Catalogue
Formations Cybersécurité
2017 - 2018

SEC-IT SOLUTIONS - 50 avenue du Docteur Aurientis 13100 AIX EN PROVENCE - RCS 823 114 087 Aix-en-Provence
Enregistré en qualité de prestataire de formation sous le numéro 93131665313 par le préfet de région PACA

1. PRESENTATION DE SEC-IT SOLUTIONS

SEC-IT SOLUTIONS est un cabinet spécialisé dans l'audit, le conseil et l'expertise en Sécurité du SI.

Les activités du cabinet sont réparties en **trois pôles** :

- Pôle « **Audit & Conseil** », composé de profils consultants, auditeurs, AMOA sécurité et chefs de projet sécurité. Ce pôle réalise les missions :
  - D'audits organisationnels, d'audit de gouvernance des données ;
  - D'audits de processus, de configuration, d'architecture ;
  - De tests d'intrusions (boite noire, boite grise, boite blanche) et d'audit de code ;
  - D'accompagnement à la définition de mesures de sécurité pour répondre aux standards, normes ou règlements tels que RGS, RGPD, ISO 27001, PCI-DSS, circulaire ARS… ;
  - De pilotage et d'accompagnement à l'implémentation de SMSI ;
  - De mesure de performance et d'amélioration de la sécurité dans les organisations ;
  - D'homologation des Systèmes d'Information ;

- Pôle « **Sécurité opérationnelle** », architectes et ingénieurs sécurité, pour les missions de :
  - Définition d'architecture, conception et coordination technique des projets sécurité réseau, infrastructures et applicatifs ;
  - Maintien en conditions de sécurité (MCS) ;
  - Détection et la gestion d'évènements et incidents de sécurité, administration des équipements et outils utilisés dans les SOC (SIEM, IDS/IPS…) ;
  - Réalisation des contrôles de sécurité récurrents (configuration, habilitations…) ;

- Pôle « **Formation** », pour répondre aux besoins des entreprises en matière de sensibilisation des utilisateurs, et aussi de formation en sécurité pour des profils techniques (administrateurs réseau, exploitants IT…). SEC-IT est inscrite au registre des organismes de formation.

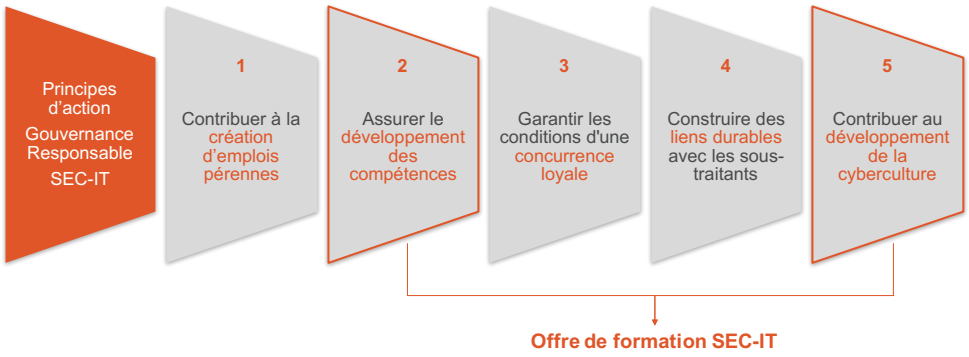
Nous réalisons des prestations sur l'ensemble du territoire, avec deux zones privilégiées : Rhône-Alpes-PACA et Ouest-IdF. Notre siège social est implanté à Aix-en-Provence.

Parmi nos clients :

CMA CGM, ASSEMBLÉE NATIONALE, BPCE INFOGÉRANCE & TECHNOLOGIES, néo-soft, cnrs, CFi, IBDO, NEOTION Innovation Attitude, NXO NEXTIRAONE

GOUVERNANCE RESPONSABLE ET FORMATION

Notre engagement à excercer une gouvernance responsable se traduit en 5 principes d'action issus de l'ISO 26000 (RSE) et présentés ci-dessous. La création d'une offre de formation contribue à nos objectifs de développement des compétences et de la culture cybersécurité :



POUR QUEL PUBLIC ?

