Portfolio & Offre de services

Conseil, audit et formation en cybersécurité

Taher Amine ELHOUARI

Expert indépendant • Auto-entrepreneur, Algérie

NOVEMBRE 2026

Une expertise au service de vos décisions

Un interlocuteur senior, des priorités de direction aux preuves techniques.

01	**Direction**	Définir la feuille de route, les responsabilités et les investissements.
02	**Assurance**	Comprendre les écarts de contrôle et préparer les audits.
03	**Opérations**	Améliorer la détection, la réponse et la reprise.
04	**Équipes**	Développer les compétences pour maintenir les progrès.

Taher Amine ELHOUARI

vCISO indépendant, conseiller senior, auditeur de systèmes de management et formateur certifié.

Plus d’une décennie

d’expérience professionnelle

Socle technique

Actif dans la technologie depuis 2010. Sécurité offensive, cyberdéfense et environnements critiques.

Vision de direction

Leadership SSI, responsabilité des risques, gouvernance et communication exécutive.

Activité indépendante

Auto-entrepreneur enregistré en Algérie depuis août 2024. Missions directes pour clients locaux et internationaux.

Un parcours technique et managérial

2016–2019

Sécurité technique et pilotage de projets

Taghellist Technology : Lead Penetration Tester. Smart Link Holding (SLC / Divona) : chef de projet SSI.

2019–2024

Conseil indépendant et fonctions spécialisées

Conseil et formation en freelance. Expériences chez Société Générale Algérie et iNET en 2023.

2025–2026

Direction SSI, conseil et opérations

EKSec : CISO et directeur du conseil et du CSIRT. GIE Monétique : responsable Sécurité, Risques et Conformité en 2025.

Depuis oct. 2026

Développement international

Directeur de la BU Cybersécurité EMEA chez Fortress Plus. Senior Security Expert chez Near Trust.

Une sélection de qualifications

Des compétences en direction, assurance et sécurité opérationnelle.

Leadership

CISSP • PMP • CCISO
CompTIA SecurityX
PECB Cybersecurity Master

Sécurité technique

CSA CCSK • TAISE
eCPPT • eCTHP
ISA/IEC 62443 Senior Lead Implementer

Systèmes de management

PECB ISO/IEC 27001 Master
PECB ISO 22301 Master
IPC Management Systems Auditor (CMSA)

Formation et nouveautés

PECB Certified GOLD Trainer
U.S. Data Privacy Officer
ISO 56001 Lead Implementer

Formation technique et managériale

Un socle académique qui relie le génie logiciel aux décisions de l’organisation.

Woolf / GMC School of Technology

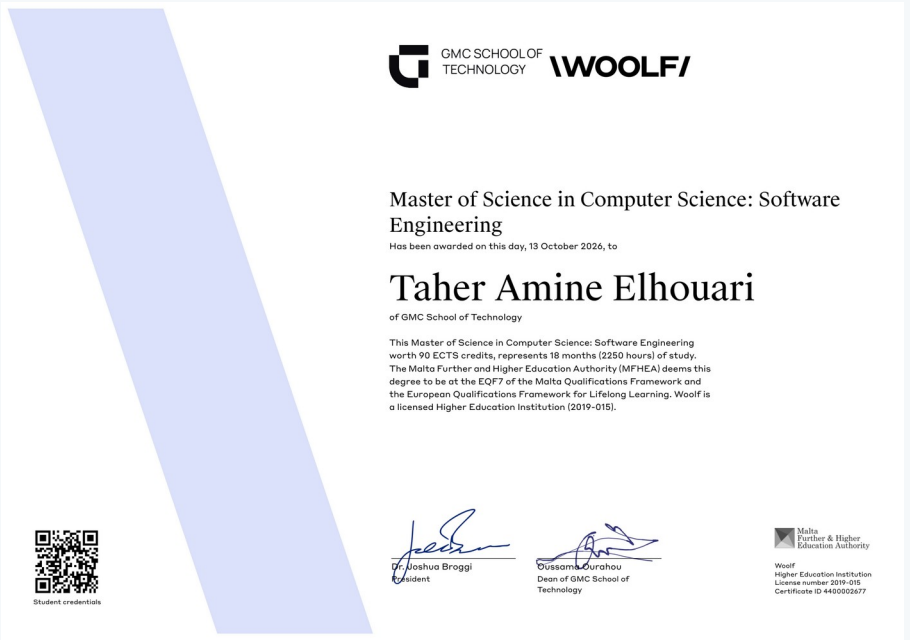
MSc in Computer Science: Software Engineering, 2026.

