TAHER AMINE ELHOUARI

Directeur, Business Unit Cybersécurité – EMEA | Expert senior et conseiller en cybersécurité | vCISO | Auditeur habilité par organisme certificateur | Formateur PECB GOLD

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

PROFIL EXÉCUTIF

Depuis octobre 2026, Directeur de la Business Unit Cybersécurité – EMEA chez Fortress Plus et Expert senior et conseiller en cybersécurité auprès de Near Trust, sa branche tunisienne. Exerce également en indépendant comme vCISO, auditeur de systèmes de management habilité par un organisme certificateur et formateur PECB Certified GOLD Trainer. Dirigeant en cybersécurité et conseiller senior indépendant, fort de plus de dix ans d'expérience professionnelle couvrant la sécurité offensive et la cyberdéfense, la gestion de projets de sécurité de l'information, les secteurs bancaires réglementés et critiques, les opérations de sécurité, la gouvernance au niveau RSSI/CISO, les risques, la conformité, l'assurance par certification et la formation professionnelle. Fait le lien entre les décisions relatives aux risques prises au niveau des organes de direction et l'efficacité opérationnelle des contrôles ; expérience en conseil multisectoriel, gestion des risques et des incidents, audit, résilience et développement de modèles opérationnels de sécurité.

VALEUR AJOUTÉE EXÉCUTIVE ET EXPERTISES CLÉS

- **Stratégie et gouvernance :** stratégie de sécurité, modèles de responsabilité, chartes RSSI/CISO, reporting aux parties prenantes, transformation pluriannuelle, acceptation des risques et gouvernance des politiques.
- **Risques, conformité et assurance :** SMSI, SMCA, NIST, ISA/IEC, CIS, DORA/NIS2, OWASP, CSA, protection des données, registres des risques, bibliothèques de contrôles, risques tiers, audits, conformité des systèmes de management, préparation à la certification et cartographie réglementaire.
- **Opérations de cybersécurité :** SOC/CSIRT/CERT, DFIR, renseignement sur les cybermenaces (CTI), supervision, recherche proactive de menaces, qualité de la détection, playbooks de réponse et coordination de crise.
- **Expertise technique opérationnelle :** VAPT, tests d'intrusion, validation des chemins d'attaque, assurance cloud et OT/ICS, architecture et cycle de vie des vulnérabilités.
- **Développement des capacités :** audits de certification habilités, formation professionnelle PECB GOLD, accompagnement, comités de programme et ressources de connaissance ouvertes.

EXPÉRIENCES PROFESSIONNELLES

Directeur, Business Unit Cybersécurité – EMEA | Oct. 2026 - Présent

Fortress Plus · EMEA (Europe, Moyen-Orient et Afrique) / Hybride

- Piloter le développement et les orientations stratégiques de la Business Unit Cybersécurité à l'échelle EMEA, en alignant les capacités de prestation sur les besoins clients et les priorités de l'entreprise.
- Orienter le portefeuille de conseil en cybersécurité : GRC, assurance et systèmes de management, sécurité IT/OT/ICS, sécurité de l'IA, résilience des infrastructures critiques et évaluations techniques.
- Coordonner l'évolution des offres SOC/CSIRT, de réponse aux incidents et de services de sécurité managés avec les experts et la direction.
- Contribuer au développement commercial international, aux partenariats, aux propositions clients, aux événements professionnels, à la formation et à la coordination des missions.

Expert senior et conseiller en cybersécurité (IT/OT, IA, GRC et SOC/CSIRT) | Oct. 2026 - Présent

Near Trust (branche tunisienne de Fortress Plus) · Tunis, Tunisie / Hybride

- Apporter une expertise senior dans les missions de conseil en cybersécurité IT, OT/ICS et cyber-physique, notamment pour les environnements industriels et les infrastructures critiques.
- Appuyer les travaux de gouvernance SSI, d'analyse des risques, de conseil en systèmes de management ISO, de conformité et d'assurance cybersécurité.
- Contribuer aux évaluations de maturité SOC/CSIRT, à la réponse aux incidents, à la gestion des menaces et à l'amélioration de la cyber-résilience.
- Collaborer avec les équipes tunisiennes sur le cadrage technique, les ateliers clients, les évaluations, les recommandations et le transfert de compétences.