Nos formations s'adressent à tous les contributeurs de la sécurité dans l'organisation, et particulièrement aux acteurs métiers, acteurs projets et équipes techniques :

- Responsables métiers, responsables et directeurs SI, directeurs et chefs de projet ;
- Développeurs logiciels, administrateurs techniques ;
- Intégrateurs de produits de sécurité ;
- Pentesteurs et équipes SOC.

APPROCHE PEDAGOGIQUE ET THEMATIQUES

Notre approche est de proposer des formations vivantes et concrètes. L'équipe pédagogique SEC-IT propose des modules de 1 à 3 jours, avec des mises en situation, l'analyse et le débat sur des cas concrets, des travaux pratiques.

La réalisation des sessions par nos collaborateurs, formateurs et experts cybersécurité confirmés, assure l'implication et l'interaction avec les stagiaires. Chaque session fait l'objet d'un questionnaire de satisfaction formation qui sert à l'amélioration continue de nos formateurs, de nos contenus et à la création de nouveaux modules.

L'axe de formation est développé autour de 3 thématiques majeures :

- Intégrer et valoriser la sécurité dans les projets SI;
- Auditer et sécuriser en profondeur ;
- Répondre aux exigences et évolutions réglementaires.

Nos thématiques de formation

- Sécurité du cycle projet SI
- Audit et défense en profondeur
- Conformité réglementaire

Modules de formation

Valoriser la sécurité dans le cycle projet

SAMM, SDLC, ISO 27001, Agilité, DevSecOps, vulnérabilités, risques, menaces, Top 10 OWASP, TOP 25 CWE SANS, SAST, DAST

1 jour
Jusqu'à 12 pers.

Présentation de la formation

Cette formation présente les principes de la sécurité intégrée directement dans le cycle de vie d'un projet, ainsi que les concepts du cycle de développement sécurisé (SAMM, SDLC) pour :

- Appliquer ces concepts dans la pratique
- Qualifier le niveau de sécurité adapté à chaque projet
- Définir et piloter les exigences de sécurité tout au long du projet
- Recueillir l'adhésion de l'équipe projet
- Garantir la bonne prise en compte des exigences
- Vérifier leur implémentation dans les livrables projet

Programme

INTRODUCTION
- Sécurité du cycle projet SI : de quoi parle-t-on ?
- Qu'est-ce qu'un risque, une menace, une vulnérabilité ?
- Illustration par bilan statistique et coûts moyens d'une fuite de données

PARTIE 1
- Principes de sécurité : se mettre à la place de l'attaquant
- Présentation de l'OWASP, du CWE SANS
- Plan d'Assurance Sécurité (PAS) et homologation du SI

PARTIE 2
- Le cycle de développement sécurisé : les concepts (SAMM, SDLC)
- L'agilité et la sécurité font-elles bon ménage ?
- DevOps vers DevSecOps

PARTIE 3
- Qualifier son niveau de sécurité
- Evaluer le budget du besoin en sécurité
- Les exigences fonctionnelles / techniques

PARTIE 4
- SAST (Static Application Security Testing)
- Revue et audit de code : Rapport type et actions de remédiaton
- DAST (Dynamic Application Security Testing) - recette de sécurité projet

Prérequis

Connaissances en méthodologies de projet (Cycle en V, Agile Scrum…)

Public visé : Chefs de projet, Product Owners, Managers, Lead Developper, Consultants en sécurité

Lieu Inter : Lyon
Tarif Inter : 560 € HT / pers.
Tarif Intra : Nous consulter

Développer des applications sécurisées

Security by design, Privacy by design, Top 10 OWASP, TOP 25 CWE SANS, données sensibles

2 jours
6-10 pers.

Présentation de la formation

Cette formation présente les principes et bonnes pratiques en matière de développement sécurisé.
Au programme :

- Définition et état de l'art pour le « Security by design » et le « Privacy by design »
- Recommandations "Secure Coding Guidelines" de l'OWASP
- Exercices pratiques sur des machines vulnérables

Programme

INTRODUCTION
- Sécurité des développements logiciels : de quoi parle-t-on ?
- Qu'est-ce qu'un risque, une menace, une vulnérabilité ?