Atlanta College of Liberal Arts and Sciences

DBA, MBA et Master in Computer Science, 2026.

Formation complémentaire

Mini-MBA IBMI, 2022. Brevet de technicien supérieur en informatique et réseaux, Algérie.


GMC SCHOOL OF TECHNOLOGY
WOOLF

Master of Science in Computer Science: Software Engineering

Has been awarded on this day, 13 October 2026, to

Taher Amine Elhouari

of GMC School of Technology

This Master of Science in Computer Science: Software Engineering worth 90 ECTS credits, represents 18 months (2250 hours) of study. The Malta Further and Higher Education Authority (MFHEA) deems this degree to be at the EQF7 of the Malta Qualifications Framework and the European Qualifications Framework for Lifelong Learning. Woolf is a licensed Higher Education Institution (2019-015).

Student credentials

Dr Joshua Broggi
President

Oussama Ourahou
Dean of GMC School of Technology

Malta Further & Higher Education Authority

Woolf
Higher Education Institution
License number 2019-015
Certificate ID 4400002677

Un engagement au-delà des missions

Responsabilités communautaires, contributions d’expert et partage de connaissances.

Leadership communautaire

Président fondateur d’OWASP Algiers, CSA Algeria et CAS Algeria. Membre professionnel et contributeur expert AfricaCERT.

Contributions d’expert

Anciennes contributions SME aux examens et contenus ISC2, travaux avec Hack The Box et comités consultatifs EC-Council.

Conférences et médias

FIRST / AfricaCERT, SECURA North Africa et établissements supérieurs. Interventions à la télévision, à la radio et dans la presse.

Publications et reconnaissance

Podcast The InfoSec Control Room et Cyber Master Series. Global 30 Under 30 in Cybersecurity, Top Cyber News Magazine, 2026.

Portfolio / gouvernance des paiements

GIE Monétique • Responsable Sécurité, Risques et Conformité • 2025

≈374

contrôles de sécurité

Contexte

Un référentiel sectoriel pour l’écosystème algérien des paiements électroniques.

Contribution

Refonte des contrôles et correspondance entre les exigences de paiement, de SSI et les référentiels techniques.

Livrables

Objectifs de contrôle, preuves attendues, critères d’évaluation et suivi de remédiation.

Un exemple concret de lien entre exigences de contrôle et preuves utilisables en évaluation.

Portfolio / opérations et assurance

Opérations de sécurité et conseil

EKSec, 2025–2026

CISO et directeur du conseil et du CSIRT. Classification des incidents, escalade, catalogues de services, playbooks et reporting de direction.

Évaluation et investigation

Sélection de missions de conseil

Évaluations SMSI et continuité, investigations techniques et audits IT / SSI. Constats étayés et recommandations de remédiation.

Formation et communication exécutive

Cadres professionnels et institutionnels

Formations officielles PECB, ateliers de praticiens et conférences reliant gouvernance et sécurité opérationnelle.

Expérience sectorielle et besoins clients

Les missions s’adaptent à vos dépendances métiers et contraintes opérationnelles.

Banque et paiements

Gouvernance SSI, référentiels de contrôle, risques tiers et preuves d’évaluation.

Industrie et services critiques

Risques IT/OT, résilience opérationnelle, accès distants et responsabilités de sécurité.

Technologie et télécoms

Assurance des infrastructures, sécurité applicative, gouvernance cloud et opérations.

Secteur public et enseignement

Maturité cyber, systèmes de management, sensibilisation des dirigeants et formation.

