TAHER AMINE ELHOUARI

Director, Cybersecurity Business Unit – EMEA | Senior Cybersecurity Expert & Advisor | vCISO | Certification Body–Approved Auditor | PECB GOLD Trainer

DBA, MBA, MSc, PMP, CISSP-SME, CCISO, SecurityX, CMSA, ISO MASTER-SLA-SLI-SM, TAISE, CCSK, eCPPT, eCTHP, OOSE

+213 7 81 04 04 82 | contact@taheramine.org | www.taheramine.org | linkedin.com/in/MrTaherAmine

EXECUTIVE PROFILE

Director of the Cybersecurity Business Unit – EMEA at Fortress Plus since October 2026, and Senior Cybersecurity Expert & Advisor at Near Trust, its Tunisian branch. Also active as an independent vCISO, certification body–approved management systems auditor and PECB Certified GOLD Trainer. Cybersecurity executive and independent senior adviser with over a decade of professional experience, spanning offensive security and cyber defense, information-security project management, regulated banking and critical sectors, security operations, CISO-level governance, risk, compliance, certification assurance and professional education. Bridges board-level risk decisions and operational control effectiveness; experienced in cross-sector advisory, risk & incident management, audit, resilience and the development of security operating models.

EXECUTIVE VALUE & CORE EXPERTISE

- **Strategy & governance:** Security strategy, accountability models, CISO charters, stakeholder reporting, multi-year transformation, risk acceptance and policy governance.
- **Risk, compliance & assurance:** ISMS, BCMS, NIST, ISA/IEC, CIS, DORA/NIS2, OWASP, CSA, privacy, risk registers, control libraries, third-party risk, audits, management-system conformity, certification readiness and regulatory mapping.
- **Cybersecurity operations:** SOC/CSIRT/CERT, DFIR, CTI, monitoring, threat hunting, detection quality, response playbooks and crisis coordination.
- **Hands-on technical depth:** VAPT, penetration testing, attack-path validation, cloud and OT/ICS assurance, architecture and vulnerability lifecycle.
- **Capability development:** Approved certification auditing, PECB GOLD professional training, coaching, program committees and open knowledge resources.

PROFESSIONAL EXPERIENCE

Director, Cybersecurity Business Unit – EMEA | Oct 2026 - Present

Fortress Plus · France / EMEA (Europe, Middle East & Africa) / Hybrid

- Lead the development and strategic direction of the cybersecurity business unit across EMEA, aligning service capabilities with client needs and organizational priorities.
- Guide the cybersecurity advisory portfolio spanning GRC, management-system assurance, IT/OT/ICS security, AI security, critical-infrastructure resilience and technical assessments.
- Coordinate the evolution of SOC/CSIRT, incident-response and managed-security offerings, working with technical specialists and company leadership.
- Contribute to cross-border business development, partner engagement, client proposals, professional events, training initiatives and delivery coordination.

Senior Cybersecurity Expert & Advisor (IT/OT, AI, GRC & SOC/CSIRT) | Oct 2026 - Present

Near Trust (Fortress Plus Tunisian branch) · Tunis, Tunisia / Hybrid

- Provide senior advisory input for cybersecurity consulting involving IT, OT/ICS and cyber-physical security in industrial and critical-infrastructure environments.
- Support security governance, risk assessment, ISO management-system advisory, regulatory alignment and cybersecurity assurance assignments.
- Contribute specialist perspectives to SOC/CSIRT maturity, incident response, threat management and cyber-resilience improvement.
- Collaborate with the Tunisian team on technical scoping, client workshops, assessments, professional recommendations and knowledge transfer.