PARTIE 1
- Principes de sécurité : se mettre à la place de l'attaquant
- Evaluer la sensibilité et la criticité des données manipulées (en vue de la GDPR)
- Présentation de l'OWASP et du CWE SANS

PARTIE 2
- Bonnes pratiques en matière de développement sécurisé
- Exigences GDPR et bonnes pratiques « *privacy by design* »
- Recommandations OWASP (présentation des *Guidelines* et autres *Cheat Sheet*)

PARTIE 3
- Les différentes vulnérabilités du Top 10 OWASP, Top 25 CWE SANS et leur exploitation
- Travaux pratiques sur machines vulnérables (DVWA, BWA), analyse de code et correctif :
  - Vulnérabilité XSS, injection SQL
  - Upload de fichier, redirection
  - Bypass et vol de session

EVALUATION DES ACQUIS

Prérequis

Pratique d'un langage de développement
Connaissances en gestion de base de données
Sensibilisation aux méthodologies de développement logiciel

Public visé : Architectes logiciels, Technical leaders, développeurs, intégrateurs logiciels, auditeurs techniques, testeurs

Lieu Inter : Lyon
Tarif Inter : 1130 € HT / pers.
Tarif Intra : Nous consulter

Sécuriser en profondeur : GNU/Linux

Linux, Grsecurity, LSM, LXC, MAC, Seccomp, Tomoyo

3 jours
6-8 pers.

Présentation de la formation

Cette formation avec travaux pratiques présente les différentes menaces et techniques de sécurisation en profondeur d'un système GNU/Linux :

- Présentation des menaces (les types de vulnérabilités, les méthodes d'exploitation)
- Les principes de sécurisation (réduction de la surface d'attaque, application du principe du moindre privilège…)
- Outils de sécurisation en mode utilisateur
- Techniques et patchs de durcissement avancé sur le noyau Linux

Programme

INTRODUCTION

- Présentation des menaces et vulnérabilités sur les systèmes Linux et de leurs méthodes d'exploitation

PARTIE 1

- Les principes de sécurisation : réduction de la surface d'attaque, application du principe du moindre privilège
- Sécurisation avancées en mode utilisateur (vérification d'intégrité, les chiffrement, les sauvegardes, confinement de processus, permissions spéciales, capacités)

PARTIE 2

- Sécurisation avancées en mode noyau avec travaux pratiques :
  - Mise en place d'un contrôle d'accès mandataire (Tomoyo)
  - Confinement de processus (LXC)
  - Réduction du principe de moindre privilège (file capabilities)
  - Application d'un patch de durcissement noyau (Grsecurity)

EVALUATION DES ACQUIS

Prérequis

Connaissances en administration de systèmes Linux (gestion des utilisateurs, permissions, processus, etc.)

Public visé : Administrateurs systèmes, ingénieurs systèmes, auditeurs techniques

Lieu Inter : Aix-en-Provence
Tarif Inter : 1875 € HT / pers.
Tarif Intra : Nous consulter

Auditer les composants middleware

Corruption de mémoire, exploitation, fuzzing, retro-ingénierie

3 jours
6-10 pers.

Présentation de la formation

Ce module avec travaux pratiques présente :

- Les différents types de vulnérabilités sur les clients lourds et les composants middleware
- Les méthodes et outils de détection de ces vulnérabilités
- Les techniques d'exploitation
- Les techniques de sécurisation

Programme

INTRODUCTION
- Principes de hacking éthique
- Sensibilisation à la norme d'audit ISO 19011
- Sensibilisation aux exigences légales concernant la rétro-ingénierie
- Présentation des différents types de vulnérabilités clients lourds et middleware (corruption de mémoire, mauvaise conception, TOCTOU, etc.)

PARTIE 1
- Présentation des techniques d'exploitation (techniques de base, contournement des mécanismes de protection, exemple de codes d'exploitation)
- Les techniques de recherche de vulnérabilités (audit de code source, rétro-ingénierie, fuzzing)

PARTIE 2
- Travaux pratiques sur des cas concrets de services et composants logiciels vulnérables :
  - Application des techniques et outils
  - Développement d'un exploit en scripting ou langage de développement

PARTIE 3
- Constitution du rapport d'audit : synthèse managériale, éléments de preuves, recommandations

EVALUATION DES ACQUIS

Prérequis

Connaissances de base des systèmes Linux
Pratique d'un langage de scripting (Bash, Python…)

Public visé : Ethical Hacker, pentesters, administrateurs systèmes, développeurs, consultants en sécurité

Lieu Inter : Aix-en-Provence
Tarif Inter : 1875 € HT / pers.
Tarif Intra : Nous consulter

Auditer une application Web

Audit de code, recette de sécurité, Top10 OWASP, outils DAST et SAST, BurpSuite, HackBar, Firebug, Zap Proxy, Checkmarx, SonarQube

3 jours
6-8 pers.

