Portfolio & Service Offering

Cybersecurity advisory, audit & training

Taher Amine ELHOUARI

Independent professional • Auto-entrepreneur, Algeria

NOVEMBER 2026

Expertise that supports your decisions

A direct senior point of contact, from executive priorities to technical evidence.

01	**Direction**	Set a security roadmap, ownership and investment priorities.
02	**Assurance**	Understand control gaps and prepare for audits.
03	**Operations**	Improve detection, response and recovery capabilities.
04	**People**	Develop the skills needed to sustain progress.

Taher Amine ELHOUARI

Independent vCISO, senior advisor, management systems auditor and certified trainer.

More than a decade

of professional experience

Technical foundation

Active in technology since 2010. Experience across offensive security, cyber defence and critical environments.

Executive perspective

Security leadership, risk ownership, governance and board-level communication.

Independent practice

Registered auto-entrepreneur in Algeria since August 2024. Direct engagements for local and international clients.

A career across technology and leadership

2016–2019

Technical security & project delivery

Taghellist Technology: Lead Penetration Tester. Smart Link Holding (SLC / Divona): information security project management.

2019–2024

Independent consulting & specialist roles

Freelance consulting and training. Professional experience with Société Générale Algérie and iNET in 2023.

2025–2026

CISO, advisory & security operations

EKSec: CISO and Head of Advisory & CSIRT. GIE Monétique: Head of Security, Risk & Compliance in 2025.

Since Oct. 2026

International practice leadership

Director, Cybersecurity Business Unit, EMEA at Fortress Plus. Senior Security Expert at Near Trust.

Selected professional credentials

Qualifications spanning leadership, assurance and hands-on security.

Leadership

CISSP • PMP • CCISO
CompTIA SecurityX
PECB Cybersecurity Master

Technical security

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

Management systems

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

Training & recent additions

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

Technology and management education

An academic foundation that connects software engineering with organisational decisions.

Woolf / GMC School of Technology

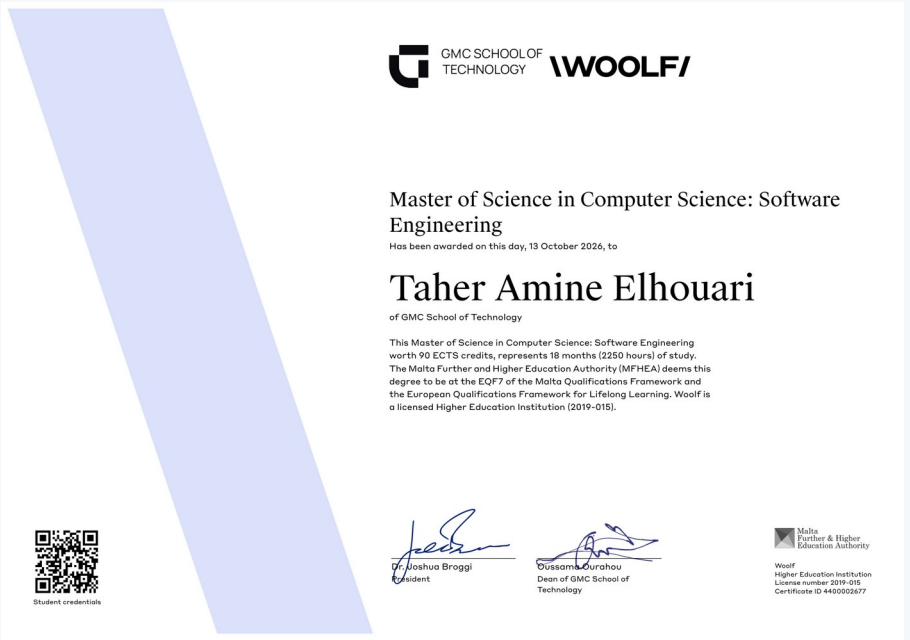
MSc in Computer Science: Software Engineering, 2026.

Atlanta College of Liberal Arts and Sciences

DBA, MBA and Master in Computer Science, 2026.

