# Catalogue de formations

Formations Techniques

Formations Organisationnelles

# Sommaire

## Formations Techniques



## Formations Organisationnelles

# Formations Techniques

## CODEX01 : COnnected Devices EXploitation

## CODEX02 : COnnected Devices EXploitation (Avancé)

## CRYPTO : Initiation à la cryptologie

## CERT : Réponse à incident et Inforensique

## SECDEV : Développement Web Sécurisé

# CODEX01 : COnnected Devices EXploitation

## Ce que nous vous proposons

- S'interfacer et communiquer avec un objet connecté
- Déterminer la surface d'attaque d'un objet connecté
- Extraire les micro-logiciels de différentes façons
- Analyser les micro-logiciels
- Identifier des vulnérabilités dans un micro-logiciel et les exploiter
- Conserver un accès résistant aux mises à jour de l'objet compromis

## Publics visés

- Pentesters IT
- Hackers
- Rétro-ingénierie
- Analystes inforensiques
- Concepteur de solutions connectées

## Prérequis

- Bases en ethical hacking
- Connaissance d'un langage de scripting : Perl, Python, Ruby
- Disposer d'un laptop pouvant exécuter une machine virtuelle

## Autres informations

- 4 375 € HT incluant les déjeuners
- 5 jours
- Fourniture d'un kit matériel complet
- Cours dispensé en anglais avec échanges possibles en français

## Le programme

### Introduction
- Sécurité matérielle
- Rappels d'électronique analogique et numérique
- Equipement de l'analyste
- Présentation du kit

### Rétro-ingénierie du schéma électronique
- Identification des composants
- Interconnexions et rôle
- Création de schéma de principe
- Analyse du schéma de principe

### Ports de communication série
- Protocole de communication UART
- Recherche de ports série et de leurs caractéristiques
- Astuces d'identification de ports série
- Interfaçage avec un ordinateur

### Protocoles de communication électroniques
- Capture de communications SPI
- Capture de communications I2C

### Extraction des micro-logiciels
- Interfaces de débogage et de programmation : JTAG, SWD, CC Debugger
- Exploitation des bootloaders
- Exploitation de mécanismes de mise-à-jour
- Chip-off et dump

### Rétro-ingénierie de micro-logiciels
- Système d'exploitation
- Interruptions matérielles
- Extraction de systèmes de fichiers
- Désassemblage et analyse du code machin

### Recherche de vulnérabilités
- Analyse de configuration
- Mots de passe faibles et par défaut
- Fonctionnalités cachées
- Vulnérabilités système

### Backdooring
- Mécanismes d'installation de porte dérobée
- Compilation de portes dérobées pour architectures embarquées : ARM, MIPS
- Persistance de la porte dérobée

### Communications sans-fil
- Introduction à la radio logicielle
- Utilisation simple de la radio logicielle : capture et rejeu de communications, brouillage
- Protocoles propriétaires : analyse d'un protocole propriétaire, attaque d'un équipement (alarme RF)
- Interception de communications SPI : détermination des caractéristiques RF, capture de paquets de données envoyés à un transceiver, réutilisation du transceiver (injection)
- Bluetooth Low Energy : capture de communications (btlejack), cassage de code d'appairage (btlejack), recherche de vulnérabilités et exploitation d'un cadenas connecté (bluepy)
- Attaque de clavier et souris sans-fil : protocole Enhanced ShockBurst, framework Mousejack, injection de frappes de touche, prise de contrôle de la souris

# CODEX02 : COnnected Devices EXploitation AVANCé

## Ce que nous vous proposons

- Contourner les protections contre l'extraction de micro-logiciel
- Obtenir un accès privilégié au système d'un objet connecté
- Analyser un micro-logiciel d'un système ne reposant pas sur un système d'exploitation
- Identifier et exploiter des vulnérabilités applicatives sur architecture ARM
- Réaliser des attaques par canaux auxiliaires afin de contourner des restrictions
- Identifier, analyser et exploiter de multiples protocoles de communications