Offre de services

Des missions cadrées, des livrables exploitables et un transfert de compétences.

CONSEILLER / ÉVALUER / DÉPLOYER / FORMER

vCISO et conseil aux dirigeants

Pour les organisations qui recherchent un pilotage SSI senior et flexible.

PÉRIMÈTRE D'INTERVENTION

01 Stratégie SSI et modèle opérationnel

02 Responsabilité des risques et investissements

03 Reporting exécutif et comités de pilotage

04 Supervision des programmes et coordination

VOS LIVRABLES

Feuille de route et actions priorisées

Charte de gouvernance et responsabilités

Tableau de bord et notes de décision

Une direction claire et un programme SSI responsabilisé.

Risques, conformité et sécurité des tiers

Pour établir une vision étayée de l’exposition et des écarts de contrôle.

PÉRIMÈTRE D’INTERVENTION

01 Maturité cyber et efficacité des contrôles

02 Analyse de risques ISO 27005 ou EBIOS RM

03 Cartographie des exigences et diagnostic

04 Évaluation des fournisseurs et traitement

VOS LIVRABLES

Registre des risques et plan de traitement

Matrice exigences, contrôles et preuves

Évaluation des tiers et registre d’actions

Des priorités fondées sur les risques métiers et les preuves.

SMSI et systèmes de management

Pour mettre en place, améliorer ou préparer un système de management à l’audit.

PÉRIMÈTRE D’INTERVENTION

01 Périmètre, contexte et analyse des écarts

02 Politiques, risques et conception des contrôles

03 Intégration opérationnelle et collecte de preuves

04 Revue de direction et amélioration continue

VOS LIVRABLES

Documentation SMSI et déclaration d’applicabilité

Responsables des contrôles et plan de déploiement

Préparation à l’audit et actions correctives

Un système de management exploitable par vos équipes.

Audit et évaluation indépendante

Pour les directions qui recherchent une assurance fondée sur les preuves.

PÉRIMÈTRE D’INTERVENTION

01 Audits internes et audits fournisseurs

02 Revues des systèmes et des contrôles techniques

03 Évaluation de préparation à la certification

04 Audits de certification sur mandat habilité

VOS LIVRABLES

Plan d’audit et constats étayés

Rapport de synthèse et priorités correctives

Évaluation du traitement des écarts

Le conseil et l’audit de certification restent distincts. La décision de certification relève de l’organisme certificateur.

Vie privée et protection des données

Pour structurer la gouvernance des données et les contrôles de protection.

PÉRIMÈTRE D’INTERVENTION

01 Cartographie des données et gouvernance

02 Appui aux analyses de risques et d’impact

03 Contrôles de protection et exigences fournisseurs

04 ISO/IEC 27701 et préparation aux audits

VOS LIVRABLES

Inventaire des traitements et analyse des écarts

Politiques et plan d’action

Preuves de contrôle et supports de sensibilisation

Les obligations applicables se cadrent avec votre fonction juridique ou protection des données.

Continuité et cyber-résilience

Pour maintenir les activités critiques face aux perturbations.

PÉRIMÈTRE D’INTERVENTION

01 Bilan d’impact et analyse des dépendances

02 Continuité d’activité et planification de reprise

03 Rôles de crise, escalade et communication

04 Exercices sur table et revue des plans

VOS LIVRABLES

BIA et stratégie de continuité

Plans de continuité et de reprise

Rapport d’exercice et actions d’amélioration

Des plans testables, alignés sur les priorités de reprise métier.

SOC, CSIRT et maturité de détection

Pour construire ou améliorer les capacités opérationnelles de sécurité.

PÉRIMÈTRE D'INTERVENTION

01 Maturité SOC/CSIRT et modèle de services

02 Couverture de détection et priorisation des cas

03 Gestion des incidents, escalade et playbooks

04 Indicateurs de performance et qualité

VOS LIVRABLES

Diagnostic et feuille de route d'amélioration

Catalogue de services, RACI et processus

Backlog de détection et playbooks opérationnels

Des services clairs et une meilleure coordination avec la direction.