Independent Cybersecurity, GRC, Audit & Training Consultant | Aug 2024 - Present

ANAE / Independent Practice · Algeria / International

- Provide independent strategic and technical cybersecurity consultancy to organizations across regulated, industrial, public-sector, financial, and technology environments, addressing governance, security operations, risk management, compliance, assurance, and organizational resilience.
- Advise executive management and security stakeholders on cybersecurity strategy, information-security governance, risk appetite, risk ownership, security investment priorities, accountability structures, and business-aligned transformation roadmaps.
- Support the establishment, implementation, evaluation, and continual improvement of Information Security Management Systems (ISMS), Business Continuity Management Systems (BCMS), privacy management practices, and related governance arrangements.
- Conduct cybersecurity maturity assessments, regulatory gap analyses, control-effectiveness reviews, information-security risk assessments, internal audits, supplier assessments, and certification-readiness evaluations.
- Perform authorized third-party management-system certification audits and assessments on behalf of certification bodies, applying applicable audit criteria, competence requirements, independence safeguards, and evidence-based conformity-assessment practices.
- Apply ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO 22301, ISO 31000, ISO 19011, ISO/IEC 17021-1, and relevant sector-specific requirements according to assignment scope and applicable editions.
- Develop and review cybersecurity policies, risk registers, Statements of Applicability, control matrices, audit programs, treatment plans, incident-management procedures, business-continuity documentation, and corrective-action tracking mechanisms.
- Perform or contribute to vulnerability assessments, penetration testing, digital forensics, incident investigation, threat hunting, security architecture reviews, and technical control validation within authorized engagement scopes.
- Evaluate SOC/CSIRT maturity and incident-response capabilities, including incident classification, detection and escalation processes, playbooks, evidence preservation, management reporting, service quality, and operational improvement.
- Assess security-governance considerations relating to cloud environments, third-party services, identity and access management, information classification, vulnerability management, and security monitoring.
- Support assessments concerning critical infrastructure and OT/ICS security, including security governance, segmentation concepts, industrial risk management, and ISA/IEC 62443 requirements where relevant to individual assignments.
- Analyze applicable Algerian cybersecurity and data-protection requirements, including RNSI 2020 and Law 18-07 as amended, and assess the relevance of international standards and foreign regulatory frameworks where required by client activities.
- Deliver documented advisory and assessment engagements, design and deliver authorized professional training, executive briefings, and practitioner workshops in cybersecurity governance, ISO management systems, risk management, security auditing, incident response, business continuity, and selected OT/ICS security disciplines.
- Translate technical vulnerabilities, audit findings, regulatory requirements, and operational weaknesses into risk-based recommendations, accountable remediation actions, executive reporting, and prioritized security-improvement roadmaps.

Chief Information Security Officer (CISO) & Head of Advisory and CSIRT

05 Jan 2025 - 04 Sep 2026

SARL EKSec · Algiers, Algeria

- Contributed to the definition and execution of cybersecurity priorities, aligning organizational security requirements with operational capabilities, client expectations, business risks, and management objectives.
- Developed and maintained information-security policies, security-management procedures, risk assessment methodologies, control requirements, remediation mechanisms, and executive reporting practices.
- Supported ISMS-aligned governance and continual-improvement activities, drawing on ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO 31000, and relevant industry security frameworks.
- Oversaw multidisciplinary advisory and assurance activities encompassing GRC, security assessments, technical testing, information-security management, operational resilience, and security improvement.
- Contributed to the development of CSIRT operating practices, including incident classification, escalation rules, response workflows, operational playbooks, evidence-handling expectations, and post-incident reviews.
- Strengthened coordination between SOC monitoring activities, incident-response stakeholders, security advisers, and management-level decision-makers.
- Supported the definition and review of cybersecurity service catalogues, operational procedures, delivery methodologies, quality criteria, SLAs, KPIs, and management-reporting requirements.
- Evaluated security-control design and implementation, emphasizing the relationship between documented governance requirements and observable operational security practices.

- Reviewed incident-management, vulnerability-management, threat-monitoring, and security-assessment findings to support remediation priorities and continuous operational improvement.
- Coordinated technical and governance stakeholders across client engagements, promoting consistent assessment methods, reporting standards, evidence traceability, and accountability for corrective actions.
- Contributed to cybersecurity maturity reviews and the development of practical improvement recommendations for organizations with different levels of security capability and regulatory exposure.
- Supported the integration of resilience and continuity considerations into cybersecurity governance, incident response, service planning, and management decisions.
- Advised stakeholders on the selection and adaptation of relevant references, including ISO/IEC 27001/27002, ISO/IEC 27035, NIST CSF, NIST incident-response guidance, CIS Controls, MITRE ATT&CK, OWASP methodologies, and FIRST/CSIRT good practices.
- Promoted professional development, knowledge sharing, technical collaboration, service quality, and structured communication between cybersecurity specialists and business stakeholders.