## Publics visés

- Pentesters Hardware (débutant) IT
- Hackers
- Rétro-ingénierie
- Analystes inforensiques
- Concepteur de solutions connectées

## Prérequis

- Suivi du cours CODEX01, ou :
- Connaissance du langage assembleur (x86 ou ARM)
- Maîtrise d'un langage de scripting (Python, Ruby)
- Connaissances de base en électronique numérique
- Maîtrises des outils de mesure et d'analyse électronique
- Connaissance de base de la radio logicielle
- Disposer d'un laptop pouvant exécuter une machine virtuelle

## Autres informations

- 4 375 € HT incluant les déjeuners
- 5 jours
- Fourniture d'un kit matériel complet
- Cours dispensé en anglais avec échanges possibles en français

## Le programme

### Introduction
- Rappels et pré-requis
- Présentation du kit

### Extraction de firmware
- Contournements des mécanismes de protection
- Forcer un shell bootloader avec Pin2Pwn
- Exploitation de bootloaders pré-installés
- Exploitation de vulnérabilités SWD pour l'extraction de mémoire : STM32F1X, nRF51
- Extraction de mémoires eMMC (BGA) et TSOP48 : dessoudage, câblage et lecture, extraction par analyseur logique (sigrock et libsigrock)
- Post-traitement de mémoires de stockage NAND : traitement du spare area, cas des architectures IMX

### Rétro-ingénierie de micro-logiciel
- Architecture des micro-contrôleurs et SoC (rappels)
- Techniques de rétro-ingénierie pour systèmes embarqués : identification des primitives usuelles, interaction entre le CPU et les différents périphériques, utilisation avancée d'IDA Pro pour l'analyse de micro-logiciels
- Recherche de vulnérabilités

### Exploitation de vulnérabilités applicatives
- Exploitation de débordement de mémoire sur architecture ARM : recherche, analyse et exploitation d'une vulnérabilité sur Linux embarqué ; recherche, analyse et exploitation d'une vulnérabilité sur système simple
- Création de shellcodes ARM sur mesure

### Attaques side-channel
- Cold-boot attack pour extraction de firmware
- Extraction de clef de chiffrement par analyse de consommation (CPA)
- Power glitching
- Clock glitching

### Communications sans-fil
- Rappels de radio logicielle (SDR) : capture et rejeu, analyse de signal
- Bluetooth Low Energy : attaques de type Man-in-the-Middle, prise de contrôle de communications, recherche de vulnérabilités, exploitation
- Zigbee (802.15.4) : utilisation de KillerBee, exploitation de vulnérabilités 802.15.4
- Protocole Sigfox : détails du protocole Sigfox, capture de paquets Sigfox via SDR
- Protocoles LoRa et LoRaWAN : détails des protocoles LoRa et LoRaWAN, capture de communications LoRa, cassage de clef de chiffrement LoRaWAN par accès physique

# CRYPTO : Initiation à la cryptologie

## Ce que nous vous proposons

- Maîtriser les concepts de la cryptographie
- Connaître les différents mécanismes
- Appréhender les différents types et usages
- Comprendre leur robustesse et faiblesse
- Anticiper les futurs concepts

## Publics visés

- Chefs de projets
- Architectes
- Responsables et ingénieurs de production
- Développeurs

## Prérequis

- Connaissances basiques en mathématiques

## Autres informations

- 3 500 € HT incluant les déjeuners
- 5 jours
- Travaux pratiques pendant la formation
- Cours dispensé en français

## Le programme

**Introduction**
- Stéganographie
- Grands services «secrets» Navajos
- Principe(s) de Kerckhoffs
- Concepts mathématiques