Réponse aux incidents, DFIR et CTI

Pour préparer la réponse ou obtenir un appui d’investigation ciblé.

PÉRIMÈTRE D’INTERVENTION

01 Préparation et planification de la réponse

02 Investigation et analyse des preuves

03 Chasse aux menaces et renseignement cyber

04 Retour d’expérience après incident

VOS LIVRABLES

Playbooks et procédures de réponse

Constats d’investigation et chronologie

Plan de remédiation et amélioration de détection

L’appui en réponse dépend du périmètre, des accès et des disponibilités convenus.

Tests d’intrusion et assurance technique

Pour valider l’exposition par des tests de sécurité autorisés.

PÉRIMÈTRE D’INTERVENTION

01 Tests réseaux, infrastructures et applications

02 Validation des vulnérabilités et chemins d’attaque

03 Exercices red/purple team aux objectifs convenus

04 Revues de configuration et contre-tests

VOS LIVRABLES

Synthèse exécutive et constats techniques

Preuves, criticité et recommandations

Résultats des contre-tests et risques résiduels

Chaque test repose sur une autorisation écrite et des règles d’engagement.

Sécurité applicative et DevSecOps

Pour intégrer la sécurité dans le cycle de développement.

PÉRIMÈTRE D'INTERVENTION

01 Évaluation Secure SDLC et maturité applicative

02 Modélisation des menaces et revue d'architecture

03 Sécurité web/API et validation des contrôles

04 Exigences SSI et ateliers développeurs

VOS LIVRABLES

Feuille de route de sécurité applicative

Modèles de menaces et exigences

Backlog priorisé et critères de validation

Des exigences de sécurité intégrées au travail des développeurs.

Cloud, identités et architecture de sécurité

Pour évaluer la protection des systèmes, identités et services tiers.

PÉRIMÈTRE D’INTERVENTION

01 Gouvernance cloud et responsabilité partagée

02 Revues IAM/PAM, accès et configurations

03 Segmentation et conseil en architecture Zero Trust

04 Assurance fournisseurs et contrôles cloud

VOS LIVRABLES

Diagnostic d’architecture et de contrôles

Plan d’amélioration des accès et configurations

Preuves d’assurance cloud et registre des risques

Des décisions d’architecture et d’accès fondées sur les risques.

OT/ICS et infrastructures critiques

Pour des environnements où la sécurité respecte les contraintes d’exploitation.

PÉRIMÈTRE D’INTERVENTION

01 Gouvernance OT et évaluation de maturité

02 Risques industriels et dépendances

03 Segmentation, accès distants et gestion des actifs

04 Alignement ISA/IEC 62443 et coordination IT/OT

VOS LIVRABLES

Évaluation des risques et feuille de route OT

Recommandations de segmentation et d’accès

Exigences de sécurité et ateliers métiers

Les méthodes et limites de test se définissent avec l’exploitation.

Gouvernance de l’IA et de l’innovation

Pour encadrer les usages de l’IA et structurer les activités d’innovation.

PÉRIMÈTRE D’INTERVENTION

01 Inventaire des usages IA et analyse des risques

02 Politiques d’usage responsable et sensibilisation

03 Appui au système de management ISO/IEC 42001

04 Mise en œuvre du management ISO 56001

VOS LIVRABLES

Cadre de gouvernance IA et politique d’usage

Évaluation des risques et plan de contrôle

Processus d’innovation, rôles et indicateurs

Des responsabilités et contrôles clairs pour les nouveaux usages.

La formation au service des compétences

PECB Certified GOLD Trainer

60+

programmes PECB à délivrer

Formations officielles

Systèmes de management, cybersécurité, risques, audit et programmes professionnels associés.
U.S. Data Privacy Officer et ISO 56001 Lead Implementer.

Nouveaux programmes

Formats pédagogiques

Sessions à distance, intra-entreprise, ateliers pratiques et briefings exécutifs.



Le programme, la langue, les supports et les modalités d'examen figurent dans la proposition.

