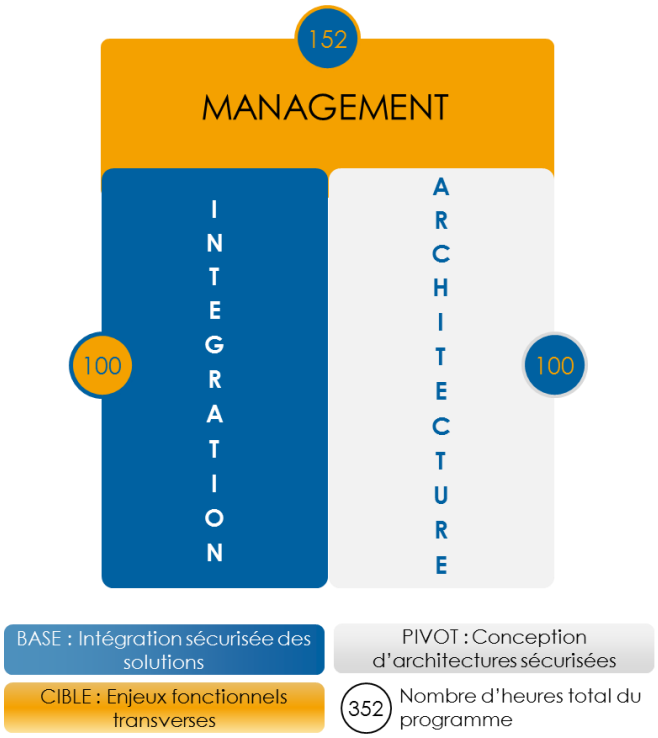
Programme

Mastère Spécialisé®
« Architecture Cyber-Sécurité et Intégration »

D'une durée de 352 heures, elle s'articule autour de trois composantes majeures : Intégration, Architecture et Management.



Il est essentiel de comprendre que la **composante de base Intégration** sécurisée précède la **composante pivot d'architecture** de sécurité. En effet, cela permet de bien comprendre les problématiques liées à l'intégration de parties différentes, qui doivent elles-mêmes répondre à des exigences de sécurité, avant d'aborder la partie conception d'architecture sécurisée. La pédagogie est donc inductive de la base à la cible en passant par le pivot. Elle part du terrain opérationnel (la base), pour remonter à la théorie et aux méthodes de conception (le pivot) pour **former des profils opérationnels concrets et pragmatiques** (la cible). Cette technique pédagogique est inspirée de certains parcours professionnels constaté sur le marché.

Composante Base : Intégration Sécurisée

- Durée : 25 demi-journées, 100 heures
- ECTS : 12 dont 8 ECTS pour les modules et 4 ECTS pour le projet transversal
- Cette composante permet de maîtriser les processus d'intégration sécurisée d'une solution SI
- Modules :

Infrastructures sécurisées	
Durée	7 demi-journées, 28 heures, dont 8 heures d'atelier
ECTS	2
Objectifs	Comprendre l'articulation des différents éléments composant l'infrastructure d'un SI d'entreprise
Thèmes	〉 Environnement physique 〉 Environnement virtuel 〉 Firewall (Next Generation, WAF – Web Application Firewall, etc.), diode, sonde, sandbox 〉 SIEM (Security Incident Event Monitoring) et SOC (Security Operations Center) 〉 Environnement sécurisé (accès, sécurité physique, bâtiment, etc.)

Serveurs	
Durée	8 demi-journées, 32 heures, dont 8 heures d'atelier
ECTS	3
Objectifs	〉 Comprendre les différents rôles d'un serveur dans le SI d'une entreprise 〉 Comprendre comment sécuriser les serveurs

Thèmes	〉 Hyperviseur 〉 IAM (Identity and Access Management) : Annuaire, méthode d'authentification (Kerberos, authentification forte, etc.), gestion des habilitations (autorisations d'accès), SSO – Single Sign-On, gestion des mots de passe) 〉 Cryptographie (fondamentaux des principes : symétrique, asymétrique, hachage), fondamentaux des services (chiffrement, signature, etc.), ingénierie de la cryptologie, infrastructures de gestion de clés (IGC), certificats, implantations matérielles et logicielles de la cryptographie, algorithmes, modes, etc.) 〉 DLP (Data Loss Prevention) : faire vivre la protection dans le temps : exfiltration d'un élément privé vers le public) 〉 OS – Operating Systems 〉 « Hardening » : comprendre les concepts (fermer les services qui ne servent plus à rien) 〉 Sécurité des bases de données, problématique Big Data, Open Data