Consultant indépendant en cybersécurité, GRC, audit et formation | Août 2024 - Présent

ANAE / Activité indépendante · Algérie / International

- Fournir des prestations indépendantes de conseil stratégique et technique en cybersécurité à des organisations des secteurs réglementés, industriels, publics, financiers et technologiques, en matière de gouvernance, d'opérations de sécurité, de gestion des risques, de conformité, d'assurance et de résilience organisationnelle.
- Conseiller les directions générales et les parties prenantes en sécurité sur la stratégie de cybersécurité, la gouvernance SSI, l'appétence et la propriété des risques, les priorités d'investissement en sécurité, les structures de responsabilité et les feuilles de route de transformation alignées sur les besoins métiers.
- Accompagner la mise en place, le déploiement, l'évaluation et l'amélioration continue des systèmes de management de la sécurité de l'information (SMSI), des systèmes de management de la continuité d'activité (SMCA), des pratiques de protection des données et de leurs dispositifs de gouvernance.
- Réaliser des évaluations de maturité cyber, des analyses d'écarts réglementaires, des revues de l'efficacité des contrôles, des analyses de risques SSI, des audits internes, des évaluations de fournisseurs et des diagnostics de préparation à la certification.
- Réaliser des audits et évaluations de certification tierce partie de systèmes de management, dûment autorisés, pour le compte d'organismes certificateurs, en appliquant les critères d'audit, exigences de compétence, garanties d'indépendance et pratiques d'évaluation de la conformité fondées sur les preuves.
- Appliquer ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO 22301, ISO 31000, ISO 19011, ISO/IEC 17021-1 et les exigences sectorielles pertinentes selon le périmètre de chaque mission et les éditions applicables.
- Élaborer et revoir des politiques de cybersécurité, registres des risques, déclarations d'applicabilité, matrices de contrôles, programmes d'audit, plans de traitement, procédures de gestion des incidents, documents de continuité d'activité et mécanismes de suivi des actions correctives.
- Réaliser des évaluations de vulnérabilités, des tests d'intrusion, des investigations numériques, des enquêtes sur incidents, de la chasse aux menaces, des revues d'architecture de sécurité et des validations techniques de contrôles, ou y contribuer, dans les périmètres de mission autorisés.
- Évaluer la maturité des SOC/CSIRT et les capacités de réponse aux incidents, notamment la classification des incidents, les processus de détection et d'escalade, les playbooks, la conservation des preuves, le reporting de gestion, la qualité de service et l'amélioration opérationnelle.
- Évaluer les aspects de gouvernance de sécurité liés aux environnements cloud, aux services tiers, à la gestion des identités et des accès, à la classification des informations, à la gestion des vulnérabilités et à la supervision de sécurité.
- Contribuer aux évaluations de la sécurité des infrastructures critiques et des environnements OT/ICS, notamment la gouvernance de sécurité, les concepts de segmentation, la gestion des risques industriels et les exigences ISA/IEC 62443 lorsqu'elles sont pertinentes pour les missions concernées.
- Analyser les exigences algériennes applicables en cybersécurité et en protection des données, notamment le RNSI 2020 et la loi 18-07 telle que modifiée, et examiner la pertinence des normes internationales et des cadres réglementaires étrangers selon les activités des clients.
- Réaliser des missions documentées de conseil et d'évaluation ; concevoir et animer des formations professionnelles autorisées, des briefings exécutifs et des ateliers de praticiens sur la gouvernance cyber, les systèmes de management ISO, les risques, l'audit de sécurité, la réponse aux incidents, la continuité d'activité et certains domaines de sécurité OT/ICS.
- Traduire les vulnérabilités techniques, constats d'audit, exigences réglementaires et faiblesses opérationnelles en recommandations fondées sur les risques, actions correctives assorties de responsabilités, reportings exécutifs et feuilles de route d'amélioration priorisées.

Responsable de la sécurité des systèmes d'information (CISO) et Directeur du conseil et du CSIRT

05 janv. 2025 - 04 sept. 2026

SARL EKSec · Alger, Algérie

- Contribuer à la définition et à la mise en œuvre des priorités de cybersécurité, en alignant les exigences de sécurité de l'organisation sur les capacités opérationnelles, les attentes des clients, les risques métiers et les objectifs de la direction.
- Élaborer et maintenir les politiques de sécurité de l'information, procédures de management de la sécurité, méthodologies d'analyse des risques, exigences de contrôle, mécanismes de remédiation et pratiques de reporting exécutif.
- Soutenir la gouvernance alignée sur les SMSI et l'amélioration continue, sur la base d'ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO 31000 et des référentiels sectoriels pertinents.
- Superviser des activités pluridisciplinaires de conseil et d'assurance couvrant la GRC, les évaluations de sécurité, les tests techniques, le management de la sécurité de l'information, la résilience opérationnelle et l'amélioration de la sécurité.
- Contribuer au développement des pratiques opérationnelles du CSIRT, notamment la classification des incidents, les règles d'escalade, les processus de réponse, les playbooks opérationnels, les exigences de traitement des preuves et les retours d'expérience post-incident.
- Renforcer la coordination entre les activités de supervision du SOC, les intervenants en réponse aux incidents, les conseillers en sécurité et les décideurs de direction.
- Appuyer la définition et la revue des catalogues de services de cybersécurité, procédures opérationnelles, méthodologies de prestation, critères de qualité, SLA, KPI et exigences de reporting.
- Évaluer la conception et la mise en œuvre des contrôles de sécurité, en mettant l'accent sur la relation entre les exigences de gouvernance documentées et les pratiques opérationnelles observables.