Head of Security, Risk & Compliance (CISO) | 14 Jul 2025 - 04 Dec 2025

GIE Monétique · Hydra, Algiers

- Led cybersecurity governance, information-security risk management, and compliance-related activities in the context of Algeria's electronic-payment ecosystem.
- Contributed to the development and improvement of sector-level cybersecurity governance requirements for financial institutions, electronic-payment stakeholders, and associated service providers.
- Redesigned and structured a sector security-control framework comprising approximately 374 controls, creating a more comprehensive basis for security assessment, compliance monitoring, and risk-based improvement.
- Mapped and harmonized security requirements from PCI DSS 4.0.1, SWIFT Customer Security Controls Framework, ISO/IEC 27001/27002, NIST guidance, CIS Controls, OWASP references, Cloud Security Alliance materials, and relevant national requirements.
- Organized overlapping control requirements into coherent security domains, reducing interpretation inconsistencies and facilitating the application of common assessment criteria.
- Developed structured control objectives, implementation expectations, assessment criteria, and evidence requirements to support consistent security-control evaluation.
- Strengthened the treatment of governance, asset inventories, access control, network security, system hardening, logging, monitoring, vulnerability management, incident response, and business continuity within the control framework.
- Supported the definition of control responsibilities, compliance indicators, documented exceptions, remediation priorities, and follow-up procedures across relevant security domains.
- Conducted or supported gap analyses and control reviews to identify security weaknesses, incomplete implementations, conflicting requirements, and opportunities for framework improvement.
- Incorporated risk-management and control-assurance principles into the sector framework, connecting security requirements with evidence, assessment outcomes, residual risk, and corrective actions.
- Facilitated coordination between cybersecurity, banking, technology, risk, compliance, and management stakeholders when reviewing security obligations and implementation priorities.
- Prepared analyses and recommendations to assist management in understanding compliance exposure, framework deficiencies, security-control priorities, and improvement requirements.
- Considered relevant Algerian information-security and data-protection obligations, including RNSI 2020 and Law 18-07 as amended by Law 25-11 of July 2025, according to their applicability.
- Supported a more consistent and auditable approach to information-security governance across the electronic-payment environment, linking regulatory expectations, recognized industry practices, and practical implementation.

Independent Cybersecurity, Information Security & GRC Consultant | Trainer & Advisor

01 Sep 2019 - 31 Aug 2024

Independent / Freelance Professional Activity · Algeria / Remote

- Delivered independent cybersecurity consultancy, technical security assessments, information-security advisory, professional training, and organizational security-improvement services.
- Supported organizations in identifying cybersecurity risks, assessing information-security controls, prioritizing vulnerabilities, and developing practical remediation recommendations.
- Conducted or contributed to authorized vulnerability assessments, penetration tests, security configuration reviews, technical investigations, and information-system security evaluations.
- Assisted clients in establishing or improving information-security policies, procedures, control documentation, risk-management processes, and organizational security practices.

- Supported ISMS implementation and audit-readiness activities based on ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, and related management-system requirements.
- Contributed to digital-forensic and incident-investigation activities, including technical analysis, evidence documentation, identification of security weaknesses, and incident-related recommendations.
- Participated in security-operations and incident-response improvement work, including monitoring concepts, vulnerability management, threat analysis, investigation procedures, and security reporting.
- Provided advice on infrastructure and network security, identity and access controls, application security, secure configuration, information protection, and technical remediation.
- Supported management-system assessment and business-continuity activities, including process reviews, continuity risk considerations, documentary evidence, and organizational preparedness.
- Applied recognized security-assessment methodologies and references appropriate to each engagement, including OWASP testing guidance, NIST guidance, CIS Controls, ISO/IEC 27001, and established penetration-testing practices.
- Developed tailored professional training materials, technical demonstrations, assessment exercises, practical workshops, and awareness sessions for different audiences.
- Delivered or supported cybersecurity and professional-development activities involving organizations and training partners such as SAIDAL, Inter Entreprises, CFN/Mobilis, SOFICLEF, the Ministry of National Defence, and Institut Supérieur de Management Tlemcen, within the documented scope of each collaboration.
- Coordinated client communications, engagement planning, technical findings, reporting, remediation recommendations, and knowledge-transfer activities.
- Participated in cybersecurity community initiatives, mentoring, conferences, technical workshops, and awareness activities aimed at strengthening professional cybersecurity capabilities.
- Progressively expanded the scope of independent engagements from hands-on technical assessments to governance, information-security management, risk assessment, audit preparation, and executive-oriented cybersecurity advisory.