Terminaux	
Durée	3 demi-journées, 12 heures
ECTS	1
Objectifs	〉 Comprendre les différents rôles d'un serveur dans le SI d'une entreprise 〉 Identifier les différents terminaux existant dans le SI d'une entreprise 〉 Comprendre comment les sécuriser
Thèmes	〉 PC, Tablettes et téléphones 〉 BYOD – Bring Your Own Device, antivirus, VPN – Virtual Private Network, Host IPS – Host Intrusion Prevention System 〉 MDM – Mobile Device Management, EDM – Enterprise Data Management, Master Data Management, Patch Management, Deploiement, Bug bounty, etc. 〉 OS – Operating Systems

Techniques pour l'intégration	
Durée	4 demi-journées, 16 heures
ECTS	2
Objectifs	〉 Appréhender la méthodologie d'intégration d'une nouvelle solution (maquettage, pré-production, production)

Thèmes	〉 Notion de Prod / Pré-prod 〉 La gestion du spécifique 〉 Ingénierie & retro-ingénierie 〉 Tests de non régression 〉 Prise en compte des impacts de déploiement 〉 Notion de VABF (Vérification d'Aptitude au Bon Fonctionnement) et de VSR (Vérification de Service Régulier) 〉 Tests intrusion 〉 Documentation 〉 Contrôle et audit : les types d'audit (organisationnel et technique avec les différentes variantes), et l'intégration dans le cycle sécurité d'un projet

〉 Projet transversal :

Projet : intégration sécurisée d'une solution	
Durée	3 demi-journées, 12 heures
ECTS	4
Objectifs	〉 Mettre en application les points précédents sur des solutions 〉 Aborder tous les aspects de l'intégration sécurisée d'une solution 〉 Ce premier projet jette les bases de la suite des 2 autres projets. 〉 **Il rassemble les compétences socle du présent cursus**
Thèmes	〉 Mise en œuvre des points précédents sur différentes solutions

Composante Pivot : Architecture Sécurisée

〉 Durée : 25 demi-journées, 100 heures

〉 ECTS : 12 dont 8 ECTS pour les modules et 4 ECTS pour le projet transversal

〉 Cette composante permet de maîtriser les processus de conception d'une architecture sécurisée dans le cadre d'une solution SI

〉 Modules :

Les architectures	
Durée	7 demi-journées, 28 heures, dont 8 heures d'atelier

ECTS	2
Objectifs	〉 Comprendre la différence entre une architecture pour le SI de Gestion et pour le SI Industriel (SCADAs), et architecture pour objets connectés 〉 Comprendre les différences entre l'architecture monolithique, multi-tiers et multi-tenante 〉 Connaitre les principes de défense en profondeur et de micro-segmentations
Thèmes	〉 Analyse de risques (ISO 27005, EBIOS-Expression des Besoins et Identification des Objectifs de Sécurité- de l'ANSSI, etc.) 〉 Différentes architectures (architecture systèmes, architectures applicatives, architectures réseaux, etc.) 〉 Spécificités du Cloud Computing (OnPremise / IaaS / SaaS / PaaS) et chiffrement homomorphe 〉 Electronique et architectures matérielles : attaques physiques, composants sécurisés, architecture des ordinateurs, systèmes embarqués, cartes à puce / éléments sécurisés. 〉 Sûreté des logs

Architectures réseaux	
Durée	7 demi-journées, 28 heures, dont 8 heures d'atelier
ECTS	3
Objectifs	〉 Comprendre le cloisonnement réseau et la communication unifiée
Thèmes	〉 Ruptures protocolaires (Proxies, PUM – Privilige User Management), DMZ – De-militarized Zone, problématique de pot de miel, black hole etc. 〉 Segmentations : VLAN – Virtual Local Area Network, ACL – Access Control List, NAC – Network Admission Control, etc. 〉 Interconnexion et chiffrement 〉 Intégration ToIP/VoIP 〉 Modèle d'interconnexion des systèmes ouverts (ISO), types de réseaux (réseaux privés, locaux, réseaux sans fil, réseaux étendus), routage, protocoles et services, équipements et produits de sécurité réseaux (pare-feu, sondes, passerelles, réseaux privés virtuels, concentrateurs, TLS, commutateurs, etc.)