- Examiner les constats issus de la gestion des incidents, des vulnérabilités, de la surveillance des menaces et des évaluations de sécurité afin d'orienter les priorités de remédiation et l'amélioration opérationnelle continue.
- Coordonner les parties prenantes techniques et de gouvernance dans les missions clients, en favorisant des méthodes d'évaluation, normes de reporting, preuves traçables et responsabilités de correction cohérentes.
- Contribuer aux revues de maturité cyber et à l'élaboration de recommandations d'amélioration concrètes pour des organisations présentant différents niveaux de capacités de sécurité et d'exposition réglementaire.
- Appuyer l'intégration des considérations de résilience et de continuité dans la gouvernance cyber, la réponse aux incidents, la planification des services et les décisions de management.
- Conseiller les parties prenantes sur le choix et l'adaptation des référentiels pertinents, notamment ISO/IEC 27001/27002, ISO/IEC 27035, NIST CSF, les guides NIST de réponse aux incidents, CIS Controls, MITRE ATT&CK, les méthodologies OWASP et les bonnes pratiques FIRST/CSIRT.
- Promouvoir le développement professionnel, le partage de connaissances, la collaboration technique, la qualité de service et une communication structurée entre spécialistes de cybersécurité et parties prenantes métiers.

Responsable Sécurité, Risques et Conformité (CISO) | 14 juil. 2025 - 04 déc. 2025

GIE Monétique · Hydra, Alger

- Piloter la gouvernance de cybersécurité, la gestion des risques SSI et les activités de conformité dans le contexte de l'écosystème algérien des paiements électroniques.
- Contribuer au développement et à l'amélioration des exigences sectorielles de gouvernance cyber pour les institutions financières, acteurs des paiements électroniques et prestataires associés.
- Refondre et structurer un référentiel sectoriel de contrôles de sécurité comprenant environ 374 contrôles, afin de disposer d'une base plus complète pour l'évaluation de la sécurité, le suivi de conformité et l'amélioration fondée sur les risques.
- Cartographier et harmoniser les exigences de sécurité issues de PCI DSS 4.0.1, du SWIFT Customer Security Controls Framework, d'ISO/IEC 27001/27002, des guides NIST, des CIS Controls, des références OWASP, des documents de la Cloud Security Alliance et des exigences nationales pertinentes.
- Organiser les exigences de contrôle qui se recoupent en domaines de sécurité cohérents, réduisant les divergences d'interprétation et facilitant l'application de critères d'évaluation communs.
- Définir des objectifs de contrôle structurés, attentes de mise en œuvre, critères d'évaluation et exigences de preuves pour permettre une évaluation cohérente des contrôles de sécurité.
- Renforcer la prise en compte de la gouvernance, des inventaires d'actifs, du contrôle des accès, de la sécurité réseau, du durcissement des systèmes, de la journalisation, de la surveillance, de la gestion des vulnérabilités, de la réponse aux incidents et de la continuité d'activité dans le référentiel.
- Appuyer la définition des responsabilités de contrôle, indicateurs de conformité, dérogations documentées, priorités de remédiation et procédures de suivi pour les domaines de sécurité concernés.
- Réaliser ou soutenir des analyses d'écarts et des revues de contrôles pour identifier les faiblesses de sécurité, mises en œuvre incomplètes, exigences contradictoires et opportunités d'amélioration du référentiel.
- Intégrer les principes de gestion des risques et d'assurance des contrôles au référentiel sectoriel, reliant les exigences de sécurité aux preuves, résultats d'évaluation, risques résiduels et actions correctives.
- Faciliter la coordination entre les parties prenantes de cybersécurité, de banque, de technologie, de risques, de conformité et de direction lors de l'examen des obligations de sécurité et des priorités de mise en œuvre.
- Préparer des analyses et recommandations pour aider la direction à comprendre l'exposition aux exigences de conformité, les insuffisances du référentiel, les priorités de contrôle et les besoins d'amélioration.
- Prendre en compte les obligations algériennes applicables en sécurité de l'information et protection des données, notamment le RNSI 2020 et la loi 18-07 modifiée par la loi 25-11 de juillet 2025, selon leur champ d'application.
- Favoriser une approche de gouvernance SSI plus cohérente et auditable dans l'environnement des paiements électroniques, reliant attentes réglementaires, pratiques sectorielles reconnues et mise en œuvre opérationnelle.