Information Security Engineer | 18 Jul 2023 - 12 Nov 2023

Société Générale Algérie · Algeria

- Contributed to information-security governance, operational cybersecurity, control assurance, and information-system protection within a regulated banking environment.
- Supported Security Operations Center activities, including security-event monitoring, alert analysis, suspicious-activity investigation, and incident escalation.
- Worked with security-monitoring and endpoint-protection capabilities, including SIEM, EDR, and DLP technologies, within assigned operational responsibilities.
- Participated in incident-analysis and digital-forensic activities, supporting technical investigation, evidence documentation, event correlation, and identification of security issues.
- Contributed to cyber-threat intelligence and threat-hunting activities to identify suspicious behavior, emerging risks, indicators of compromise, and potential security weaknesses.
- Supported vulnerability-management activities, including assessment findings, vulnerability prioritization, remediation recommendations, and follow-up with relevant stakeholders.
- Assisted in information-security assessments and control reviews involving banking information systems, infrastructure, access controls, logging, and security configurations.
- Supported documentation of security incidents, technical findings, protective measures, corrective actions, and operational lessons learned.
- Collaborated with security, risk, compliance, and information-technology stakeholders on the evaluation and improvement of security controls.
- Applied banking security principles and relevant information-security practices, drawing on applicable internal policies and established references such as ISO/IEC 27001/27002, NIST guidance, and recognized industry control frameworks.
- Contributed to continuous improvement of incident-handling procedures, operational security monitoring, security reporting, and technical assurance.

Senior Cybersecurity Consultant | 08 Feb 2023 - 10 Jul 2023

Intelligent Network SPA (iNET) · Hydra, Algiers

- Delivered senior-level cybersecurity consulting and information-security advisory services for client organizations, supporting security assessments and improvement initiatives.
- Conducted or contributed to information-security reviews, vulnerability assessments, technical assurance activities, and the preparation of remediation recommendations.
- Supported the identification of organizational and technical security risks affecting information systems, infrastructure, applications, and business operations.

- Assisted in the development or review of information-security policies, control documentation, security requirements, and management-system improvement measures.
- Contributed to cybersecurity assessment and audit-preparation activities, including gap identification, evidence review, reporting, and recommendations for corrective actions.
- Supported projects requiring coordination between cybersecurity specialists, technical teams, management representatives, and external stakeholders.
- Advised on relevant security-control practices, including identity and access management, infrastructure security, vulnerability management, incident response, and secure configuration.
- Used appropriate assessment methodologies and international references, including ISO/IEC 27001/27002, NIST security guidance, CIS Controls, and OWASP methodologies where relevant to assignments.
- Prepared technical and management-oriented reports communicating vulnerabilities, risks, control weaknesses, and recommended security improvements.
- Contributed to professional cybersecurity training and knowledge-transfer initiatives through collaboration with technical teams and educational stakeholders.
- Supported the consistent delivery of consultancy assignments through defined scopes, reporting expectations, documentation, client communication, and follow-up activities.