**Cryptographie symétrique classique**
- Substitution mono et poly-alphabétique
- Vernam
- Permutation
- Enigma

**Chiffrement de flux**
- Concept
- Registre à décalage à rétroaction linéaire
- RC4
- WEP
- Le futur ?

**Chiffrement par bloc**
- DES, 3DES, AES
- Problématique de chaînage
- ECB, CBC, CTR

**L'aléatoire**
- Usages
- Sources physiques
- Sources logiques
- Attaque sur la pile TCP

**Les empreintes**
- Codes correcteurs d'erreurs
- RAID
- Reed-Solomon
- Fonctions irréversibles, Fonctions de hachage
- Famille SHA2
- HMAC

**La cryptographie asymétrique**

**La signature électronique**

**Les infrastructures de gestion des clés**
- Politique de certification
- Rôles importants
- Émission d'un certificat
- Formats de fichiers
- Révocation d'un certificat

**La robustesse**
- Capacités de calcul
- Compromis temps-mémoire
- Tables arc-en-ciel
- Clés et mots de passe
- Espace de clés
- Performances
- Force des algorithmes
- Tailles de clés minimales
- Attaques par canaux auxiliaires

**Chiffrement des flux réseaux**
- SSL - Versions
- SSL - Navigateurs
- SSL - procédure
- SSL - Attaques
- IPSEC

**Cryptographie quantique**
- Modalités
- Conséquences

# CERT : Réponse à incident et Inforensique

## Ce que nous vous proposons

- Comprendre les principes d'une réponse à incident et d'une analyse inforensique
- Appréhender la mise en œuvre, les outils et méthodologies associées

## Publics visés

- Intervenants en réponse à incidents & inforensique
- Managers et chefs de projets des équipes sécurité
- Membres de CERT/CSIRT

## Prérequis

- Connaissances techniques confirmées en sécurité

## Autres informations

- 3 500 € HT incluant les déjeuners
- 5 jours
- Ateliers pratiques pendant la formation
- Cours dispensé en français

## Le programme

**Analyse inforensique**
- Définitions et type d'attaque
- Principales étapes d'une analyse inforensique

**La notion de preuve**
- Définitions
- Intégrité et admission de la preuve
- Création d'une image
- Inforensique « dead » or « live »

**Analyse d'une image disque**
- Les différents types d'analyses
- Les types d'acquisition, d'outils et de méthodes

**Les images disques**
- Monter une image disque
- Création d'une image virtuelle

**Windows**
- Système de fichiers Windows
- Artefacts Windows

**Création d'une super Timeline**

**L'information en mémoire RAM**
- Capture de la mémoire (RAM)
- Analyse de la mémoire

**Analyse de malwares**

**Présentation générale d'Android**

**Analyse d'une application Android (APK) malveillante**

# SECDEV : Développement Web Sécurisé

## Ce que nous vous proposons

- Comprendre les enjeux de la sécurité applicative en environnement web
- Comprendre les vulnérabilités applicatives les plus courantes
- Déterminer la surface d'attaque d'une application web
- Appréhender les moyens de correction, de sécurisation et de prévention
- Comprendre l'intégration de la sécurité dans le SDLC

## Publics visés

- Développeurs

## Prérequis

- Connaissance des environnements web
- Pratique du développement

## Autres informations

- 1 800 € HT incluant les déjeuners
- 3 jours
- Travaux pratiques pendant la formation
- Cours dispensé en français

## Le programme

### Introduction

- Pourquoi la sécurité applicative ?
- Les normes et règlementations
- Les concepts généraux de la SSI : les besoins de sécurité, les types de données, la notion d'impact, la notion de risque
- Architectures des applications web

### Les vulnérabilités

- Introduction à l'OWASP
- Les systèmes de gradations
- Les différentes typologies
- Détection des vulnérabilités
- Le traitement de la vulnérabilité

### Rappels de cryptographie

- Chiffrement : rappel de crypto classique, principe de crypto moderne
- Signature
- Hachage

### Comprendre les vulnérabilités et les attaques les plus courantes

- Top 10 OWASP
- Les nouvelles vulnérabilités
- Exemples réels et étude de cas
- Collecte d'informations sensibles
- Vulnérabilités d'injection de code : cross-site scripting, SQL injection, Remote code execution
- Attaques sur les mécanismes d'authentification
- Téléchargement de fichiers malveillants
- Utilisation de composants vulnérables
- Vulnérabilités de logique métier
- Problèmes liés à la désérialisation de données