Consultant indépendant en cybersécurité, sécurité de l'information et GRC | Formateur et conseiller

01 sept. 2019 - 31 août 2024

Activité professionnelle indépendante / Freelance · Algérie / À distance

- Fournir des prestations indépendantes de conseil en cybersécurité, d'évaluations techniques de sécurité, de conseil en sécurité de l'information, de formation professionnelle et d'amélioration de la sécurité des organisations.
- Accompagner les organisations dans l'identification des risques cyber, l'évaluation des contrôles SSI, la hiérarchisation des vulnérabilités et l'élaboration de recommandations de remédiation concrètes.
- Réaliser des évaluations de vulnérabilités, tests d'intrusion autorisés, revues de configurations de sécurité, investigations techniques et évaluations de sécurité des systèmes d'information, ou y contribuer.
- Aider les clients à élaborer ou améliorer les politiques SSI, procédures, documents de contrôle, processus de gestion des risques et pratiques organisationnelles de sécurité.
- Soutenir la mise en œuvre des SMSI et la préparation aux audits sur la base d'ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 et des exigences connexes des systèmes de management.
- Contribuer aux activités d'investigation numérique et d'analyse d'incidents, notamment l'analyse technique, la documentation des preuves, l'identification des faiblesses de sécurité et les recommandations liées aux incidents.

- Participer à l'amélioration des opérations de sécurité et de la réponse aux incidents, couvrant les concepts de surveillance, la gestion des vulnérabilités, l'analyse des menaces, les procédures d'investigation et le reporting de sécurité.
- Conseiller sur la sécurité des infrastructures et réseaux, les identités et accès, la sécurité applicative, les configurations sécurisées, la protection de l'information et la remédiation technique.
- Contribuer à l'évaluation des systèmes de management et aux activités de continuité d'activité, notamment les revues de processus, l'analyse des risques de continuité, les preuves documentaires et la préparation organisationnelle.
- Appliquer les méthodologies et références reconnues adaptées à chaque mission, notamment les guides OWASP de tests de sécurité, les guides NIST, les CIS Controls, ISO/IEC 27001 et les pratiques établies de tests d'intrusion.
- Développer des supports de formation professionnelle adaptés, démonstrations techniques, exercices d'évaluation, ateliers pratiques et séances de sensibilisation pour différents publics.
- Réaliser ou soutenir des activités de cybersécurité et de développement professionnel impliquant des organisations et partenaires de formation tels que SAIDAL, Inter Entreprises, CFN/Mobilis, SOFICLEF, le ministère de la Défense nationale et l'Institut Supérieur de Management Tlemcen, dans les limites du périmètre documenté de chaque collaboration.
- Coordonner les échanges avec les clients, la planification des missions, les constats techniques, les rapports, les recommandations de remédiation et les activités de transfert de compétences.
- Participer à des initiatives communautaires en cybersécurité, du mentorat, des conférences, des ateliers techniques et des actions de sensibilisation visant à renforcer les compétences professionnelles en cybersécurité.
- Élargir progressivement les missions indépendantes, depuis les évaluations techniques pratiques jusqu'à la gouvernance, au management SSI, à l'analyse des risques, à la préparation des audits et au conseil stratégique destiné aux directions.

Ingénieur en sécurité de l'information | 18 juil. 2023 - 12 nov. 2023

Société Générale Algérie · Algérie

- Contribuer à la gouvernance SSI, à la cybersécurité opérationnelle, à l'assurance des contrôles et à la protection des systèmes d'information dans un environnement bancaire réglementé.
- Soutenir les activités du Security Operations Center, notamment la surveillance des événements de sécurité, l'analyse des alertes, les investigations sur les activités suspectes et l'escalade des incidents.
- Travailler avec des moyens de surveillance de sécurité et de protection des terminaux, notamment les technologies SIEM, EDR et DLP, dans les limites des responsabilités opérationnelles confiées.
- Participer à l'analyse des incidents et aux investigations numériques, en appuyant les enquêtes techniques, la documentation des preuves, la corrélation des événements et l'identification des problèmes de sécurité.
- Contribuer au renseignement sur les cybermenaces et au threat hunting pour identifier les comportements suspects, risques émergents, indicateurs de compromission et faiblesses potentielles.
- Soutenir les activités de gestion des vulnérabilités, notamment l'analyse des constats, la priorisation des vulnérabilités, les recommandations de remédiation et leur suivi auprès des parties prenantes concernées.
- Participer aux évaluations SSI et aux revues de contrôles portant sur les systèmes bancaires, les infrastructures, les contrôles d'accès, la journalisation et les configurations de sécurité.
- Contribuer à la documentation des incidents de sécurité, des constats techniques, des mesures de protection, des actions correctives et des enseignements opérationnels.
- Collaborer avec les équipes sécurité, risques, conformité et IT pour évaluer et améliorer les contrôles de sécurité.
- Appliquer les principes de sécurité bancaire et les pratiques SSI pertinentes, selon les politiques internes applicables et des références établies telles qu'ISO/IEC 27001/27002, les guides NIST et les cadres de contrôle sectoriels reconnus.
- Contribuer à l'amélioration continue des procédures de gestion des incidents, de la surveillance opérationnelle, du reporting de sécurité et de l'assurance technique.