Présentation de la formation

Cette formation avec travaux pratiques présente :

- Les différents types de vulnérabilités applicatives Web (front-end, back-end, webservices…)
- Les méthodes et outils de détection
- Les techniques d'exploitation
- Les techniques de sécurisation

Programme

INTRODUCTION
- Principes de hacking éthique
- Sensibilisation à la norme d'audit ISO 19011
- Sensibilisation aux exigences légales concernant les tests d'intrusion
- Présentation des différents types de vulnérabilités Web et de leur exploitation

PARTIE 1
- Découverte d'outils utiles pour les tests d'intrusion : burpsuite, HackBar, firebug, Zap Proxy
- Les techniques de recherche de vulnérabilités (audit de code source, tests d'intrusion manuels, fuzzing)

PARTIE 2
- Mise en pratique de tests statiques : audit de code avec SonarQube ou CheckMarx : relecture des résultats et identification des faux positifs
- Mise en pratique de tests dynamiques sur machines vulnérables (XSS, injection SQL, bypass, vol de session, redirection…)

PARTIE 3
- Constitution du rapport d'audit : synthèse managériale, éléments de preuves, recommandations

EVALUATION DES ACQUIS

Prérequis

Pratique d'un langage de développement logiciel (JEE, PHP, JS, .NET, C#)
Connaissances en principes de conception Web
Connaissances en gestion de bases de données

Public visé : Développeurs, Chefs de projets techniques, intégrateurs, responsables applications, Product Owner, consultants sécurité

Lieu Inter : Lyon
Tarif Inter : 1875 € HT / pers.
Tarif Intra : Nous consulter

Comprendre la rétro-ingénierie

Angr, Assembleur, Gdb, IDA, ImmunityDgb, Intel x86, Linux, LXC, Python, Radare2

3 jours
6-8 pers.

Présentation de la formation

Cette formation initie les stagiaires à l'activité de rétro-ingénierie sur architecture x86 au travers du langage assembleur, des méthodes d'analyse et des outils spécifiques (désassembleurs, déboguer, sandbox, etc.).

Programme

INTRODUCTION
- → Rétro ingénierie : de quoi parle-t-on ?
- → Principes de hacking éthique
- → Sensibilisation à la norme d'audit ISO 19011
- → Sensibilisation aux exigences légales concernant la rétro-ingénierie

PARTIE 1
- → Introduction à l'assembleur x86 (les registres, les instructions, l'organisation de la mémoire, les interruptions, les conventions d'appel, les appels systèmes)
- → Les méthodologies d'analyse (statique vs dynamique)

PARTIE 2
- → Les outils (radare2 / IDA, gdb / ImmunityDBG, angr)
- → Mise en place d'un labo (virtualisation et cloisonnement, émulation de réseau sur environnement cloisonné)

PARTIE 3
- → Les protections : comprendre les techniques d'obfuscation, techniques d'anti-debug
- → Travaux pratiques sur cas concrets (sur binaires du type CrackMe ou KeygenMe, application malfaisante factice) : dans le cadre sécurisé du labo, apprendre à manipuler les binaires pour récupérer leur code et comprendre leur mécanique.

Prérequis

Pratique des langages de programmation C et C++
Connaissance de base des systèmes Linux

Public visé : Ethical Hacker, pentesters, administrateurs systèmes, développeurs, consultants sécurité

Lieu Inter : Aix-en-Provence
Tarif Inter : 1875 € HT / pers.
Tarif Intra : Nous consulter