Information Systems Security Project Manager | 14 Oct 2018 - 08 Aug 2019

S.P.A. Smart Link Holding (SLC / DIVONA) · Algiers, Algeria

- Coordinated information-systems security projects within a telecommunications and technology-services environment, supporting the protection of infrastructure, networks, and operational services.
- Assisted in project planning, scope definition, technical coordination, security requirements analysis, progress tracking, and stakeholder communication.
- Supported security activities relating to network infrastructure, data centers, NOC operations, server environments, and information-system architecture.
- Coordinated or contributed to security assessment and penetration-testing activities, helping translate technical findings into project-level improvement actions.
- Supported the identification and evaluation of infrastructure vulnerabilities, configuration weaknesses, operational security risks, and security-control gaps.
- Contributed to network-security and infrastructure-protection initiatives covering access restrictions, segmentation, secure configuration, monitoring, and technical security requirements.
- Assisted in incident-response and operational-resilience planning, including escalation requirements, service dependencies, restoration priorities, and coordination with technical teams.
- Worked with engineering, network operations, infrastructure, and project stakeholders to integrate information-security requirements into technical delivery activities.
- Contributed to the development and review of security procedures, technical documentation, reporting materials, and implementation recommendations.
- Applied relevant information-security and project-management principles, including established ISO/IEC 27001, NIST, and recognized infrastructure-security practices where appropriate.
- Supported the translation of organizational security needs into defined project deliverables, responsibilities, risk considerations, and implementation priorities.

Lead Penetration Tester | 07 Aug 2016 - 18 Sep 2018

Taghellist Technology · Algiers, Algeria

- Led authorized penetration-testing and technical security-assessment activities targeting applications, networks, systems, and supporting information infrastructure.
- Planned and executed security-testing assignments according to defined objectives, permitted scope, technical constraints, and assessment methodologies.
- Performed vulnerability discovery, security reconnaissance, configuration reviews, and validation of exploitable security weaknesses.
- Assessed application and network security controls to identify potential attack paths, weaknesses in access restrictions, insecure configurations, and opportunities for unauthorized access.
- Applied penetration-testing methodologies and industry guidance, including OWASP testing practices and recognized technical assessment approaches available during the engagement period.
- Investigated technical vulnerabilities and validated exploitation scenarios within authorized testing boundaries, documenting relevant observations and evidence.

- Evaluated the security implications of discovered weaknesses, considering confidentiality, integrity, availability, business exposure, and potential remediation complexity.
- Prepared penetration-testing reports describing assessment scope, testing methodology, technical findings, affected assets, risk severity, supporting evidence, and recommended corrections.
- Communicated findings to technical and organizational stakeholders, explaining attack scenarios and supporting remediation prioritization.
- Contributed to the verification of security-control effectiveness and the identification of opportunities for infrastructure and application-security improvement.
- Developed and applied hands-on expertise in security-testing workflows, vulnerability validation, technical analysis, attack-path assessment, and practical security assurance.

SELECTED PROJECTS & DELIVERABLES

- **Electronic payments / sector security governance:** Redesigned a payment-ecosystem security baseline containing approximately 374 controls, mapped to industry requirements and international frameworks; improved the structure for evidence, risk ownership, review and follow-up.
- **SOC, CSIRT and advisory-service operating models:** Work across incident classification, service definition, escalation, playbooks, managed SOC governance, control validation, KPIs, quality review and coordination between security operations and business leadership.
- **ISMS and business continuity:** ISO/IEC 27001 information-security management and ISO 22301 continuity-oriented assessment, governance and documentation activities.
- **Incident investigation and audit:** DFIR and IT / information-security audit assignment, with technical evidence and remediation-oriented findings.
- **Multi-client GRC, training and assurance:** Selected engagements or delivery relationships: CETIC, iNET Academy, SAIDAL, Inter Entreprises, CFN/Mobilis, Algerian Ministry of National Defense, ARAMCO, SOFICLEF; and many other clients and industries.
- **Training and certification-readiness activities:** Official PECB education and other professional training (ISC2, ISACA, TRECCERT, EC-Council, CSA, OffSec, GIAC..), on ISO management systems, cyber leadership, incident management, risk, auditing and selected OT/ICS security topics.

PROFESSIONAL APPOINTMENTS & COMMUNITY LEADERSHIP

- Founding President / Leader — OWASP Algiers (Open Worldwide Application Security Project).
- Founding President / Leader — CSA Algeria (Cloud Security Alliance).
- Founding Chairman & President — CAS Algeria (Conformity Assessment Society).
- Former Global Advisory Boards — EC-Council C|CISO and C|PENT.
- Professional Member & Cybersecurity SME — AfricaCERT (ongoing since March 2025).
- Former Cybersecurity SME and Exam Content/Items Creator – ISC2 (International Information System Security Certification Consortium).
- Founder / leader — DEF CON Group Algeria (DC11213) and Imperium international CTF team.
- Program lead — Cyber Master Series: practitioner field guides, certification study resources and free security tools.
- Creator and host — The InfoSec Control Room podcast; Cyber Master Series Briefing newsletter.