Consultant senior en cybersécurité | 08 févr. 2023 - 10 juil. 2023

Intelligent Network SPA (iNET) · Hydra, Alger

- Fournir des prestations de conseil senior en cybersécurité et en sécurité de l'information aux organisations clientes, au soutien des évaluations de sécurité et initiatives d'amélioration.
- Réaliser ou contribuer à des revues SSI, évaluations de vulnérabilités, activités d'assurance technique et recommandations de remédiation.
- Aider à identifier les risques de sécurité organisationnels et techniques affectant les systèmes d'information, infrastructures, applications et opérations métiers.
- Contribuer à l'élaboration ou à la revue de politiques SSI, documents de contrôle, exigences de sécurité et mesures d'amélioration des systèmes de management.
- Participer aux évaluations de cybersécurité et à la préparation des audits, notamment identification des écarts, revue des preuves, reporting et recommandations d'actions correctives.
- Soutenir les projets nécessitant la coordination entre spécialistes de cybersécurité, équipes techniques, représentants de direction et parties prenantes externes.
- Conseiller sur les pratiques pertinentes de contrôle de sécurité, notamment la gestion des identités et des accès, la sécurité des infrastructures, la gestion des vulnérabilités, la réponse aux incidents et les configurations sécurisées.
- Utiliser les méthodologies d'évaluation et références internationales appropriées, notamment ISO/IEC 27001/27002, les guides de sécurité NIST, les CIS Controls et les méthodologies OWASP lorsque pertinentes pour les missions.

- Préparer des rapports techniques et destinés à la direction exposant les vulnérabilités, risques, faiblesses de contrôle et améliorations recommandées.
- Contribuer aux initiatives de formation professionnelle et de transfert des connaissances en cybersécurité, en collaboration avec les équipes techniques et les acteurs pédagogiques.
- Soutenir la réalisation cohérente des missions de conseil grâce à des périmètres définis, des attentes de reporting, de la documentation, la communication client et le suivi.

Chef de projet en sécurité des systèmes d'information | 14 oct. 2018 - 08 août 2019

S.P.A. Smart Link Holding (SLC / DIVONA) · Alger, Algérie

- Coordonner des projets de sécurité des systèmes d'information dans un environnement de télécommunications et de services technologiques, afin de protéger les infrastructures, réseaux et services opérationnels.
- Contribuer à la planification des projets, au cadrage, à la coordination technique, à l'analyse des exigences de sécurité, au suivi de l'avancement et à la communication avec les parties prenantes.
- Soutenir les activités de sécurité relatives aux infrastructures réseau, centres de données, opérations NOC, environnements serveurs et architectures de systèmes d'information.
- Coordonner ou contribuer aux évaluations de sécurité et aux tests d'intrusion, afin de traduire les constats techniques en actions d'amélioration au niveau des projets.
- Participer à l'identification et à l'évaluation des vulnérabilités d'infrastructure, faiblesses de configuration, risques opérationnels de sécurité et écarts de contrôle.
- Contribuer aux initiatives de sécurité réseau et de protection des infrastructures couvrant les restrictions d'accès, la segmentation, les configurations sécurisées, la supervision et les exigences techniques de sécurité.
- Participer à la planification de la réponse aux incidents et de la résilience opérationnelle, notamment les exigences d'escalade, dépendances de services, priorités de restauration et la coordination avec les équipes techniques.
- Collaborer avec les équipes d'ingénierie, d'exploitation réseau, d'infrastructure et de gestion de projet pour intégrer les exigences SSI aux activités de réalisation technique.
- Participer à l'élaboration et à la revue de procédures de sécurité, documents techniques, supports de reporting et recommandations de mise en œuvre.
- Appliquer les principes pertinents de sécurité de l'information et de gestion de projet, notamment ISO/IEC 27001, NIST et les pratiques reconnues de sécurité des infrastructures selon les besoins.
- Contribuer à traduire les besoins organisationnels de sécurité en livrables de projet, responsabilités définies, considérations de risque et priorités de mise en œuvre.

