des fournisseurs d'accès et des prestataires de service, droits nationaux dans un réseau d'échanges internationaux, la sécurité des réseaux (ANSSI, directive NIS, loi de programmation militaire et OIV)...
- Appréhender l'environnement professionnel lié au RGPD : le RGPD et ses implications concrètes dans le travail du technicien RT (systèmes d'information, bases de données, sécurité, confidentialité...).

Préconisation de mise en oeuvre :

- Etude de documents réels et à jour, visite aux Prud'hommes, visite en entreprise (service RH), intervention d'un avocat spécialisé dans les questions numériques...
- Intervention d'un juriste en entreprise R&T, études de cas réels et concrets (FAI pour les professionnels sollicité par les services de police ou la justice afin de transmettre des données clients dans le cadre d'enquêtes ou renseignements)
- Intervention d'un formateur RGPD en entreprise auprès des techniciens SI ou DSi.

Apprentissages critiques ciblés :

- AC31.01 | Concevoir un projet de réseau informatique d'une entreprise en intégrant les problématiques de haute disponibilité, de QoS, de sécurité et de supervision
- AC31.03 | Réaliser une maquette de démonstration du projet
- AC32.01 | Déployer un système de communication pour l'entreprise
- AC32.02 | Déployer un réseau d'accès sans fil pour le réseau d'entreprise en intégrant les enjeux de la sécurité
- AC32.03 | Déployer un réseau d'accès fixe ou mobile pour un opérateur de télécommunications en intégrant la sécurité
- AC33.01 | Élaborer les spécifications techniques et le cahier des charges d'une application informatique
- AC33.02 | Mettre en place un environnement de travail collaboratif
- AC33.03 | Participer à la formation des utilisateurs

Mots clés :

Droit du travail – FAI – DSi – RGPD – Droits utilisateur – Obligations légales – Marché

Volume horaire :

Volume horaire défini nationalement : 11 heures dont 2 heures de TP

4.3.4. Ressource R6.Cyber.04 : Réponse à incident

Compétence ciblée :

- Surveiller un système d'information sécurisé

SAÉ au sein de laquelle la ressource peut être mobilisée et combinée :

- SAÉ 6.Cyber.01 | Réagir face à une cyber-attaque
- STAGE.Cyber | Stage

Descriptif :

Contexte et ancrage professionnel :

Suite à un incident sur son infrastructure, le professionnel R&T doit être en mesure d'intervenir et de continuer la cyber-attaque et de faire une analyse de celle-ci après coup.

Contenus :

En cas de suspicion d'intrusion ou d'incident, les diplômés seront capables :

- A chaud :
 - de reconnaître les artefacts symptomatiques des attaques usuelles sous Windows ou Linux
 - de prendre les bonnes décisions immédiates, dans le respect des directives fixées par le RSSI (PCA, ...), en gérant au mieux l'équilibre impacts opérationnels/risques d'aggravation.
- A froid :
 - d'effectuer les prélèvements (mémoire vive, disques, logs, ...) nécessaires pour les investigations forensiques futures et de les conserver
 - d'effectuer les premières investigations dans le strict respect du cadre juridique.

Apprentissage critique ciblé :

- AC35.03Cyber | Réagir face à un incident de sécurité

Mots clés :

Réponse à incident – CERT – PCA – PRA – Forensics – Forensique – Détection d'intrusion

Volume horaire :

Volume horaire défini nationalement : 18 heures dont 9 heures de TP