### Protection

- Bonnes pratiques de développement
- Gestion de l'authentification
- Sécurisation des cookies
- Gestion des en-têtes HTTP
- Gestion des mots de passe
- Gestion des droits d'accès
- Gestion des messages d'erreurs
- Gestion des données
- Gestion des téléversements
- Sécurisation de la base de données

### Garantir et maintenir la sécurité

- Supervision des logs
- Equipement de sécurité périmétriques
- Utilisation de Frameworks : de développement, pour les fonctions de sécurité, pour l'accès aux données
- Common Vulnerabilities and Exposures
- Ressources documentaires : guides de développement

# Formations Organisationnelles

ISO 27001 – Certified Lead Implementer

ISO 27001 – Certified Lead Auditor

ISO 22301 – Certified Lead Implementer

ISO 27005 – Certified Risk Manager

GSSI01 : RSSI : les outils & méthodes indispensables

GSSI02 : Organiser et piloter la gestion des risques de sécurité SI - Quelques clés pour aller à l'essentiel

RGPD01 : Fondamentaux RGPD

RGPD02 : Privacy framework et conformité  RGPD

ADRIOT : Analyse de risques en environnement IoT

# ISO 27001 – Certified Lead Implementer

## Ce que nous vous proposons

- Comprendre la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002, ainsi qu'avec d'autres normes et cadres réglementaires
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMSI
- Savoir interpréter les exigences de la norme ISO/CEI 27001 dans un contexte spécifique de l'organisation
- Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance, et la tenue à jour du SMSI
- Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives au Système de management de la sécurité de l'information

## Le programme

- **Jour 1** : Introduction à la norme ISO/CEI 27001 et initialisation d'un SMSI
- **Jour 2** : Planification de la mise en œuvre d'un SMSI
- **Jour 3** : Mise en œuvre d'un SMSI
- **Jour 4** : Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI
- **Jour 5** : Examen de certification

## Publics visés

- Responsables ou consultants impliqués dans le management de la sécurité de l'information
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management de la sécurité de l'information
- Toute personne responsable du maintien de la conformité aux exigences du SMSI
- Membres d'une équipe du SMSI

## Prérequis

- Une bonne connaissance de la norme ISO/CEI 27001 et des connaissances approfondies des principes de mise en œuvre.

## Autres informations

- Prix 3500 € HT coupon d'examen et déjeuners inclus
- 5j examen compris
- Cours dispensé en français

## Examen de certification

Après avoir maîtrisé l'ensemble des concepts relatifs aux Systèmes de management de la sécurité de l'information, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO/CEI 27001 Lead Implementer ». En étant titulaire d'une certification PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles pour mettre en œuvre la norme ISO/CEI 27001 dans une organisation.

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées pour la mise en œuvre du SMSI
- Les cours magistraux sont illustrés par des exemples basés sur une étude de cas
- Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification

# ISO 27001 – Certified Lead Auditor

## Ce que nous vous proposons

- Comprendre le fonctionnement d'un Système de management de la sécurité de l'information (SMSI) conforme à la norme ISO /CEI 27001
- Expliquer la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002, ainsi qu'avec d'autres normes et cadres réglementaires
- Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011
- Savoir diriger un audit et une équipe d'audit
- Savoir interpréter les exigences d'ISO/CEI 27001 dans le contexte d'un audit du SMSI
- Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011

## Le programme

- **Jour 1** : Introduction au Système de management de la sécurité de l'information et à la norme ISO/CEI 27001
- **Jour 2** : Principes, préparation et déclenchement de l'audit
- **Jour 3** : Activités d'audit sur site
- **Jour 4** : Clôture de l'audit
- **Jour 5** : Examen de certification

## Publics visés

- Auditeurs souhaitant réaliser et diriger des audits de certification du Système de management de la sécurité de l'information
- Responsables ou consultants désirant maîtriser le processus d'audit du Système de management de la sécurité de l'information
- Toute personne responsable du maintien de la conformité aux exigences du SMSI
- Experts techniques désirant préparer un audit du Système de management de la sécurité de l'information
- Conseillers spécialisés en management de la sécurité de l'information

## Prérequis

- Une bonne connaissance de la norme ISO/CEI 27001 et des connaissances approfondies sur les principes de l'audit.