Responsable des tests d'intrusion (Lead Penetration Tester) | 07 août 2016 - 18 sept. 2018

Taghellist Technology · Alger, Algérie

- Diriger des missions autorisées de tests d'intrusion et d'évaluations techniques de sécurité ciblant les applications, réseaux, systèmes et infrastructures informatiques associées.
- Planifier et exécuter des missions de tests de sécurité selon les objectifs définis, périmètres autorisés, contraintes techniques et méthodologies d'évaluation.
- Réaliser la découverte de vulnérabilités, la reconnaissance de sécurité, les revues de configuration et la validation des faiblesses exploitables.
- Évaluer les contrôles de sécurité applicatifs et réseau afin d'identifier les chemins d'attaque possibles, les faiblesses des restrictions d'accès, les configurations non sécurisées et les possibilités d'accès non autorisé.
- Appliquer les méthodologies de tests d'intrusion et guides sectoriels, notamment les pratiques OWASP et les approches reconnues d'évaluation technique disponibles au cours de cette période.
- Analyser les vulnérabilités techniques et valider les scénarios d'exploitation dans les limites des périmètres autorisés, en documentant les observations et preuves pertinentes.
- Évaluer les conséquences des faiblesses identifiées sur la confidentialité, l'intégrité, la disponibilité, l'exposition métier et la complexité potentielle des remédiations.
- Rédiger des rapports de tests d'intrusion précisant le périmètre, la méthodologie, les constats techniques, les actifs concernés, la sévérité des risques, les preuves et les corrections recommandées.
- Présenter les constats aux parties prenantes techniques et organisationnelles, expliquer les scénarios d'attaque et soutenir la priorisation des remédiations.
- Contribuer à la vérification de l'efficacité des contrôles de sécurité et à l'identification des opportunités d'amélioration de la sécurité des infrastructures et applications.
- Développer et mobiliser une expertise technique pratique en tests de sécurité, validation des vulnérabilités, analyse technique, évaluation des chemins d'attaque et assurance de sécurité.

PROJETS ET LIVRABLES SÉLECTIONNÉS

- **Paiements électroniques / gouvernance sectorielle de la sécurité :** refonte d'un référentiel de sécurité de l'écosystème des paiements comprenant environ 374 contrôles, mis en correspondance avec des exigences sectorielles et des référentiels internationaux ; amélioration de la structure de gestion des preuves, des responsabilités liées aux risques, des revues et du suivi.

- **Modèles opérationnels SOC, CSIRT et de services de conseil :** travaux sur la classification des incidents, la définition des services, l'escalade, les playbooks, la gouvernance SOC managé, la validation des contrôles, les KPI, les revues qualité et la coordination entre opérations de sécurité et direction métier.
- **SMSI et continuité d'activité :** activités d'évaluation, de gouvernance et de documentation liées au management SSI selon ISO/IEC 27001 et à la continuité d'activité selon ISO 22301.
- **Investigation sur incidents et audit :** mission d'investigation numérique (DFIR) et d'audit IT / SSI, avec preuves techniques et constats orientés vers la remédiation.
- **GRC, formation et assurance auprès de plusieurs clients :** exemples de missions ou de collaborations de prestation : CETIC, iNET Academy, SAIDAL, Inter Entreprises, CFN/Mobilis, ministère algérien de la Défense nationale, ARAMCO, SOFICLEF ; ainsi que de nombreux autres clients et secteurs.
- **Formation et préparation à la certification :** formations officielles PECB et autres formations professionnelles (ISC2, ISACA, TRECCERT, EC-Council, CSA, OffSec, GIAC..) sur les systèmes de management ISO, le leadership cyber, la gestion des incidents, les risques, l'audit et certains sujets de sécurité OT/ICS.

NOMINATIONS PROFESSIONNELLES ET RESPONSABILITÉS COMMUNAUTAIRES

- Président fondateur / Responsable — OWASP Algiers (Open Worldwide Application Security Project).
- Président fondateur / Responsable — CSA Algeria (Cloud Security Alliance).
- Président fondateur et président du chapitre — CAS Algeria (Conformity Assessment Society).
- Anciens comités consultatifs mondiaux — EC-Council C|CISO et C|PENT.
- Membre professionnel et expert métier (SME) en cybersécurité — AfricaCERT (depuis mars 2025).
- Ancien expert métier (SME) en cybersécurité et créateur de contenus / questions d'examen — ISC2 (International Information System Security Certification Consortium).
- Fondateur / Responsable — DEF CON Group Algeria (DC11213) et équipe internationale de CTF Imperium.
- Responsable du programme — Cyber Master Series : guides pratiques destinés aux professionnels, ressources de préparation aux certifications et outils de sécurité gratuits.
- Créateur et animateur — podcast The InfoSec Control Room ; newsletter Cyber Master Series Briefing.