Architectures applicatives	
Durée	6 demi-journées, 24 heures, dont 4 heures d'atelier
ECTS	2
Objectifs	〉 Comment sécuriser une application

Thèmes	〉 Vulnérabilité des applications 〉 Cycle de développement sécurisé OWASP – Open Web Application Security Project 〉 WAF – Web Application Firewall – et DDOS – Distributed Denial of Service 〉 Analyse de code & ingénierie logicielle 〉 Hardenning

Référentiels	
Durée	1 demi-journée, 4 heures
ECTS	1
Objectifs	〉 Initiation aux référentiels d'architecture existants
Thèmes	〉 TOGAF – The Open Group Architecture Framework, IAF – Integrated Architecture Framework (Framework d'architecture d'entreprise créé par Capgemini), etc. 〉 Les métiers de la sécurité 〉 Les organismes ANSSI, DGA, IHEDN, SGDNS, etc. 〉 ISO 27000, Cobit, ITIL

〉 Projet transversal :

Projet : conception de l'architecture sécurisée d'une solution	
Durée	4 demi-journées, 16 heures
ECTS	4
Objectifs	〉 Mettre en application les points précédents sur différentes architectures 〉 Concevoir l'Architecture Sécurisée d'une solution 〉 **Ce projet transversal intermédiaire constitue la bascule, le pivot du présent cursus permet de viser la cible métier, à savoir les architectures sécurisées**
Thèmes	〉 Mise en œuvre des points précédents dans différents contextes

Composante Cible : Management

〉 Durée : 38 demi-journées, 152 heures

〉 ECTS : 20 dont 13 ECTS pour les modules et 7 ECTS pour le projet transversal

〉 Cette composante permet de maîtriser les bases de la sécurité, tant au niveau de l'intégration que de l'architecture et de brosser la paysage de cette problématique. En effet, il est important de former des professionnels qui savent parfaitement de quoi ils parlent en toute connaissance de causes.

〉 Modules :

Ateliers : rentrée, suivi, soutenances des Thèses Professionnelles	
Durée	2 demi-journées, 8 heures
ECTS	-
Objectifs	〉 Constitution de la promotion 〉 Présentation du Mastère, de son fonctionnement, de son outillage
Thèmes	〉 Constitution d'équipe, faire connaissance, comprendre ses différences, ses richesses à partager 〉 Présentation de l'esprit et des règles Mastère, de son fonctionnement (calendrier, planning, notation, absences), de la mission de la thèse professionnelle, de son outillage (intranet « Moodle » et réseau social « Qu'OnPoste »), etc.

Panorama : de la sécurité de l'intégration à l'architecture	
Durée	4 demi-journées, 16 heures
ECTS	1
Objectifs	〉 Comprendre les piliers de la sécurité
Thèmes	〉 Mode de raisonnement de l'attaquant : logiciels malveillants, rétro ingénierie (black hats, white hats, hackers éthiques), etc. 〉 Stéganographie (notions) 〉 Contrainte de production et d'exploitation (« Comment raisonne l'attaquant ? Comment l'exploitant va-t-il faire vivre la solution en prenant en compte la réponse à la précédente question ? ») 〉 Anonymat et déférencement 〉 Données personnelles 〉 DICP (Disponibilité, Intégrité, Confidentialité, Preuve) 〉 Ecosystème 〉 Typologies de data et leur cycle de vie 〉 Normes, certifications, guides organisationnel : ISO2700x, ISO22301, plan de continuité d'activité (PCA), plan de reprise d'activité (PRA), standards industriels et métiers (PCI-DSS, W3C, IEEE, IETF, UIT, UEFI, etc.), management de la qualité, guides

	(ANSSI, ENISA, NIST, SANS, NSA/CSS, etc.), certifications et évaluations de produits schémas d'évaluation et de certification – critères Communs (CC), certification sécurité de premier niveau (CSPN) 〉 « Bonnes pratiques » / « hygiène » (cf les 40 règles d'hygiènes de l'ANSSI) 〉 Sensibilisation à la notion de ROI – Return On Investment – de la sécurité en amont (la sécurité n'est pas qu'un poste de coût !) 〉 Historique (de la cybersécurité, de la sécurité des systèmes d'information), vocabulaire et principes fondamentaux de la cybersécurité, objectifs et propriétés de la cybersécurité, objectifs et profils des attaquants, typologie des attaques, vulnérabilités, menaces et contre-mesures, malwares, type et évolution, principes de fonctionnement, protection contre les malwares, analyse et gestion de risques, acteurs de la cybersécurité, sûreté de fonctionnement. 〉 Contextes spécifiques

Retours d'expérience	
Durée	1 demi-journée, 4 heures
ECTS	-
Objectifs	〉 Comment capitaliser sur une expérience ?
Thèmes	〉 Lost review ou win review 〉 Fin projet 〉 Fiche de référence et témoignage client 〉 Veille technologique