## Autres informations

- Prix 3500 € HT coupon d'examen et déjeuners inclus
- 5j examen compris
- Cours dispensé en français

## Examen de certification

Après avoir maîtrisé les concepts d'audit démontrés et réussi l'examen, vous pourrez demander la certification « PECB Certified ISO/IEC 27701 Lead Auditor ». Cette certification, reconnue à l'échelle internationale, démontre que vous possédez l'expertise et les compétences nécessaires pour auditer des organismes basés sur les bonnes pratiques.

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées dans l'audit du SMSI
- Les cours magistraux sont illustrés par des exemples basés sur une étude de cas
- Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification

# ISO 22301 – Certified Lead Implementer

## Ce que nous vous proposons

- Comprendre la corrélation entre la norme ISO 22301 et les autres normes et cadres réglementaires
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMCA
- Savoir interpréter les exigences de la norme ISO 22301 dans un contexte spécifique de l'organisation
- Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et la tenue à jour du SMCA
- Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives au Système de management de la continuité d'activité

## Le programme

- **Jour 1** : Introduction à la norme ISO 22301 et initialisation d'un SMCA
- **Jour 2** : Planification de la mise en œuvre d'un SMCA
- **Jour 3** : Mise en œuvre d'un SMCA
- **Jour 4** : Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMCA
- **Jour 5** : Examen de certification

## Publics visés

- Responsables ou consultants impliqués dans le management de la continuité d'activité
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management de la continuité d'activité
- Toute personne responsable du maintien de la conformité aux exigences du SMCA
- Membres d'une équipe du SMCA

## Prérequis

- Une bonne connaissance de la norme ISO 22301 et des connaissances approfondies des principes de sa mise en œuvre.

## Autres informations

- Prix 3500 € HT coupon d'examen et déjeuners inclus
- 5j examen compris
- Cours dispensé en français

## Examen de certification

Après avoir maîtrisé l'ensemble des concepts relatifs aux Systèmes de management de la continuité d'activité, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO 22301 Lead Implementer ». En étant titulaire d'une certification PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles pour mettre en œuvre la norme ISO 22301 dans une organisation.

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées pour la mise en œuvre du SMCA
- Les cours magistraux sont illustrés par des exemples basés sur une étude de cas
- Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification

# ISO 27005 – Certified Risk Manager

## Ce que nous vous proposons

- Comprendre la relation entre la gestion des risques de la sécurité de l'information et les mesures de sécurité
- Comprendre les concepts, approches, méthodes et techniques permettant un processus de gestion des risques efficace et conforme à ISO/IEC 27005
- Savoir interpréter les exigences de la norme ISO/IEC 27001 dans le cadre du management du risque de la sécurité de l'information
- Acquérir les compétences pour conseiller efficacement les organisations sur les meilleures pratiques en matière de management du risque lié à la sécurité de l'information

## Le programme

- **Jour 1** : Introduction au programme de gestion des risques conforme à ISO/IEC 27005
- **Jour 2** : Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005
- **Jour 3** : Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification

## Publics visés

- Responsables de la sécurité d'information
- Membres d'une équipe de sécurité de l'information
- Tout individu responsable de la sécurité d'information, de la conformité et du risque dans un organisme
- Tout individu mettant en œuvre ISO/IEC 27001, désirant se conformer à la norme ISO/IEC 27001 ou impliqué dans un programme de management du risque
- Consultants des TI
- Professionnels des TI
- Agents de la sécurité de l'information
- Agents de la protection de la vie privée

## Prérequis

- Une compréhension fondamentale de la norme ISO/IEC 27005 et une connaissance approfondie de l'évaluation des risques et de la sécurité de l'information.

