PROGRAMME DE FORMATION

-

Sécurité des Objets Connectés — Niveau 1

Comprendre et exploiter les vulnérabilités IoT

Version	V1.0
Date	Mars 2026
Organisme	DVID SAS
Modalité	100% FOAD asynchrone (e-learning autonome)
Contact	contact@dvid.eu

Table des matières

1 Informations générales

Intitulé	Sécurité des Objets Connectés — Niveau 1 : Comprendre et exploiter les vulnérabilités
Modalité	100% FOAD asynchrone — e-learning autonome sur plateforme SaaS (experience.dvid.eu)
Support matériel	Carte open source DVID V2 (ESP32 + STM32)
Durée estimée	21 heures en autonomie
Délai d'accès	Sous 48h après validation de l'inscription et réception de la carte DVID
Tarif	3 000 € HT par apprenant (licence annuelle nominative)
Contact	contact@dvid.eu
Référent pédagogique	Arnaud COURTY
Référent handicap	Lionel CAUBET
NDA	75170346017
Catégorie Qualiopi	Actions de Formation (L. 6313-1, 1°)

2 Analyse du besoin

Avant toute inscription, un questionnaire d'analyse du besoin est transmis au bénéficiaire et/ou à l'entreprise commanditaire.

Ce questionnaire permet d'identifier le contexte professionnel, les objectifs visés, les compétences attendues et l'adéquation de la formation avec le projet du bénéficiaire.

Sur la base de cette analyse, le référent pédagogique valide l'inscription ou oriente vers un parcours plus adapté.

3 Objectifs opérationnels / Compétences acquises

À l'issue de la formation, l'apprenant sera capable de :

- **Cartographier** les surfaces d'attaque IoT.
- **Identifier** et **exploiter** des vulnérabilités matérielles, middleware et cloud.
- **Analyser** un firmware et extraire des artefacts sensibles.
- **Proposer** des mesures de remédiation adaptées.
- **Rédiger** un rapport technique complet.

4 Public visé et prérequis

4.1 Public visé

- Développeurs et intégrateurs IoT / systèmes embarqués
- Pentesters et chercheurs en sécurité
- Ingénieurs sécurité, RSSI, responsables produit IoT
- Décideurs IT souhaitant anticiper les risques liés à l'IoT

4.2 Prérequis

- Connaissances de base en sécurité informatique
- Connaissances Linux (ligne de commande)
- Notions de programmation (Python recommandé)

4.3 Prérequis techniques

- Ordinateur avec port USB et connexion internet stable
- Navigateur web récent (Chrome, Firefox, Edge)
- Carte DVID V2
- Logiciel de communication série (ex. : PuTTY, minicom, screen)

5 Positionnement à l'entrée

Avant le démarrage de la formation, un test de positionnement automatisé est proposé à l'apprenant sur la plateforme experience.dvid.eu.

Ce test évalue les connaissances en sécurité, réseaux, Linux et embarqué pour orienter l'apprenant vers le niveau adapté (Easy, Medium, Hard) et les modules pertinents.

6 Contenu pédagogique détaillé

Le parcours comprend 21 modules répartis en 4 catégories. Chaque module combine théorie, démonstration et pratique sur la carte DVID V2 ou l'environnement cloud virtualisé.

N°	Module	Description	Catégorie	Niveau	HW
1	**Découverte du DVID**	Prise en main de la carte DVID V2, identification des composants	Matériel	Facile	Oui
2	**Premier Flash**	Flasher un premier firmware sur la carte DVID	Matériel	Facile	Oui