COMITÉS CONSULTATIFS INTERNATIONAUX ET EXPERTISE MÉTIER / CONCEPTION D'EXAMENS

- EC-Council | anciennes nominations à des comités consultatifs (2024–2026) : C|PENT Global Advisory Board (inscription publique par EC-Council) et C|CISO International Advisory Board ; contribution par des retours de terrain sur les compétences des dirigeants cyber, les programmes de formation, les évaluations et la pertinence des tests d'intrusion avancés.
- ISC2 | ancien expert métier en cybersécurité, développement des examens et des contenus (mars 2024 – sept. 2026) : revues par les professionnels et ateliers d'experts relatifs aux certifications Certified in Cybersecurity (CC), CISSP et aux thématiques plus larges du Unified Body of Knowledge ; contribution à la pertinence des questions et contenus.
- Hack The Box | ancien expert métier en cybersécurité (mai 2024 – sept. 2026) : avis professionnels sur la sécurité offensive et les pratiques red team, contributions éditoriales et revue de contenus pédagogiques ; rôle distinct de tout emploi permanent ou soutien officiel à une certification.
- AfricaCERT | expert métier / contributeur professionnel toujours actif : concepts de contrôles et de maturité cyber, perspectives d'évaluation et de mise en œuvre, renforcement des capacités régionales et rapprochement entre assurance et pratiques de réponse aux incidents.

CONFÉRENCES INTERNATIONALES ET CONTRIBUTIONS PROFESSIONNELLES

- 2026 — Entreprise Portuaire de Skikda : invitation officielle du PDG et du RSSI pour intervenir à la Journée de la sécurité de l'information (15 oct., Skikda).
- 2025 — FIRST & AfricaCERT Regional Symposium, Maurice : membre du comité de programme et intervenant, « Évaluation de la conformité et cybersécurité : construire un langage commun entre auditeurs et analystes ».
- 2025 — Conférence des officiers de sécurité de l'information du ministère de la Défense nationale / ASSI (20 mai) : intervenant désigné sur « Alignement SecOps et GRC : un impératif stratégique pour les RSSI modernes ».
- 2025 — CERIST Innovation Hub (30 juin) : reconnaissance officielle pour la contribution à l'organisation du concours Cybersecurity Youth Challenge.
- 2023 — SECURA North Africa (19 sept., Alger) : conférencier, « Évolution de la cybersécurité : adapter les stratégies face à l'évolution des menaces ».
- 2024 — Conférencier distingué, International Workshop on Cyber Security and Forensics, Jaipur, Inde (12 sept.).
- 2024 — Membre du jury local « Galactic », NASA International Space Apps Challenge (5–6 oct.).
- 2024 — Techverse Intelligence Day (20 avril) : reconnaissance pour les conseils professionnels et la contribution aux contenus d'un événement destiné aux étudiants et praticiens des technologies.
- 2021 — ITC Talks, Blida : intervenant (25 mai).
- 2025 — TechZone (31 juillet) : animation d'une formation aux fondamentaux de la cybersécurité pour la génération numérique ; certificat de reconnaissance.
- 2019 — HackQuake, Médéa : membre du jury et coach (août).
- Contribution antérieure — hackathon GDG DevFest Blida (participant en 2017) ; HackQuake (membre du jury et coach en 2019).

TÉLÉVISION NATIONALE, RADIO ET PRESSE INTERNATIONALE

- Télévision nationale algérienne (ENTV / télévision publique) : interventions récurrentes en qualité d'expert ; sujets enregistrés : sensibilisation cyber (mai 2023), incident mondial CrowdStrike et dépendance technologique (août 2024), manipulation de l'information (mars 2025) et cyberextorsion dans Taqassi, saison 5 (nov. 2025).
- Médias audiovisuels nationaux et régionaux : Radio Algérienne / Chaîne 3 Médiatics (8 août 2024 ; mention officielle du diffuseur), Radio Médéa / discussions OWASP Algiers et TechVerse (dont le 18 avril 2024), et séquence TV publiée le 17 févr. 2024 sur El Iktisadia El Oula concernant les cookies des sites web.
- D'autres interventions télévisées et radiophoniques figurent dans les archives médiatiques professionnelles pour Ennahar TV, ElChourouk TV et ExpressFM Tunisie.
- Couverture médiatique internationale : présentation dans deux articles d'USA News (11 et 23 janv. 2026) sur le leadership cyber et les pratiques reliant gouvernance et résilience ; une annonce professionnelle distincte datant de janv. 2026 a été reprise sous forme de communiqué de presse.

PRIX ET RECONNAISSANCES

- Global 30 Under 30 in Cybersecurity (2026) — Top Cyber News Magazine.
- Nommé officiellement — Cybersecurity Leader of the Year, International Cybersecurity Conference Awards 2026 (courrier NITDA du 14 oct. 2026).
- Best Cybersecurity Thought Leader — Governance, Risk & Resilience (Royaume-Uni, 2026) — Best of Best Review.
- Première place, Catch the Flag Challenge — Séminaire international de cybersécurité, ministère algérien de la Défense nationale / Gendarmerie nationale (27–28 mars 2018).
- Rang GOD sur TryHackMe / Top 0,1 % (2024) et Top 10 sur HackTheBox en 2018/2019.
- Participation à des compétitions internationales Capture The Flag et plusieurs classements dans le Top 10 (preuves des événements et des classements disponibles sur demande).