Les thématiques de formation

Programmes officiels et ateliers sur mesure selon les besoins de vos équipes.

Management SSI

ISO/IEC 27001, 27002 et leadership cyber.

Risques et audit

ISO 27005, ISO 31000, techniques d’audit et preuves.

Continuité et incidents

ISO 22301, gestion des incidents et exercices de crise.

Vie privée et IA

ISO/IEC 27701, U.S. CDPO et ISO/IEC 42001.

Sécurité technique

OT/ICS, cloud, sécurité applicative et pratiques offensives/défensives.

Management et innovation

ISO/IEC 20000, ISO 21502 et ISO 56001.

Ateliers, conférences et transmission

Des interventions adaptées au public et à un objectif pédagogique concret.

Briefings dirigeants

Décisions de risque, responsabilités SSI, usages de l’IA et résilience.

Ateliers praticiens

Registres des risques, preuves d’audit, playbooks et modèles de menaces.

Conférences et masterclasses

Carrières cyber, leadership, sécurité IT/OT et retours d’expérience.

Mentorat et ressources

Coaching d’équipe, parcours de progression et contenus pédagogiques originaux.

Conseil aux prestataires de cybersécurité

Un appui aux partenaires qui développent une activité ou un portefeuille de services.

Conception des services

Catalogues, méthodes de prestation, critères qualité et responsabilités.

Avant-vente technique

Ateliers de découverte, cadrage des besoins et propositions techniques.

Développement d’activité

Feuilles de route de compétences, partenariats et positionnement expert.

Contenus et accompagnement

Webinaires, présentations techniques, ressources et développement des équipes.

Quatre points de départ

Des missions autonomes ou la première étape d’un programme plus large.

01 / Diagnostic cyber

Revue ciblée de maturité et des contrôles. Synthèse des risques et feuille de route priorisée.

02 / Préparation à l’audit

Revue des preuves et des écarts d’un système de management. Plan d’actions correctives.

03 / Accompagnement vCISO

Conseil senior récurrent et supervision du programme. Reporting et appui aux décisions.

04 / Programme de compétences

Parcours de formation ou ateliers par rôle. Supports et méthode d’évaluation des acquis.

Une démarche de réalisation claire

01	**Cadrer**	Objectifs métiers, acteurs, systèmes et limites.
02	**Évaluer**	Preuves, entretiens et analyses ciblées.
03	**Prioriser**	Constats fondés sur les risques et ordre des actions.
04	**Réaliser**	Appui au déploiement, documentation ou formation.
05	**Transmettre**	Restitution, transfert et suivi convenu.

Des livrables utiles à vos équipes

Direction	Synthèse exécutive, risques clés et décisions à prendre.
Équipes opérationnelles	Constats détaillés, preuves et actions correctives priorisées.
Responsables des contrôles	Responsabilités, échéances et critères d’acceptation ou de contre-test.
Transfert de compétences	Documents de travail, ateliers et séances de restitution.

La proposition définit chaque livrable, son format, le processus de revue et les critères de clôture.

Modalités de mission et conditions commerciales

Une proposition adaptée au périmètre, à la complexité, au calendrier et au budget.

Identité contractante

Taher Amine ELHOUARI, auto-entrepreneur en Algérie. Activité enregistrée : Expert sécurité informatique.

Organisation

À distance par défaut. Besoins sur site, déplacements et disponibilité à convenir. Langue de prestation selon le public.

Modes d’intervention

Projet au forfait, journées de conseil, accompagnement récurrent ou session de formation. Honoraires sur devis après cadrage.

Clarté commerciale

Périmètre, contributions client, jalons, paiement, confidentialité et acceptation des livrables définis avant le démarrage.

Construisons votre prochaine mission

Partagez vos priorités, votre périmètre et vos échéances.
Recevez une proposition technique et commerciale adaptée.

Taher Amine ELHOUARI

Conseiller indépendant • Auditeur • Formateur PECB GOLD

contact@taheramine.org

+213 7 81 04 04 82

www.taheramine.org

Auto-entrepreneur, Algérie • Missions internationales