## Autres informations

- Prix 2380€ HT coupon d'examen et déjeuners inclus
- 3 jours examen compris
- Cours dispensé en français

## Examen de certification

Après avoir compris tous les concepts nécessaires du management du risque de la sécurité de l'information basé sur la norme ISO/IEC 27005, vous pouvez vous présenter à l'examen et demander une certification "PECB Certified ISO/IEC 27005 Risk Manager". En détenant un certificat PECB Risk Manager, vous serez en mesure de démontrer que vous avez les compétences et les connaissances nécessaires pour effectuer une évaluation optimale des risques de sécurité de l'information et gérer les risques de sécurité de l'information dans les délais impartis.

- Cette formation est basée à la fois sur la théorie et sur les bonnes pratiques utilisées dans le management du risque de la sécurité de l'information
- Les sessions de cours sont illustrées par des exemples basés sur des études de cas
- Les exercices pratiques sont basés sur une étude de cas qui comprend des jeux de rôle et des discussions
- Les tests de pratique sont similaires à l'examen de certification

# GSSI01 : RSSI, les outils & méthodes indispensables

## Ce que nous vous proposons

- Donner au nouveau RSSI les méthodes, outils et approches sur tout ce qui est important dans sa nouvelle vie

## Publics visés

- Nouvel RSSI
- RSSI cherchant à savoir par quel chantier commencer dans son activité

## Prérequis

- Aucun

## Autres informations

- 1 750 € HT incluant les déjeuners
- 2 jours
- Travaux pratiques pendant la formation
- Cours dispensé en français

## Le programme

### Introduction
- Ma nomination, mon organisation, ma hiérarchie
- Mon positionnement dans l'entreprise et ma lettre de mission

### Une politique de sécurité pour mon entreprise
- Un patrimoine informationnel à estimer (données, services métiers) ;
- L'analyse de risque, la base angulaire
- Rédiger sa politique de sécurité (PSSI)
- La présentation à la direction, son engagement, son support, son exemple

### Les métiers de l'entreprise
- Découverte des applications métiers, des processus et des méthodes projet
- Interviewer les directeurs sur leur business
- Travailler une déclinaison de la PSSI applicable
- Mettre en place les premiers indicateurs de contrôle pertinents

### Accueillir le collaborateur dans l'entreprise
- La sensibilisation à la sécurité du numérique et les enjeux pour l'entreprise
- La signature de la charte : quel est son contenu et l'impact pour le collaborateur

### La sécurité opérationnelle
- Maintien en conditions opérationnelles de sécurité
- Protection des données
- Sauvegarde et archivage
- Gestion des socles
- Aspects réseau et gestion des traces
- Gestion de la mobilité et des appareils mobiles
- Veille sécurité
- Tests d'intrusion
- Audits
- Gestion des incidents
- Continuité d'activité

### Les défis de l'identité, véritable projet d'entreprise
- Sa finalité et ses impacts
- Les difficultés de mise en place et de maintien

### Gérer les tiers de l'entreprise ou rassurer ses clients
- Prestataires de services
- Externalisation (Cloud, Solution as a Service)

### Standards – Normes – Règlements
- 27001 et ses cousines
- PCI DSS
- RGPD
- NIS

# GSSI02 : Organiser et piloter la gestion des risques de sécurité SI - quelques clés pour aller à l'essentiel

## Ce que nous vous proposons

Acculturer les participants à une approche pragmatique de la gouvernance SSI :
- Centrée sur les risques clés, en combattant les erreurs et approximations usuelles à l'origine d'évaluations approximatives
- Mettant la notion de « processus SSI » au coeur de l'approche organisationnelle

Appréhender quelques clés du pilotage de la sécurité SI et savoir les mettre en place en termes :
- D'identification des ressources SI les plus sensibles
- De cartographie des risques clés
- De mise en place du contrôle permanent SSI
- D'élaboration de tableaux de bord