CERTIFICATIONS SÉLECTIONNÉES ET STATUT PROFESSIONNEL

Direction et leadership cyber

- 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

Audit de certification, GRC et risques

- PECB Certified IPC Management Systems Auditor (CMSA)
- Auditeur principal / évaluateur de systèmes de management habilité par un organisme certificateur – Accurate Global Inc.
- Ancien auditeur désigné par MSECB – ISO/IEC 27001, ISO 22301 et CSA STAR
- PECB ISO/IEC 27001 MASTER (SMSI Senior Lead Implementer / Senior Lead Auditor)
- PECB ISO 22301 MASTER (SMCA 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

Formation et enseignement professionnels

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

Cloud, opérations et sécurité technique

- CSA CCSK v4/v5 ; CCZT ; TAISE
- eCPPTv2 ; eCTHPv2 ; PECB Lead PenTest Professional
- ISA/IEC 62443 Senior Lead Implementer
- OPSWAT OT Security Expert (OOSE) et portefeuille de formations/certifications en sécurité offensive ; Nozomi NNCTSP
- EC-Council CEH v12 / CPENT
- **PECB Certified U.S. Data Privacy Officer — délivré le 4 novembre 2026**
- **PECB Certified ISO 56001 Lead Implementer — délivré le 4 novembre 2026**

FORMATION ACADÉMIQUE

- Master of Science en informatique : génie logiciel (MSc) | Woolf (Malte / UE) | 2026
- Doctorat en administration des affaires (DBA) | Atlanta College of Liberal Arts and Sciences (ACLAS / États-Unis) | 2026

- Master en informatique (MCS) | Atlanta College of Liberal Arts and Sciences (ACLAS / États-Unis) | 2026
- Master en administration des affaires (MBA) | Atlanta College of Liberal Arts and Sciences (ACLAS / États-Unis) | 2026
- Mini-MBA – Management des entreprises | International Business Management Institute (IBMI / Allemagne) | 2022
- Brevet de technicien supérieur (BTS) – Informatique / Réseaux | Établissement de formation professionnelle, Algérie | 2019–2022

NORMES, RÉFÉRENTIELS ET RÉGLEMENTATIONS

- **Sécurité de l'information, GRC et systèmes de management:** 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, conformité et résilience:** 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 et référentiels de cybersécurité américains:** 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.
- **Sécurité technique, menaces et détection:** 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.
- **Sécurité applicative, DevSecOps et assurance logicielle:** 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).
- **Sécurité du cloud:** CSA CCM • CSA CAIQ • CSA STAR • ISO/IEC 27017 • ISO/IEC 27018 • Zero Trust Architecture • NIST SP 800-207.
- **Sécurité des paiements, de la banque et des services financiers:** PCI DSS • PCI Secure Software Standard • PCI Secure SLC • SWIFT CSCF • DORA • PSD2 • SAMA Cybersecurity Framework.
- **Réponse aux incidents, SOC, CSIRT et 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 / infrastructures critiques:** ISA/IEC 62443 • IEC 61508 • IEC 61511 • NIST SP 800-82 • MITRE ATT&CK for ICS • NERC CIP • Saudi NCA OTCC.
- **Protection des données, vie privée et gouvernance de l'IA:** ISO/IEC 27701 • ISO/IEC 29100 • HIPAA Security Rule • ISO/IEC 42001 • EU AI Act • NIST AI RMF.
- **Réglementations européennes en cybersécurité et numérique:** NIS2 • DORA • Cyber Resilience Act • eIDAS • PSD2 • ENISA guidance and sectoral good practices.
- **Référentiels algériens, moyen-orientaux et régionaux:** 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 ET RESSOURCES PROFESSIONNELLES ORIGINALES

- **The InfoSec Control Room (2026) :** créateur et animateur d'un podcast éditorial consacré à la gouvernance, aux contrôles, aux décisions de risque, aux SOC/CSIRT, à la résilience et à la responsabilité des dirigeants.
- **Cyber Master Series Briefing (2026) :** articles originaux et éditions d'une newsletter destinés aux praticiens sur l'efficacité des SOC, la gouvernance de sécurité et les nouvelles responsabilités des RSSI.
- **Cyber Master Series Field Guides and Certification Study Series (2026) :** auteur de ressources pédagogiques, références téléchargeables et éditions interactives de préparation aux certifications, avec des dépôts GitHub publics.
- Conférences professionnelles, supports d'ateliers et programmes gratuits de développement des capacités en cybersécurité, y compris l'accompagnement des praticiens et des ressources de préparation aux certifications.

LANGUES ET DISPONIBILITÉ

- Arabe : langue maternelle | Anglais : courant / bilingue | Français : intermédiaire.
- Disponible pour des fonctions permanentes de direction et une mobilité internationale ; également ouvert aux missions de conseil, d'audit et de formation.

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

Informations détaillées et justificatifs disponibles sur demande.