

FORMATIONS INTENSIVES · 2026

Bootcamps **Cybersécurité**

Quatre parcours pratiques pour comprendre, détecter, tester et traiter les risques numériques.

5 jours · 30 heures

Labs pratiques · Livrables professionnels

Prix public recommandé

120 000 DZD

Une gamme claire, quatre expertises

Les bootcamps sont conçus pour transformer les connaissances en compétences professionnelles. Chaque parcours a un objectif distinct, un public ciblé et des livrables concrets.

01 · Socle

Security+

Comprendre les concepts, les menaces, l'architecture et les opérations de cybersécurité.

02 · Défensif

SOC Analyst

Analyser les alertes, construire des détections et documenter une investigation.

03 · Offensif

Pentest Web & API

Tester des applications et des API dans un environnement autorisé.

04 · Investigation

DFIR

Préserver les preuves, reconstruire les faits et piloter la réponse à incident.

Comment choisir son parcours ?

Entrer en cybersécurité	Security+	Socle de connaissances et préparation certification
Travailler en SOC	SOC Analyst	Analyse d'alertes et règles de détection
Tester des applications	Pentest Web & API	Vulnérabilités documentées et rapport de test
Répondre à un incident	DFIR	Timeline, preuves et plan de remédiation

Certifications associées : CompTIA Security+ · CompTIA CySA+ · CEH v13 AI. Les examens officiels et vouchers sont inclus uniquement lorsqu'ils sont mentionnés dans le devis.

Bootcamp 01 · Socle

5 jours · 30 h

Socle Cybersécurité **CompTIA Security+**

Une formation intensive pour comprendre les fondamentaux de la cybersécurité et acquérir un socle applicable aux environnements IT modernes.

Niveau

Débutant
avancé

Public

Techniciens ·
Admins ·
Étudiants

Prix

120 000 DZD

Programme en 5 jours

J1 · Concepts & menaces

CIA, AAA, acteurs, vecteurs et vulnérabilités.

J2 · Architecture

Réseaux, cloud, IAM, segmentation et cryptographie.

J3 · Opérations

Durcissement, pare-feu, IDS/IPS, actifs et logs.

J4 · Vulnérabilités

Analyse, priorisation, patching et réponse à incident.

J5 · Gouvernance

Risques, conformité, continuité et examen blanc.

Ce que le participant emporte

- Labs guidés et quiz de validation
- Accès CertMaster Lab annoncé : 12 mois
- Examen blanc et plan de révision
- Attestation Code213

Parcours de certification : **CompTIA Security+** comme certification principale · **CompTIA CySA+** comme parcours défensif optionnel après le socle. Examens et vouchers non inclus par défaut.

Prérequis : aisance informatique, bases en réseaux et systèmes, lecture de l'anglais technique.

Bootcamp 02 · Offensif

5 jours · 30 h

Pentest Web & API

 Parcours offensif pratique

Apprendre à identifier, reproduire et documenter des vulnérabilités web et API dans un environnement de laboratoire autorisé.

Niveau

**Intermédiaire
à avancé**

Public

**Développeurs ·
Testeurs ·
Pentesters**

Prix

120 000 DZD

Programme en 5 jours

J1 · Méthodologie

Périmètre, règles d'engagement, cartographie et reconnaissance.

J2 · Authentification

Sessions, contrôles d'accès, IDOR et élévation de privilèges.

J3 · Injections

SQLi, XSS, command injection et logique métier.

J4 · API

Tokens, exposition de données et scénario complet.

J5 · Rapport

Criticité, preuves, remédiation et restitution client.

Ce que le participant emporte

- Cartographie d'une cible de laboratoire
- Fiches de vulnérabilités reproductibles
- Rapport de test d'intrusion
- Préparation possible CEH v13 AI ou eJPT

Parcours de certification : **CEH v13 AI** comme parcours offensif associé · **eJPT** comme alternative pratique du pentest. Examens et vouchers non inclus par défaut.

Règle de sécurité : tous les tests sont réalisés exclusivement dans les labs ou sur des systèmes couverts par une autorisation écrite.

Bootcamp 03 · Défensif

5 jours · 30 h

SOC Analyst

Detection Engineering

Passer d'une alerte brute à une investigation documentée et à une règle de détection testée.

Niveau

Intermédiaire

Public

Analystes SOC

• Admins • IT

Prix

120 000 DZD

Programme en 5 jours

J1 · Télémétrie

SOC, collecte des logs, normalisation et IoC.

J2 · Triage

Qualification, investigation, escalade et rapport.

J3 · Détection

Écriture, test, faux positifs et versioning.

J4 · Hunting

MITRE ATT&CK, hypothèses et validation.

J5 · Réponse

Playbooks, automatisation, reporting et cas final.

Ce que le participant emporte

- Rapport de triage d'une alerte
- Pack de règles de détection
- Fiche de threat hunting
- Préparation possible CompTIA CySA+

Parcours de certification : **CompTIA CySA+** comme parcours défensif associé · **BTL1** comme alternative pratique blue team.
Examens et vouchers non inclus par défaut.

Prérequis : bases en réseaux, systèmes, journaux et sécurité. Une expérience IT ou SOC est recommandée.

Bootcamp 04 · Investigation

5 jours · 30 h

DFIR Réponse à incident & investigation numérique

Transformer les traces techniques d'un incident en chronologie, décision et plan de remédiation.

Niveau

**Intermédiaire
à avancé**

Public

**Analystes N2 ·
Admins · RSSI**

Prix

120 000 DZD

Programme en 5 jours

J1 · Acquisition

Cadre, rôles, collecte et conservation des preuves.

J2 · Windows

Artefacts, événements, persistance et timeline.

J3 · Mémoire & réseau

Processus, connexions, captures et IoC.

J4 · Remédiation

Confinement, éradication, Linux, cloud et reprise.

J5 · Restitution

Cause probable, rapport, communication et scénario final.

Ce que le participant emporte

- Chronologie d'un incident
- Rapport d'investigation
- Fiche d'indicateurs de compromission
- Plan de confinement et remédiation

Parcours de certification associés : **ecIR** pour la réponse à incident · **FTIA** pour la threat intelligence. Examens et vouchers non inclus par défaut.

Prérequis : expérience en systèmes, réseaux ou sécurité. DFIR est un parcours avancé et ne convient pas à un débutant complet.