FORMATION INTRA OU BESOIN SUR MESURE ? NOUS SOMMES A VOTRE ECOUTE

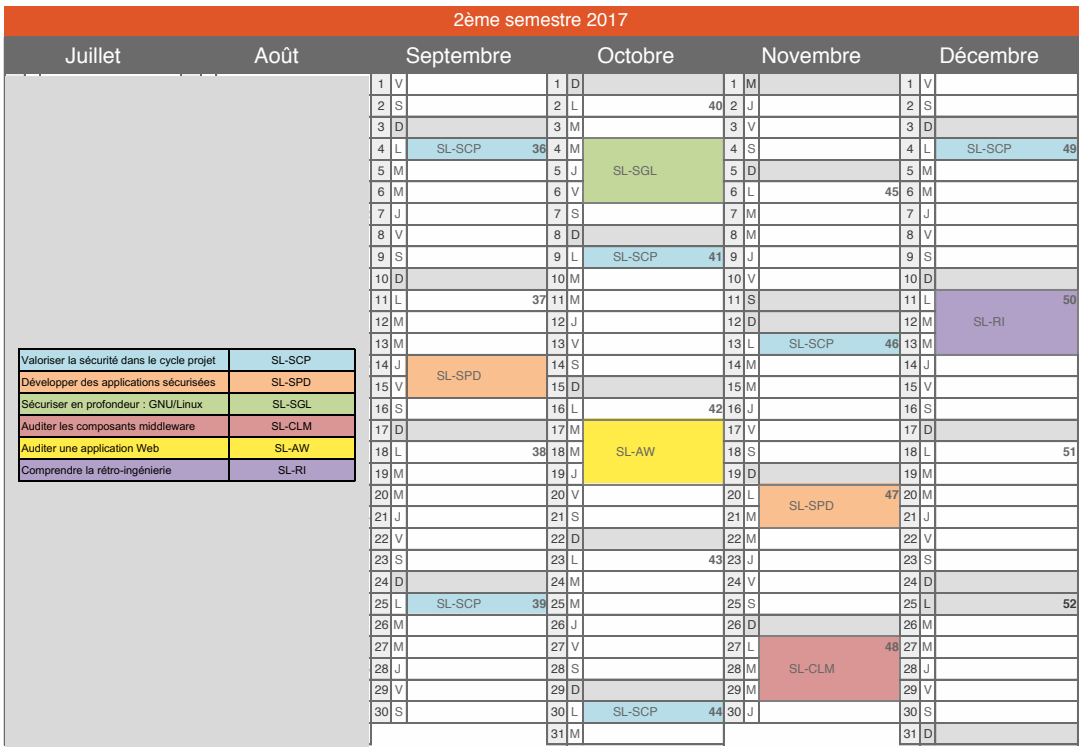
Notre équipe pédagogique est à votre écoute pour définir le parcours de formation spécifique répondant à vos besoins : réutilisation de vos contenus, adaptation des travaux pratiques à votre environnement…

SYNTHESE DE L'OFFRE DE FORMATION

Intitulé du module	Durée	Code	Tarif € HT *
Valoriser la sécurité dans le cycle projet	1 jour	SL-SCP	560
Développer des applications sécurisées	2 jours	SL-SPD	1130
Sécuriser en profondeur : GNU/Linux	3 jours	SL-SGL	1875
Auditer les composants middleware	3 jours	SL-CLM	1875
Auditer une application Web	3 jours	SL-AW	1875
Comprendre la rétro-ingénierie	3 jours	SL-RI	1875

(*) Tarif par stagiaire pour une formation inter-entreprise. Ce prix inclut les supports de cours, l'évaluation des acquis et les repas de midi.