Additional education

IBMI Mini-MBA, 2022. Higher Technician diploma in IT & Networking, Algeria.


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

Professional contribution beyond assignments

Community leadership, expert contributions and knowledge sharing.

Community leadership

Founding leadership of OWASP Algiers, CSA Algeria and CAS Algeria. AfricaCERT professional member and subject-matter contributor.

Public speaking & media

FIRST / AfricaCERT, SECURA North Africa and higher education events. Television, radio and professional media contributions.

Expert contributions

Previous ISC2 examination/content SME work, Hack The Box contributions and EC-Council advisory board appointments.

Publishing & recognition

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

Portfolio / payment security governance

GIE Monétique • Head of Security, Risk & Compliance • 2025

≈374

security controls

Context

A sector security framework for Algeria’s electronic payments ecosystem.

Contribution

Restructured controls and mapped requirements across payment, information security and technical frameworks.

Deliverables

Control objectives, evidence expectations, assessment criteria and remediation tracking.

A concrete example of connecting control requirements with usable assessment evidence.

Portfolio / operations and assurance

Security operations & advisory

EKSec, 2025–2026

CISO and Head of Advisory & CSIRT. Work on incident classification, escalation, service catalogues, operational playbooks and management reporting.

Systems assessment & investigation

Selected consulting assignments

ISMS and continuity assessments, technical investigations and IT/SSI audit work. Evidence-based findings and remediation recommendations.

Learning & executive communication

Professional and institutional settings

Official PECB training, practitioner workshops and conference sessions connecting governance with operational security.

Sector experience and client needs

Engagements adapt to your business dependencies and operating constraints.

Banking & payments

Security governance, control frameworks, third-party risk and assessment evidence.

Industry & critical services

IT/OT risk, operational resilience, remote access and security responsibilities.

Technology & telecoms

Infrastructure assurance, application security, cloud governance and security operations.

Public sector & education

Cyber maturity, management systems, executive awareness and professional training.

Service offering

Assignments with a defined scope, practical deliverables and a clear handover.

ADVISE / ASSESS / IMPLEMENT / TRAIN

vCISO & executive advisory

For organisations that need senior security leadership on a flexible basis.

SCOPE OF WORK

01 Security strategy and operating model

02 Risk ownership and investment priorities

03 Executive reporting and steering committees

04 Programme oversight and stakeholder coordination

YOUR DELIVERABLES

Security roadmap and prioritised backlog

Governance charter and responsibility matrix

Management dashboard and decision briefs

A clear direction and an accountable security programme.

Risk, compliance & third-party assurance

For organisations that need a defensible view of exposure and control gaps.

SCOPE OF WORK

01 Cyber maturity and control effectiveness reviews

02 Risk analysis using ISO 27005 or EBIOS RM

03 Requirements mapping and compliance diagnostics

04 Supplier security reviews and risk treatment

YOUR DELIVERABLES

Risk register and treatment plan

Requirements-to-controls evidence matrix

Third-party assessment and action register

Priorities based on business exposure and documented evidence.

ISMS & management systems

For organisations implementing, improving or preparing a management system for audit.

SCOPE OF WORK

01 Scope, context and gap assessment

02 Policies, risk methodology and control design

03 Operational integration and evidence collection

04 Management review and improvement planning

YOUR DELIVERABLES

ISMS documentation and applicability statement

Control ownership and implementation plan

Audit preparation and corrective-action register

A management system that teams can operate and maintain.

Audit & independent assessment

For management teams seeking evidence-based assurance.

SCOPE OF WORK

01 Internal and supplier audits

02 Management system and technical control reviews

03 Certification readiness assessments

04 Certification audits under an authorised body mandate

YOUR DELIVERABLES

Audit plan and evidence-based findings

Executive report and corrective-action priorities

Follow-up assessment of corrective actions

Internal consulting and certification audit roles remain separate. Certification decisions belong to the certification body.

Privacy & data protection

For organisations structuring data governance and privacy controls.