INTERNATIONAL ADVISORY BOARDS & SME / EXAM DEVELOPMENT

- EC-Council | former advisory-board appointments (2024–2026): C|PENT Global Advisory Board (listed publicly by EC-Council) and C|CISO International Advisory Board; contributed practitioner feedback on executive cybersecurity capabilities, curricula, assessments and advanced penetration-testing relevance.
- ISC2 | former Cybersecurity SME, Exam & Content Development (Mar 2024 – Sep 2026): practitioner review and expert workshops relating to Certified in Cybersecurity (CC), CISSP and broader Unified Body of Knowledge subjects; contribution to question / content relevance.
- Hack The Box | former Cybersecurity SME (May 2024 – Sep 2026): offensive-security and red-team practitioner commentary, professional editorial input and educational content review; distinguished from any permanent employment or certification endorsement.
- AfricaCERT | ongoing SME / professional contributor: cybersecurity control and maturity concepts, assessment and implementation perspectives, regional capacity building and links between assurance and incident-response practice.

INTERNATIONAL SPEAKING & PROFESSIONAL CONTRIBUTION

- 2026 — Enterprise Portuaire de Skikda: formally invited by the CEO & CiSO to intervene at the Information Security Day (15 Oct, Skikda).
- 2025 — FIRST & AfricaCERT Regional Symposium, Mauritius: program committee member and speaker, "Conformity Assessment Meets Cybersecurity: Building a Common Language Between Auditors and Analysts".
- 2025 — Ministry of National Defence / ASSI information-security officers' conference (20 May): named speaker on "SecOps and GRC Alignment: A Strategic Imperative for Modern CISOs".
- 2025 — CERIST Innovation Hub (30 Jun): formally recognized for contributing to the organization of the Cybersecurity Youth Challenge competition.
- 2023 — SECURA North Africa (19 Sep, Algiers): conference speaker, "CyberSecurity Evolution: Adapting Strategies to Shifting Threats".
- 2024 — Distinguished Speaker, International Workshop on Cyber Security and Forensics, Jaipur, India (12 Sep).
- 2024 — Galactic Local Judge, NASA International Space Apps Challenge (5–6 Oct).
- 2024 — Techverse Intelligence Day (20 Apr): recognized for professional guidance and content contribution to a student- and practitioner-facing technology event.
- 2021 — ITC Talks, Blida: speaker (25 May).
- 2025 — TechZone (31 Jul): delivered Cybersecurity Foundations education for the digital generation; certificate of appreciation.
- 2019 — HackQuake, Médéa: judge and coach (Aug).
- Earlier contribution — GDG DevFest Blida hackathon (2017 participant); HackQuake (2019 judge and coach).

NATIONAL TV, RADIO & INTERNATIONAL PRESS

- Algerian National Television (ENTV / public television): recurring expert appearances; recorded topics include cyber awareness (May 2023), the global CrowdStrike incident and technology dependency (Aug 2024), information manipulation (Mar 2025), and cyber extortion in Taqassi, season 5 (Nov 2025).
- National and regional broadcast media: Radio Algérienne / Chaîne 3 Médiatics (8 Aug 2024; official broadcaster listing), Radio Médéa / OWASP Algiers and TechVerse discussions (including 18 Apr 2024), and a published 17 Feb 2024 El Iktisadia El Oula TV segment on website cookies.
- Additional televised and broadcast commentary is listed in the professional media archive for Ennahar TV, ElChourouk TV and ExpressFM Tunisia.
- International media profile: featured in two USA News articles (11 & 23 Jan 2026) on cybersecurity leadership and governance-to-resilience practice; a separate Jan 2026 career announcement was syndicated as a press release.

AWARDS & RECOGNITION

- Global 30 Under 30 in Cybersecurity (2026) — Top Cyber News Magazine.
- Official nominee — Cybersecurity Leader of the Year, International Cybersecurity Conference Awards 2026 (NITDA letter, 14 Oct 2026).
- Best Cybersecurity Thought Leader — Governance, Risk & Resilience (UK, 2026) — Best of Best Review.
- First place, Catch the Flag Challenge — International Cybersecurity Seminar, Algerian Ministry of National Defence / National Gendarmerie (27–28 Mar 2018).
- TryHackMe GOD Rank / Top 0.1% (2024) and Top 10 HackTheBox in 2018/2019.
- International Capture The Flag competition participation and multiple Top 10 finishes (events and placement evidence available on request).

