Fiche descriptive de module

Sécurité — ST220

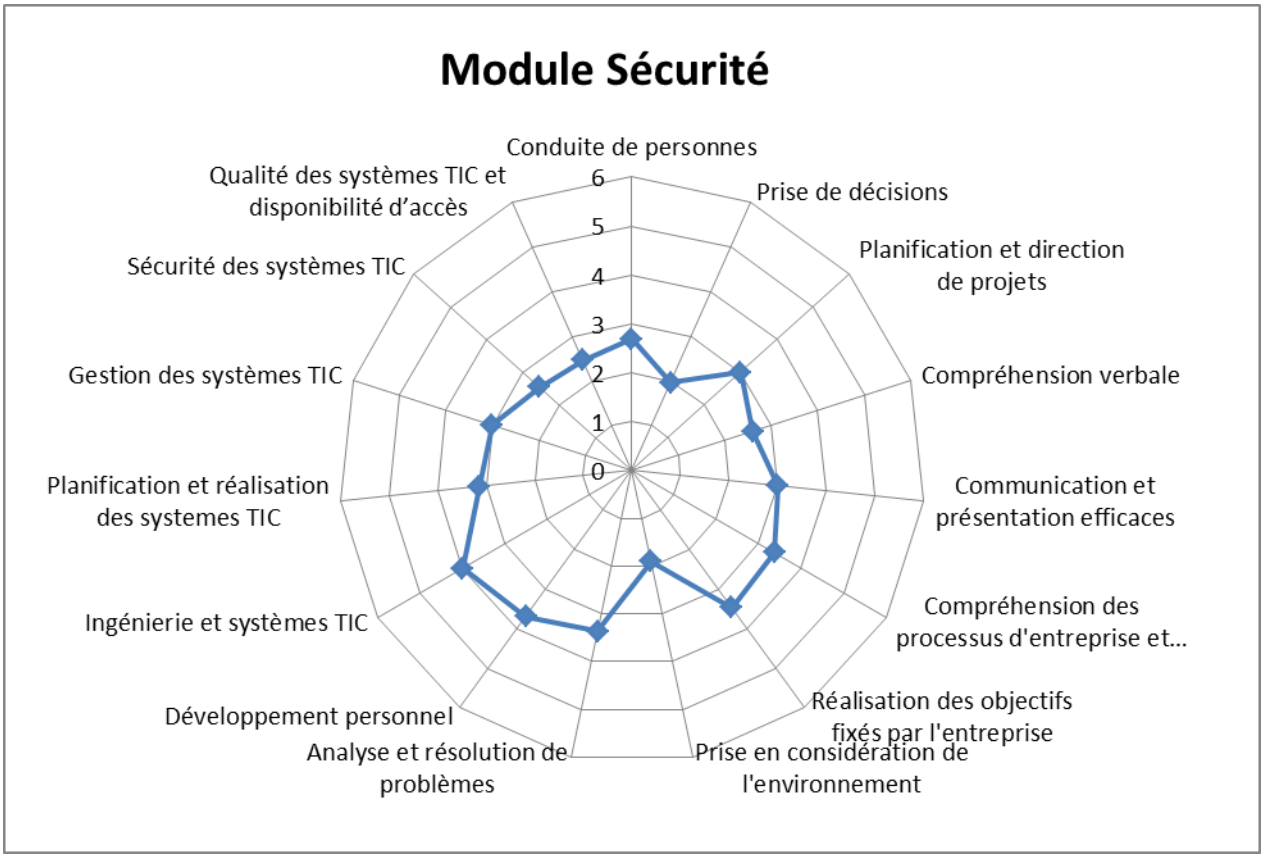
Pér. 1er semestre	*Pér. 2ème semestre*	*Pér. 3ème semestre*	*Total périodes:*	*Filière(s) / année*
		200	**200**	**STE / 2**

Numéro de version: 03-0
Date entrée en vigueur : 01.08.2017
Date de fin de validité :

Prérequis	Les prérequis sont fixés par le plan modulaire de la filière de formation.
Formes d'enseignement	Enseignements et exercices théoriques, applications pratiques en laboratoire de systèmes et réseaux
Processus PEC associés	01.1-01.2-01.3-01.4-02.1-02.3-03.1-03.2-03.3-03.4-04.1-04.3-04.4-05.1-05.2-05.3-05.4-05.5-05.6-06.1-06.2-06.3-07.1-07.2-08.2-08.3-08.4-08.5-09.1-09.2-09.3-09.4-09.5-10.1-10.2-10.3-11.1-11.2-11.3-11.4-12.1-12.3-12.4-12.5-12.6-12.7-13.1-13.2-13.3-13.4-13.5-13.6-14.1-14.2-14.3-15.1-15.2-15.3
Objectifs de compétences spécifiques	Mettre en place des systèmes de filtres réseau (firewall et proxy) Comprendre et appliquer les mécanismes de cryptographie Mettre en place et gérer des solutions VPN Utiliser les outils de monitoring et de détection d'intrusion
Modalité d'évaluation	Evaluations continues (théoriques et pratiques) dans chacun des cours La note de module est calculée en établissant la moyenne des moyennes de cours.
Conditions de réussite	La moyenne de ce module doit être égale ou supérieure à 4,0 La moyenne de chaque cours est calculée au dixième. La moyenne de module est calculée au dixième à partir des moyennes de cours pondérées selon le coefficient ci-dessous. *Les cas particuliers sont traités par la direction*
Remarques	