## Publics visés

- Responsables de la filière risques / risques opérationnels / sécurité de l'information
- Responsables de la qualité / efficience au sein de la DSI
- Contrôleurs internes du périmètre DSI
- Managers, consultants et auditeurs sécurité
- Propriétaires ou gestionnaires de processus SSI

## Prérequis

- 2 à 3 ans d'expérience en gestion des risques SSI ou avoir suivi la formation « GSSI 01 : RSSI, les outils et méthodes indispensables »

## Autres informations

- 1 750 € HT incluant les déjeuners
- 2 jours
- Travaux pratiques pendant la formation
- Cours dispensé en français

## Le programme

### Organiser la gestion des risques SSI

**Organiser la gouvernance SSI**
- Transformation numérique & contexte d'évolution des risques
- Gouvernance SSI – Concepts – Objectifs & Apports
- Gouvernance SSI – Optimisation

**Elaborer le cadre constitutionnel SSI**
- Articulation du référentiel documentaire SSI
- Politique Générale de sécurité SI (PGSSI)
- Référentiel de directives de sécurité SI

**Concevoir une organisation SSI « pertinente » et savoir l'évaluer**
- Présentation d'un modèle d'organisation « universel »
- Présentation d'une approche d'évaluation de la maturité SSI d'une organisation

**Cadrer les pratiques pour analyser efficacement les risques SSI**
- Concepts fondamentaux
- Bonnes pratiques en matière d'identification / qualification / évaluation d'un risque

**La charte d'utilisation du SI, entre nécessité et paradoxe**
- Aspects clés de la formalisation
- Cyber-surveillance et opposabilité
- Exemples d'éléments de contenu

### Piloter la gestion des risques SSI

**Avant-propos**
- Complexité du pilotage de la SSI
- Un parti-pris au travers de quelques clés

**Identifier et classifier les ressources SI « sensibles »**
- De quoi parle-t-on ?
- Les enjeux
- L'approche
- Présentation d'un cas

**Cartographier les risques SSI**
- Ecosystème « Cartographier les risques SSI » & Notions fondamentales
- Référentiel de risques SSI clés : Approche méthodologique et exemple
- Méthodologie et outils

**Concevoir et déployer le contrôle permanent SSI**
- Elaborer une stratégie de contrôle SSI
- Notions de « contrôle interne » & « contrôle permanent »
- Notion de « processus SSI »
- Ecosystème SSI & exemple de processus SSI
- Démarche de mise en oeuvre du contrôle permanent SSI

**Concevoir un tableau de bord SSI**
- Quels contenus et finalités pour quels destinataires ?
- Principes méthodologiques
- Système d'indicateurs types issus du terrain
- Exemples de maquette de tableaux de bord

# RGPD01 : Fondamentaux RGPD

## Ce que nous vous proposons

- Comprendre les principes et enjeux du RGPD
- Appréhender les étapes d'une mise en conformité

## Publics visés

- DSI, RSSI
- DPO
- CIL
- Chef de projet RGPD
- Responsable ou propriétaire de données

## Prérequis

- Connaissances légales basiques

## Autres informations

- 800 € HT incluant le déjeuner
- 1 jour
- Cours dispensé en français

## Le programme

**Introduction et notions fondamentales**

- Enjeux et contexte
- Historique juridique
- Présentation RGPD & normes associées
- Vocabulaire et définitions
- Les acteurs de la protection des DCP
- Principes essentiels de la protection des DCP

**Mise en conformité RGPD**

- Démarche
- Organisation
- Cartographie des traitements
- Conformité juridique des traitements
- Gestion des risques
- Plan de mise en conformité

# RGPD02 : Privacy framework et conformité RGPD

## Ce que nous vous proposons

- Comprendre les principes et enjeux du RGPD
- Appréhender les étapes d'une mise en conformité
- Savoir mettre en œuvre un PIA
- Gérer l' « accountability »