SELECTED CERTIFICATIONS & PROFESSIONAL STANDING

Executive and cyber leadership

- **PMP** – Project Management Professional (PMI), 2026–2029
- ISC2 Certified Information Systems Security Professional (**CISSP**)
- PECB & EC-Council Certified Chief Information Security Officer (**CCISO**)
- PECB **Certified Cybersecurity MASTER**
- PECB **Senior Lead Cybersecurity Manager** (ISO/IEC 27032)
- CompTIA **SecurityX**

Certification audit, GRC and risk

- PECB Certified IPC Management Systems Auditor (**CMSA**)
- **Certification body–approved Management Systems Lead Auditor** / Assessor – Accurate Global Inc.

- Previously appointed **MSECB auditor – ISO/IEC 27001, ISO 22301 and CSA STAR**
- PECB **ISO/IEC 27001 MASTER** (ISMS Senior Lead Implementer / Senior Lead Auditor)
- PECB **ISO 22301 MASTER** (BCMS Senior Lead Implementer / Senior Lead Auditor)
- PECB **ISO/IEC 27701 Senior Lead Auditor**; **ISO/IEC 42001** Lead Auditor + Lead Implementer
- PECB **ISO 31000 Senior Lead Risk Manager**; **ISO/IEC 27005 Senior Risk Manager**
- PECB **NIST Cybersecurity Consultant**; **Senior Lead SOC 2 Analyst**

Instruction and professional education

- **PECB Certified GOLD Trainer** – GT20395871
- **PECB Certified Trainer** – CT07549-06-2024
- **TRECCERT Certified Trainer**; Certified Cybersecurity Educator Professional (**CCEP**)

Cloud, operations and technical security

- CSA **CCSK** v4/v5; **CCZT**; **TAISE**
- **eCPPTv2**; **eCTHPv2**; PECB **Lead PenTest Professional**
- **ISA/IEC 62443 Senior Lead Implementer**
- OPSWAT OT Security Expert (**OOSE**) and offensive-security learning/certification portfolio; Nozomi NNCTSP
- EC-Council **CEH v12 / CPENT**
- **PECB Certified U.S. Data Privacy Officer — issued 04 November 2026**
- **PECB Certified ISO 56001 Lead Implementer — issued 04 November 2026**

EDUCATION

- Master of Science in Computer Science: Software Engineering (**MSc**) | Woolf (**Malta / EU**) | 2026
- Doctor of Business Administration (**DBA**) | Atlanta College of Liberal Arts and Sciences (**ACLAS / USA**) | 2026
- Master of Computer Science (**MCS**) | Atlanta College of Liberal Arts and Sciences (**ACLAS / USA**) | 2026
- Master of Business Administration (**MBA**) | Atlanta College of Liberal Arts and Sciences (**ACLAS / USA**) | 2026
- **Mini-MBA** – Business Management | International Business Management Institute (**IBMI / Germany**) | 2022
- Higher Technician Diploma (**BTS**) – Computer Science / Networks | Vocational Training Institution, **Algeria** | 2019–2022