Contenu du module	*Cours*	*Titre / Contenu*	Coefficient	*Total pér.*
	$CRYP_{01}$	Cryptographie	1	30
	$IDST_{01}$	IDS et outils de test	2	60
	$VPNT_{01}$	VPN	2	60
	$FIRE_{01}$	Firewall et filtrage	2	50

Fiche descriptive de module



Fiche descriptive de cours

Cryptographie **CRYP**01

Pér. 1er semestre	*Pér. 2ème semestre*	*Pér. 3ème semestre*	*Total périodes:*	*Filière(s) / année*
		30	**30**	**STE / 2**

Module(s) intégrant ce cours	*Numéro(s)*	*Sigle(s)*	*Titre(s)*
	ST220		Sécurité
Formes d'enseignement	Enseignements théoriques et applications pratiques en laboratoire de systèmes et réseaux		
Objectifs de compétences	• Identifier les différents mécanismes de cryptographie: encryption, empreintes (C1) • Appliquer la cryptographie à l'authentification, à l'encryption et au contrôle d'intégrité (C3) • Choisir et expérimenter un système de type PKI et PGP (C3)		
Contenus	• Principes de base de la cryptographie • Calcul et utilisation d'empreintes (md5, SHA1): authentification et contrôle d'intégrité • Clés asymétriques et encryption • Certificats • PKI • PGP		
Modalité d'évaluation	Minimum 3 travaux notés (travaux écrits et travaux pratiques)		
Mode de validation finale des compétences	La note finale de cours est la moyenne arithmétique des notes de contrôle continu. Le mode de validation finale est défini dans la fiche de module.		
Remarques			

Fiche descriptive de cours

IDS et outils de test **IDST**01

Pér. 1er semestre	*Pér. 2ème semestre*	*Pér. 3ème semestre*	*Total périodes:*	*Filière(s) / année*
		60	**60**	**STE / 2**

Module(s) intégrant ce cours	*Numéro(s)* ST220	*Sigle(s)*	*Titre(s)* Sécurité
Formes d'enseignement	Enseignements théoriques et applications pratiques en laboratoire de systèmes et réseaux		
Objectifs de compétences	• Classifier les différents outils de sécurité (Monitoring, IDS, PENTEST) (C2) • Choisir et expérimenter un outil de monitoring (C3) • Choisir et expérimenter un IDS (C3) • Choisir et expérimenter un PENTEST (C3)		
Contenus	• Outils d'audit et de surveillance • Outils de détection d'intrusions (IDS) • Outils de test de pénétration (PENTEST)		
Modalité d'évaluation	Minimum 4 travaux notés (travaux écrits et travaux pratiques)		
Mode de validation finale des compétences	La note finale de cours est la moyenne arithmétique des notes de contrôle continu. Le mode de validation finale est défini dans la fiche de module.		
Remarques			

Fiche descriptive de cours

VPN **VPNT**01

Pér. 1er semestre	*Pér. 2ème semestre*	*Pér. 3ème semestre*	*Total périodes:*	*Filière(s) / année*
		60	**60**	**STE / 2**

Module(s) intégrant ce cours	*Numéro(s)* ST220	*Sigle(s)*	*Titre(s)* Sécurité
Formes d'enseignement	Enseignements théoriques et applications pratiques en laboratoire de systèmes et réseaux		
Objectifs de compétences	• Identifier les différents composants d'un VPN (C2) • Identifier les différentes architectures VPN (C2) • Choisir l'architecture et les protocoles adaptés selon les besoins (C3) • Proposer, installer et tester un VPN (C4)		
Contenus	• Virtual Private Network (VPN) • SSL / TLS		
Modalité d'évaluation	Minimum 4 travaux notés (travaux écrits et travaux pratiques)		
Mode de validation finale des compétences	La note finale de cours est la moyenne arithmétique des notes de contrôle continu. Le mode de validation finale est défini dans la fiche de module.		
Remarques			

Fiche descriptive de cours

Firewall et filtrage **FIRE**01

Pér. 1er semestre	*Pér. 2ème semestre*	*Pér. 3ème semestre*	*Total périodes:*	*Filière(s) / année*
		50	**50**	**STE / 2**

Module(s) intégrant ce cours	*Numéro(s)* ST220	*Sigle(s)*	*Titre(s)* Sécurité
Formes d'enseignement	Enseignements théoriques et applications pratiques en laboratoire de systèmes et réseaux		
Objectifs de compétences	• Planifier une DMZ (C3) • Proposer, installer et tester un firewall réseau (C4) • Proposer, installer et tester un proxy / firewall applicatif (C4)		
Contenus	• Principe de la DMZ • Mécanismes de translation d'adresses (NAT / PAT) • Les différents types de firewall • Principe et utilisation d'ACL (Access Control List) • Appliance Firewall • Proxy et firewall applicatif		
Modalité d'évaluation	Minimum 3 travaux notés (travaux écrits et travaux pratiques)		
Mode de validation finale des compétences			
Remarques			