SCOPE OF WORK

01 Data mapping and privacy governance reviews

02 Privacy risk and impact assessment support

03 Privacy controls and supplier requirements

04 ISO/IEC 27701 implementation and audit preparation

YOUR DELIVERABLES

Data processing inventory and gap analysis

Privacy policies and action plan

Control evidence and awareness materials

Applicable obligations are scoped with your legal or privacy function.

Continuity & cyber resilience

For organisations that need to sustain critical activities during disruption.

SCOPE OF WORK

01 Business impact analysis and dependency review

02 Continuity and disaster recovery planning

03 Crisis roles, escalation and communications

04 Tabletop exercises and recovery plan reviews

YOUR DELIVERABLES

BIA and continuity strategy

Business continuity and recovery plans

Exercise report and improvement actions

Testable plans aligned with business recovery priorities.

SOC, CSIRT & detection maturity

For security teams building or improving their operating capability.

SCOPE OF WORK

01 SOC/CSIRT maturity and service model review

02 Detection coverage and use-case prioritisation

03 Incident handling, escalation and playbooks

04 Performance metrics and operational quality

YOUR DELIVERABLES

Maturity assessment and improvement roadmap

Service catalogue, RACI and workflow definitions

Detection backlog and operational playbooks

Clearer services and stronger coordination between operations and management.

Incident response, DFIR & threat intelligence

For organisations preparing for incidents or seeking scoped investigation support.

SCOPE OF WORK

01 Incident readiness and response planning

02 Technical investigation and evidence review

03 Threat hunting and intelligence-led analysis

04 Post-incident review and lessons learned

YOUR DELIVERABLES

Response playbooks and incident procedures

Investigation findings and technical timeline

Remediation and detection improvement plan

Response support is subject to agreed scope, access and availability.

Penetration testing & technical assurance

For teams that need to validate exposure through authorised testing.

SCOPE OF WORK

01 Network, infrastructure and application testing

02 Vulnerability validation and attack-path analysis

03 Red/purple team exercises with agreed objectives

04 Configuration reviews and remediation retesting

YOUR DELIVERABLES

Executive summary and technical findings

Evidence, risk ratings and corrective guidance

Retest results and residual-risk observations

Written authorisation and agreed rules of engagement govern every test.

Application security & DevSecOps

For development teams integrating security throughout delivery.

SCOPE OF WORK

01 Secure SDLC and application maturity assessment

02 Threat modelling and architecture reviews

03 Web/API security and control validation

04 Security requirements and developer workshops

YOUR DELIVERABLES

Application security roadmap

Threat models and security requirements

Prioritised backlog and validation criteria

Security requirements that fit your development workflow.

Cloud, identity & security architecture

For organisations reviewing how systems, identities and providers are protected.

SCOPE OF WORK

01 Cloud governance and shared responsibility

02 IAM/PAM, access and configuration reviews

03 Segmentation and Zero Trust architecture advisory

04 Provider assurance and cloud control assessments

YOUR DELIVERABLES

Architecture and control gap assessment

Access and configuration improvement plan

Cloud assurance evidence and risk register

A risk-based view of architecture and access decisions.

OT/ICS & critical infrastructure

For industrial environments where security must respect operational constraints.

SCOPE OF WORK

01 OT security governance and maturity assessment

02 Industrial risk and dependency analysis

03 Segmentation, remote access and asset governance

04 ISA/IEC 62443 alignment and IT/OT coordination

YOUR DELIVERABLES

OT risk assessment and improvement roadmap

Segmentation and access recommendations

Operational security requirements and workshops

Assessment methods and testing constraints are agreed with operations.

AI governance & innovation management

For organisations adopting AI or structuring their innovation activities.

SCOPE OF WORK

01 AI use-case inventory and risk assessment

02 Responsible AI policies and security awareness

03 ISO/IEC 42001 management system support

04 ISO 56001 innovation management implementation

YOUR DELIVERABLES

AI governance framework and use policy

Risk assessment and control improvement plan

Innovation process, roles and performance measures

Clear ownership and controls for new technologies and innovation.

