# CATALOGUE DE FORMATIONS

FORMATIONS TECHNIQUES
&
FORMATIONS ORGANISATIONNELLES

digital.security

digital.security et ses 200 experts accompagnent les entreprises et les administrations afin de protéger les actifs de leur système d'information avec une approche mesurée des risques.

digital.security

L'activité de formation d'Econocom Digital Security est enregistrée sous le numéro 11755704275 auprès du préfet de région d'Ile-de-France

# 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

digital.security

# 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

## AUTRES INFORMATIONS

- **3 500 €** HT incluant les déjeuners
- 4 jours
- Fourniture d'un kit matériel complet

## 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 machine

### 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

digital.security

# 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

## AUTRES INFORMATIONS

- **4 375 €** HT incluant les déjeuners
- 5 jours
- Fourniture d'un kit matériel complet

## 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

digital.security

# 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

## 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

digital.security

# 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

## 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

digital.security

# 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

## PUBLIC VISÉ

Développeurs

## PRÉREQUIS

- Connaissance des environnements web
- Pratique du développement

## AUTRES INFORMATIONS

- **1 800 €** HT incluant les déjeuners
- 3 jours
- Travaux pratiques pendant la formation

## 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

**RSSI** : Les outils & méthodes pour survivre

**RGPD01**: Fondamentaux RGPD

**RGPD02** : Privacy framework et conformité RGPD

**ADRIOT**: Analyse de risques en environnement IoT

digital.security

# Formation RSSI : les outils & méthodes pour survivre

## 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 dans une PME
- 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

## 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

digital.security

# 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

## 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

digital.security

# 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

## 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)

digital.security

# 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

## 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

digital.security | econocom

**digital.security**

50 avenue Daumesnil
75012 Paris

formations@digital.security