Droit et réglementations	
Durée	5 demi-journées, 20 heures
ECTS	2
Objectifs	〉 Initiation aux bases juridiques 〉 Initiation aux bases de la règlementation
Thèmes	〉 Contrat d'un projet d'intégration 〉 Contrat d'achat revente 〉 Propriété intellectuelle 〉 Protection des Données Personnelles / CNIL – Commission Nationale Informatique et Libertés 〉 Exportation de produits sensibles 〉 Droit du travail

	〉 Droit et réglementation en France, en Europe, cas des opérateurs d'infrastructures vitales (OIV)

Les phases du projet	
Durée	6 demi-journées, 24 heures
ECTS	3
Objectifs	〉 Gérer le cycle de vie d'une réponse à Appel d'offre
Thèmes	〉 Méthode de pilotage de projet (par les risques ; le consommé, le reste à faire, etc.) 〉 Rédaction du RFI, cahier des charges 〉 Planification budgétaire 〉 Grille de sélection 〉 Avant-vente 〉 Soutenance 〉 Lancement du projet 〉 Méthodologies (cycle en V, AGILE / itérative, / en cloche) 〉 Contrôle et d'audit : audits technique et de configuration, intégration dans le cycle sécurité d'un projet 〉 Retours sur VABF (Vérification d'Aptitude au Bon Fonctionnement) et VSR (Vérification de Service Régulier) 〉 Documentations 〉 Exploitation 〉 Démarche d'homologation de sécurité

Management d'équipe	
Durée	4 demi-journées, 16 heures
ECTS	2
Objectifs	〉 Gérer le Appréhender la gestion humaine (client, équipe projet, etc.)
Thèmes	〉 L'équipe 〉 La relation client 〉 Le conflit

	〉 Le budget 〉 Le management des compétences 〉 La cellule de gestion de crise

Pilotage de projet	
Durée	5 demi-journées, 20 heures d'atelier
ECTS	3
Objectifs	〉 Apprentissage Par Projet du pilotage de projet appliqué sur le projet transversal
Thèmes	〉 Management d'équipe appliqué 〉 Gestion de projet appliquée

Outils du manager	
Durée	3 demi-journées, 12 heures d'atelier
ECTS	1
Objectifs	〉 Identifier les outils nécessaires au bon déroulement d'un projet
Thèmes	〉 Compte rendu de réunion 〉 Le danger du mail et du web 〉 The « brown paper » 〉 Diagramme de Gantt 〉 Suivi budgétaire

Technique de communication	
Durée	3 demi-journées, 12 heures d'atelier
ECTS	1
Objectifs	〉 Restituer un contenu à différents interlocuteurs
Thèmes	〉 Communication autour des aspects sociaux et sociétaux : Ingénierie sociale, phishing, contournement de la politique de sécurité, ergonomie de la sécurité, hygiène informatique, géopolitique et intelligence économique 〉 VISIO / PowerPoint / Excel 〉 Approche technique 〉 Approche cXo : cTo(Technical), cISo(Information Security Officer), cEo(Executif), cFo (Financial), cHo (Happiness), etc.

	〉 Approche interne 〉 Communication de en cas de gestion de crise

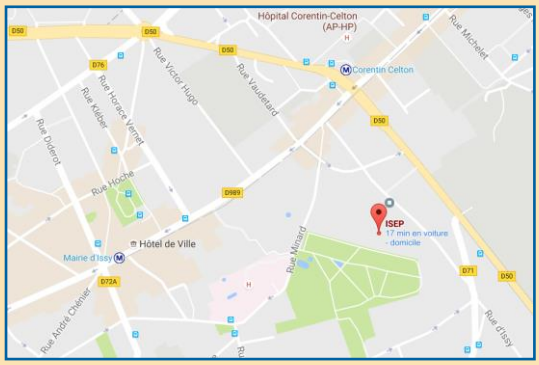
〉 Projet transversal :

Projet : management de l'Architecture à l'Intégration	
Durée	6 demi-journées, 24 heures
ECTS	7
Objectifs	〉 Mettre en application les points précédents dans différents contextes 〉 **Ce projet transversal est le point d'orgue de cette formation pour ce métier** 〉 Il fédère toutes les compétences des professionnels que nous formons 〉 Il capitalise les apprentissages vécus dans les 2 précédents projets transversaux
Thèmes	〉 Mise en œuvre d'un projet de bout en bout, de son architecture à son intégration

Une question ? Besoin de précisions ? Sollicitez-nous.

Aïcha ABDAT
Assistante administrative ISEP
Formation Continue
01 49 54 52 59
formation-continue@isep.fr

10, rue de Vanves
92130 Issy-les-Moulineaux



A TRES BIENTÔT !