Training that builds working capability

PECB Certified GOLD Trainer

60+

PECB delivery programmes

Official training
Management systems, cybersecurity, risk, audit and related professional programmes.

Recent additions
U.S. Data Privacy Officer and ISO 56001 Lead Implementer.

Learning formats
Remote cohorts, private corporate sessions, practical workshops and executive briefings.



Course scope, language, materials and examination arrangements are confirmed in the proposal.

Training themes

Official programmes and tailored workshops, selected for your team’s needs.

Security management

ISO/IEC 27001, 27002 and cybersecurity leadership.

Risk & audit

ISO 27005, ISO 31000, audit techniques and control evidence.

Continuity & incidents

ISO 22301, incident management and crisis exercises.

Privacy & AI

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

Technical security

OT/ICS, cloud, application security and offensive/defensive practices.

Management & innovation

ISO/IEC 20000, ISO 21502 and ISO 56001.

Workshops, speaking & knowledge transfer

Sessions designed around the audience and a usable learning outcome.

Executive briefings

Cyber risk decisions, security accountability, AI use and resilience.

Practitioner workshops

Risk registers, audit evidence, incident playbooks and threat modelling.

Conferences & masterclasses

Cybersecurity careers, leadership, IT/OT security and operational lessons.

Mentoring & learning resources

Team coaching, tailored learning paths and original educational content.

Advisory for cybersecurity service providers

Support for partners building a practice, a service portfolio or a training offer.

Service design

Service catalogues, delivery methods, quality criteria and operational ownership.

Technical pre-sales

Discovery workshops, scope definition and technical proposals.

Practice development

Capability roadmaps, partnership discussions and subject-matter positioning.

Content & enablement

Webinars, technical presentations, learning content and team development.

Four ways to begin

Starting points that can stand alone or lead into a wider programme.

01 / Cyber diagnostic

A scoped maturity and control review. Receive a concise risk view and prioritised improvement roadmap.

02 / Audit readiness

An evidence and gap review for an agreed management system. Receive a corrective-action plan.

03 / vCISO support

Recurring senior advisory and programme oversight. Receive management reporting and decision support.

04 / Skills programme

A role-based training or workshop plan. Receive learning materials and an assessment approach.

A clear delivery approach

01	**Scope**	Business objectives, stakeholders, systems and boundaries.
02	**Assess**	Evidence collection, interviews and targeted analysis.
03	**Prioritise**	Risk-based findings and an agreed action sequence.
04	**Deliver**	Implementation support, documentation or training.
05	**Transfer**	Management readout, handover and agreed follow-up.

Deliverables your teams can use

Management	Executive summary, key risks and decisions requiring ownership.
Operational teams	Detailed findings, evidence and prioritised corrective actions.
Control owners	Responsibilities, target dates and acceptance or retest criteria.
Knowledge transfer	Working documents, workshops and handover sessions.

The statement of work defines each deliverable, its format, the review process and completion criteria.

Engagement & commercial arrangements

A written proposal tailored to scope, complexity, timing and budget.

Contracting identity

Taher Amine ELHOUARI, auto-entrepreneur in Algeria. Registered activity: Expert sécurité informatique.

Engagement models

Fixed-scope project, day-based advisory, recurring support or training cohort. Fees quoted after scope definition.

Delivery arrangements

Remote delivery as the default. On-site needs, travel arrangements and availability agreed separately. Language agreed per audience.

Commercial clarity

Scope, client inputs, milestones, payment schedule, confidentiality and deliverable acceptance defined before commencement.

Let’s define your next assignment

Share your priorities, scope and target timeline.
Receive a tailored technical and commercial proposal.

Taher Amine ELHOUARI

Independent advisor • Auditor • PECB GOLD Trainer

contact@taheramine.org

+213 7 81 04 04 82

www.taheramine.org

Auto-entrepreneur, Algeria • International engagements