## Publics visés

- DSI, RSSI
- DPO
- CIL
- Chef de projet RGPD
- Responsable ou propriétaire de données

## Prérequis

- Connaissances légales basiques

## Autres informations

- 2 350 € HT incluant les déjeuners
- 3 jours
- Cours dispensé en français

## Le programme

### Introduction et notions fondamentales

- Enjeux et contexte de la protection des données
- Impacts pour les entreprises
- Présentation RGPD
- Ecosystème normatif de la Privacy
- Norme ISO 29100
- Vocabulaire et définitions
- Acteurs de la protection des données

### Principes fondamentaux de la protection des données

- Principes de la Privacy
- Comparaison des principes ISO 29100 et RGPD
- Nouveautés apportées par le RGPD : sanctions, accountability, Privacy by Design, droits des personnes opérationnelles

### Démarche de mise en conformité RGPD

- Organiser la protection de la vie privée
- Cartographier les traitements de DCP
- Mettre en conformité les traitements
- Gérer les risques
- Planifier la mise en conformité

### Privacy Impact Assessment PIA

- Quand doit-on faire un PIA ?
- Méthodologie pour la réalisation d'un PIA (contexte, mesures, risques, décision)

# ADRIOT : Analyse de risques en environnement IoT

## Ce que nous vous proposons

- Comprendre l'intérêt d'une analyse de risques
- Connaître les risques inhérents à un écosystème IoT
- Maîtriser les risques liés aux lois et règlements
- Savoir exprimer des besoins de sécurité
- Savoir traiter et piloter les risques IoT

## Publics visés

- DSI, RSSI
- Risk managers
- Chefs de projets
- Architectes
- Directeur de l'innovation

## Prérequis

- Connaissances légales basiques
- Connaissances du traitement des risques

## Autres informations

- 1 750 € HT incluant les déjeuners
- 2 jours
- Cours dispensé en français

## Le programme

**Introduction**
- IoT, de l'objet à l'écosystème connecté : définitions
- Mise en perspective : enjeux et objectifs
- Méthodologies d'analyse de risques

**Architecture type d'un écosystème IoT**
- Composants matériels
- Infrastructures Cloud et services associés
- Applicatifs mobiles
- Protocoles de communication

**Cartographie et étude des risques**
- Lois et règlements
- Métriques à considérer
- Spécificités sectorielles à prendre en compte
- Identification et appréciation des risques
- Traitement des risques
- Processus d'acceptation des risques résiduels

**Conclusion : et après ?**
- Le suivi des risques, un processus itératif
- Veille juridique
- Veille en menaces et en vulnérabilités
- Détection des incidents de sécurité
- Réaction sur incident

# A propos d'Atos

Atos est un leader international de la transformation digitale avec 105 000 collaborateurs et un chiffre d'affaires annuel de plus de 11 milliards d'euros. Numéro un européen du cloud, de la cybersécurité et des supercalculateurs, le Groupe fournit des solutions intégrées pour tous les secteurs, dans 71 pays. Pionnier des services et produits de décarbonation, Atos s'engage à fournir des solutions numériques sécurisées et décarbonées à ses clients. Atos opère sous les marques Atos et Atos|Syntel. Atos est une SE (Société Européenne) cotée sur Euronext Paris et fait partie de l'indice CAC 40.

La raison d'être d'Atos est de contribuer à façonner l'espace informationnel. Avec ses compétences et ses services, le Groupe supporte le développement de la connaissance, de l'éducation et de la recherche dans une approche pluriculturelle et contribue au développement de l'excellence scientifique et technologique. Partout dans le monde, Atos permet à ses clients et à ses collaborateurs, et plus généralement au plus grand nombre, de vivre, travailler et progresser durablement et en toute confiance dans l'espace informationnel.

Pour en savoir plus, rendez-vous sur
atos.net
atos.net/career

Échangez avec nous :



CT-210810-JM-BR-Catalogue-de-formations-fr