STANDARDS, FRAMEWORKS & REGULATIONS

- **Information Security, GRC & Management Systems:** ISO/IEC 27001 • ISO/IEC 27002/3/4 • ISO/IEC 27005/6/7/8 • ISO/IEC 27017 • ISO/IEC 27018 • ISO/IEC 27031 • ISO/IEC 27032 • ISO/IEC 27034/33 • ISO/IEC 27035 • ISO/IEC 27036 • ISO/IEC 27100 • ISO/IEC 27102 • ISO/IEC 27210 • ISO/IEC 27400 • ISO/IEC 27701 • ISO/IEC 29100 • ISO 31000 • ISO/IEC 31010 • ISO/IEC 38500 • ISO 37301 • COBIT • FAIR • EBIOS Risk Manager.
- **Audit, Assurance, Compliance & Resilience:** ISO 19011 • ISO/IEC 17021-1 • ISO 22301 • ISO 22313 • ISO 22316 • ISO 22317 • ISO 22320 • ISO 22329 • ISO/IEC 20000-1 • SOC 2 Trust Services Criteria • SOC for Cybersecurity • HITRUST CSF • SOX ITGC.
- **NIST & US Cybersecurity References:** NIST CSF 2.0 • NIST RMF • NIST SP 800-53 • NIST SP 800-37 • NIST SP 800-30 • NIST SP 800-61 • NIST SP 800-82 • NIST SP 800-115 • NIST SP 800-171 • NIST SP 800-172 • NIST SP 800-207 • NIST SP 800-218 • NIST AI RMF • FISMA • FedRAMP • CMMC.
- **Technical Security, Threat & Detection:** CIS Controls • CIS Benchmarks • MITRE ATT&CK • MITRE D3FEND • MITRE ATT&CK for ICS • CVSS • CVE • CWE • CAPEC • YARA • Sigma • STIX • TAXII • Cyber Kill Chain • Diamond Model • STRIDE • DREAD.
- **Application Security, DevSecOps & Software Assurance:** OWASP Top 10 • OWASP ASVS • OWASP MASVS • OWASP WSTG • OWASP API Security Top 10 • OWASP SAMM • NIST SP 800-218 Secure Software Development Framework (SSDF).
- **Cloud Security:** CSA CCM • CSA CAIQ • CSA STAR • ISO/IEC 27017 • ISO/IEC 27018 • Zero Trust Architecture • NIST SP 800-207.
- **Payment, Banking & Financial Security:** PCI DSS • PCI Secure Software Standard • PCI Secure SLC • SWIFT CSCF • DORA • PSD2 • SAMA Cybersecurity Framework.
- **Incident Response, SOC, CSIRT & PSIRT:** FIRST CSIRT Services Framework • FIRST PSIRT Services Framework • SIM3 • ENISA CSIRT Maturity Framework • TF-CSIRT Trusted Introducer • NIST SP 800-61 • MITRE ATT&CK • Threat Intelligence Frameworks CTI-CMM.
- **OT / ICS / Critical Infrastructure:** ISA/IEC 62443 • IEC 61508 • IEC 61511 • NIST SP 800-82 • MITRE ATT&CK for ICS • NERC CIP • Saudi NCA OTCC.
- **Privacy, Data Protection & AI Governance:** ISO/IEC 27701 • ISO/IEC 29100 • HIPAA Security Rule • ISO/IEC 42001 • EU AI Act • NIST AI RMF.

- **EU Cyber & Digital Regulations:** NIS2 • DORA • Cyber Resilience Act • eIDAS • PSD2 • ENISA guidance and sectoral good practices.
- **Algeria, Middle East & Regional References:** Algerian RNSI 2020 • Algerian National Information Systems Security Strategy 2025–2029 • Saudi NCA ECC • Saudi NCA CCC • Saudi NCA OTCC • SAMA Cybersecurity Framework • UAE IA Regulation • Qatar NIAS • QCB Cybersecurity Framework.

PUBLICATIONS & ORIGINAL PROFESSIONAL RESOURCES

- **The InfoSec Control Room (2026):** creator and host of an editorial podcast focused on governance, controls, risk decisions, SOC/CSIRT, resilience and leadership accountability.
- **Cyber Master Series Briefing (2026):** original practitioner-oriented articles and newsletter editions on SOC effectiveness, security governance and emerging responsibilities for CISOs.
- **Cyber Master Series Field Guides and Certification Study Series (2026):** authored learning materials, downloadable references and interactive study editions, with public GitHub repositories.
- Professional talks, workshop materials and free cybersecurity capacity-building programs, including practitioner support and certification-study resources.

LANGUAGES & AVAILABILITY

- **Arabic**: Native | **English**: Fluent / bilingual | **French**: Intermediate.
- Available for senior permanent leadership opportunities and international relocation; also open to advisory, audit and training assignments.

Portfolio: www.taheramine.org | **GitHub**: github.com/MrTaherAmine | **LinkedIn**: linkedin.com/in/MrTaherAmine

Details and supporting evidence available on request.