

# Formation Test d'intrusion des objets connectés IOT

## Présentation

Cette formation en sécurité des objets connectés couvre l'écosystème IoT, la reconnaissance et la cartographie des systèmes IoT, l'analyse matérielle et du firmware, ainsi que les attaques sur les protocoles et réseaux IoT. Les participants apprendront également à sécuriser les interfaces web et mobiles, et à mettre en œuvre des contre-mesures pour protéger les objets connectés.

Durée : 21,00 heures (3 jours)

Tarif INTRA : Nous consulter

## Objectifs de la formation

- Identifier les menaces spécifiques et les réglementations en vigueur.
- Utiliser des outils pour cartographier et analyser les dispositifs IoT.
- Effectuer du reverse engineering et analyser les firmwares.
- Mettre en œuvre des attaques et des contre-mesures efficaces.
- Tester et renforcer la sécurité des applications et des services cloud associés.
- Identifier les vulnérabilités et proposer des recommandations de sécurité.

## Prérequis

- Une compréhension des concepts fondamentaux en informatique et en réseaux est essentielle.
- Avoir des bases en programmation (Python, C, ou C++) peut être très utile, surtout pour l'analyse de firmware et le reverse engineering.
- Avoir un bon esprit d'analyse pour comprendre et identifier les vulnérabilités dans les systèmes IoT.

## Public

Cette formation s'adresse aux professionnels de l'informatique souhaitant renforcer leurs compétences en sécurité IoT, aux étudiants et chercheurs en informatique ou cybersécurité, aux développeurs et ingénieurs concevant des solutions IoT, ainsi



qu'aux décideurs et gestionnaires responsables de la sécurité des objets connectés dans leur organisation.

## Programme de la formation

### 1/ Introduction à la Sécurité des Objets Connectés

- Définition et écosystème de l'IoT
- Architecture d'un système IoT : appareils, passerelles, cloud, applications mobiles
- Enjeux et menaces spécifiques à l'IoT
- Réglementations et normes en cybersécurité IoT (ISO 27001, IoT Security Foundation, GDPR, NIST)

### 2/ Reconnaissance et Cartographie des Systèmes IoT

- Identification des dispositifs IoT et cartographie du réseau
- Analyse des protocoles de communication IoT (MQTT, CoAP, Zigbee, LoRa, BLE, etc.)
- OSINT et collecte d'informations (Shodan, Censys, IoT search engines)
- Analyse des métadonnées et des configurations exposées

### 3/ Analyse Matérielle des Objets Connectés

- Démontage et reverse engineering du hardware
- Identification des ports de communication (UART, JTAG, SPI, I2C)
- Dumping et analyse de la mémoire flash (firmware extraction)
- Interception et manipulation des signaux radio (SDR, RFID, NFC)

### 4/ Analyse du Firmware et Exploitation des Vulnérabilités

- Techniques d'extraction du firmware (JTAG, SPI, NAND, UART)
- Analyse statique et dynamique du firmware
- Détection des vulnérabilités logicielles (buffer overflow, injections, failles crypto)
- Automatisation de l'analyse avec Binwalk, Radare2, Ghidra, Firmware Mod Kit

**5/ Attaques sur les Protocoles et Réseaux IoT**

- Sniffing et interception des communications réseau
- Analyse et exploitation des failles des protocoles IoT (Zigbee, Bluetooth, MQTT, LoRaWAN)
- Attaques MITM (Man-in-the-Middle) sur les objets connectés
- Détection et exploitation des vulnérabilités Wi-Fi (WPA2, KRACK, Evil Twin)

**6/ Sécurité des Interfaces Web et Mobile liées à l'IoT**

- Tests d'intrusion sur les applications mobiles IoT (Android/iOS)
- Reverse engineering des APK et identification des failles (Frida, JADX, MobSF)
- Sécurité des API IoT (REST, WebSockets, GraphQL)
- Attaques sur les services Cloud liés aux objets connectés

**7/ Exploitation et Contre-Mesures**

- Prise de contrôle d'un objet connecté à distance
- Attaques par déni de service (DDoS, botnets IoT - Mirai, Mozi)
- Bonnes pratiques de sécurisation des objets connectés
- Implémentation de mesures de défense : chiffrement, authentification, segmentation réseau

## Organisation

**Formateur**

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

**Moyens pédagogiques et techniques**

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.

- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

## **Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation**

### **En amont de la formation** *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

### **Tout au long de la formation**

- Évaluations continues réalisées par le formateur travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

### **À l'issue de la formation** *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

## **Accessibilité**

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.