CALENDRIER DES SESSIONS 2017-2018 INTRA ENTREPRISE



SEC-IT SOLUTIONS

SEC-IT SOLUTIONS
Catalogue Formations Cybersécurité 2017-2018

1er semestre 2018

Janvier			Février			Mars			Avril			Mai			Juin		
1	L	1	1	J		1	J		1	D		1	M		1	V	
2	M		2	V		2	V		2	L	14	2	M	SL-SGL	2	S	
3	M		3	S		3	S		3	M		3	J		3	D	
4	J		4	D		4	D		4	M		4	V		4	L	SL-SCP 23
5	V		5	L	SL-SCP 6	5	L	10	5	J		5	S		5	M	
6	S		6	M		6	M		6	V		6	D		6	M	
7	D		7	M		7	M		7	S		7	L	19	7	J	
8	L	SL-SCP 2	8	J		8	J		8	D		8	M		8	V	
9	M		9	V		9	V		9	L	SL-SCP 15	9	M		9	S	
10	M		10	S		10	S		10	M		10	J		10	D	
11	J		11	D		11	D		11	M		11	V		11	L	24
12	V		12	L	7	12	L	SL-SCP 11	12	J		12	S		12	M	
13	S		13	M		13	M		13	V		13	D		13	M	SL-AW
14	D		14	M	SL-AW	14	M		14	S		14	L	SL-SCP 20	14	J	
15	L	3	15	J		15	J		15	D		15	M		15	V	
16	M		16	V		16	V		16	L	16	16	M		16	S	
17	M		17	S		17	S		17	M		17	J		17	D	
18	J		18	D		18	D		18	M	SL-AW	18	V		18	L	25
19	V		19	L	8	19	L	12	19	J		19	S		19	M	
20	S		20	M		20	M	SL-CLM	20	V		20	D		20	M	
21	D		21	M		21	M		21	S		21	L	21	21	J	
22	L	4	22	J	SL-SGL	22	J		22	D		22	M	SL-SPD	22	V	
23	M	SL-SPD	23	V		23	V		23	L	17	23	M		23	S	
24	M		24	S		24	S		24	M	SL-RI	24	J		24	D	
25	J		25	D		25	D		25	M		25	V		25	L	SL-SCP 26
26	V		26	L	SL-SCP 9	26	L	13	26	J		26	S		26	M	
27	S		27	M		27	M	SL-SPD	27	V		27	D		27	M	
28	D		28	M		28	M		28	S		28	L	22	28	J	
29	L	5				29	J		29	D		29	M		29	V	
30	M					30	V		30	L	SL-SCP 18	30	M		30	S	
31	M					31	S					31	J				

2ème semestre 2018

Juillet			Août			Septembre			Octobre			Novembre			Décembre		
1	D		1	M		1	S		1	L	SL-SCP 40	1	J		1	S	
2	L	27	2	J		2	D		2	M		2	V		2	D	
3	M	SL-SPD	3	V		3	L	36	3	M		3	S		3	L	49
4	M		4	S		4	M		4	J		4	D		4	M	
5	J		5	D		5	M	SL-SGL	5	V		5	L	45	5	M	SL-SGL
6	V		6	L	32	6	J		6	S		6	M	SL-SPD	6	J	
7	S		7	M		7	V		7	D		7	M		7	V	
8	D		8	M		8	S		8	L	41	8	J		8	S	
9	L	28	9	J		9	D		9	M	42	9	V		9	D	
10	M		10	V		10	L	SL-SCP 37	10	M	SL-CLM	10	S		10	L	SL-SCP 50
11	M		11	S		11	M		11	J		11	D		11	M	
12	J		12	D		12	M		12	V		12	L	46	12	M	
13	V		13	L	33	13	J		13	S		13	M		13	J	
14	S		14	M		14	V		14	D		14	M		14	V	
15	D		15	M		15	S		15	L	42	15	J		15	S	
16	L	SL-SCP 29	16	J		16	D		16	M	SL-AW	16	V		16	D	
17	M		17	V		17	L	38	17	M		17	S		17	L	51
18	M		18	S		18	M	SL-AW	18	J		18	D		18	M	SL-RI
19	J		19	D		19	M		19	V		19	L	SL-SCP 47	19	M	
20	V		20	L	34	20	J		20	S		20	M		20	J	
21	S		21	M		21	V		21	D		21	M		21	V	
22	D		22	M		22	S		22	L	43	22	J		22	S	
23	L	30	23	J		23	D		23	M		23	V		23	D	
24	M		24	V		24	L	39	24	M		24	S		24	L	52
25	M		25	S		25	M	SL-SPD	25	J		25	D		25	M	
26	J		26	D		26	M		26	V		26	L	48	26	M	
27	V		27	L	SL-SCP 35	27	J		27	S		27	M		27	J	
28	S		28	M		28	V		28	D		28	M	SL-AW	28	V	
29	D		29	M		29	S		29	L	SL-SCP 44	29	J		29	S	
30	L	31	30	J		30	D		30	M		30	V		30	D	
31	M		31	V					31	M					31	L	1

Valoriser la sécurité dans le cycle projet	SL-SCP
Développer des applications sécurisées	SL-SPD
Sécuriser en profondeur : GNU/Linux	SL-SGL
Auditer les composants middleware	SL-CLM
Auditer une application Web	SL-AW
Comprendre la rétro-ingénierie	SL-RI

Votre interlocuteur SEC-IT

Pascal MONTEL
06 40 94 18 33
pascal.montel@sec-it-solutions.fr
www.linkedin.com/in/pascalmontel

www.sec-it-solutions.fr