3	**Découverte du protocole UART**	Lire les traces série, comprendre le brochage et la communication UART	Matériel	Facile	Oui
4	**Baudrate personnalisé**	Démontrer qu'un baudrate personnalisé n'améliore pas la sécurité	Matériel	Moyen	Oui
5	**Découverte des fiches techniques**	Lire une fiche technique pour extraire brochage et câblage	Matériel	Facile	Oui
6	**Comprendre I2C**	Comprendre le protocole I2C via l'analyse de trafic	Matériel	Facile	Oui
7	**Mot de passe codé en dur**	Détecter des secrets embarqués dans le code/firmware	Matériel	Facile	Oui
8	**Firmware non chiffré**	Extraire des secrets d'un firmware mal protégé via UART et clé AES	Matériel	Moyen	Oui
9	**Découverte du MQTT**	Principes du protocole MQTT, premiers pas avec clients et brokers	Middleware	Moyen	Non
10	**Policies MQTT mal configurées**	Exploiter des policies MQTT mal configurées	Middleware	Moyen	Non
11	**Harcèlement publicitaire**	Persistance publicitaire permettant l'exfiltration d'identifiants	Matériel	Facile	Oui
12	**Exposition de token de sécurité**	Repérer des tokens exposés et comprendre l'impact cloud	Cloud	Facile	Non
13	**API trop verbeuse**	Analyser la verbosité d'API et détecter des fuites d'informations	Cloud	Moyen	Non
14	**Découverte de la vulnérabilité CSRF**	Comprendre et reproduire une attaque CSRF	Cloud	Moyen	Non
15	**PKI Faible**	Analyser l'impact d'une mauvaise implémentation PKI	Cloud	Moyen	Non
16	**Mauvaise gestion des erreurs**	Exploiter une mauvaise gestion des erreurs dans un environnement cloud	Cloud	Moyen	Non
17	**Téléchargement arbitraire de fichiers**	Exploiter un téléchargement arbitraire pour accéder à des données	Cloud	Moyen	Non
18	**Identifiant d'objet prévisible**	Exploiter des identifiants prévisibles pour accéder à des données confidentielles	Cloud	Moyen	Non

19	**Écoute du trafic WiFi**	Capturer et analyser les données échangées sur un réseau Wi-Fi	Matériel	Moyen	Oui
20	**SSID WiFi masqué**	Démontrer qu'un réseau WiFi masqué n'est pas une mesure fiable	Matériel	Moyen	Oui
21	**Problème de vérification de signature du firmware**	Charger un firmware modifié en contournant la vérification de signature	Matériel	Moyen	Oui

7 Moyens pédagogiques et techniques

- Plateforme SaaS DVID (experience.dvid.eu) : modules e-learning interactifs, accessible 24/7
- Carte hardware DVID V2 (ESP32 + STM32) : pratique sur matériel réel pour les modules Matériel
- Environnement cloud virtualisé : labs sécurisés pour les modules Cloud et Middleware
- Documentation en ligne : guides, fiches techniques, références protocoles
- Assistance technique : email (contact@dvid.eu) + canal Discord dédié — délai de réponse < 48h ouvrées

8 Modalités d'évaluation

8.1 Évaluation continue (formative)

- Validation de chaque module par soumission d'une preuve technique (flag) sur la plateforme
- Suivi de progression automatisé via le dashboard apprenant (Skill Radar)

8.2 Évaluation finale (sommative)

- Challenge technique final intégrant plusieurs vulnérabilités à exploiter de manière combinée
- Seuil de réussite : réussite du challenge technique final

8.3 Attestation

Une attestation de fin de formation est délivrée automatiquement par la plateforme à tout apprenant ayant atteint le seuil de réussite. Une certification DVID est également délivrée (badge numérique).

9 Suivi et prévention des abandons

Suivi automatisé de la progression

Alertes d'inactivité à 7 / 14 / 21 jours

Relance par le référent pédagogique

Assistance technique par email (contact@dvid.eu) et Discord (délai < 48h ouvrées)

10 Accessibilité

Adaptations possibles : temps majoré, supports alternatifs, assistance personnalisée.
Référent handicap : contact@dvid.eu

11 Indicateurs de résultats

Collecte trimestrielle via la plateforme (complétion, satisfaction, réussite).
Publication sur dvid.eu dès la première cohorte terminée.