Ali LARIBI
CEO Fortress Plus (France) - Trustwave et Near Trust (Tunisie)
Expert International en cybersécurité IT/OT/des systèmes industriels
Ingénieur IIA, INSAT
Certifié CISSP®, CISM®, CPP®, ISA/IEC 62443, ISO 27001 LA, ISO 27005 LRM, MEHARI RM, ISO 22301 LI, PECB Certified Trainer, CISCO CCNA R&S, CCNA SECURITY
Zone d'intervention : France / International
Expérience : +15 ans
Réferences: EDF, Faurecia/Forvia group, Total Energies, chantiers de l'atlantique (Engie, EDP renewables, Ørsted), Qatar Energies, SFR, ADP, Yogosha, wkw automotive, ATB Bank, BH Bank, Attijari Bank, Société Générale, novation city, etc.

DIPLOMES

- **2001 – 2007 : Diplôme d'ingénieur** en Sciences Appliquées & Technologie
  Filière : Informatique Industrielle & Automatique, INSAT

LANGUES

- **Français :** Courant, **Anglais :** Courant, **Arabe** : native

CERTIFICATIONS

- **Certified Information Systems Security Professional, CISSP®**, $(ISC)^2$, **ID 882191**
- **Certified Information Security Manager CISM®,** ISACA, **ID 1948180**
- **Certified Protection Professional CPP®,** ASIS, **ID 20625**
- **ISA/IEC 62443 CFS,** ISA
- **ISO/IEC 27001** Information security management Lead Auditor, PECB
- **ISO 27005** Lead Information security Risk Manager, PECB
- **MEHARI /EBIOS** Risk Manager-PECB
- **ISO/IEC 22301** Business Continuity Lead Implementer, PECB
- **Certified PECB Trainer**
- **Expert-Auditeur** en Cyber sécurité, Certifié par ANSI TN
- **CCNA Security**, CISCO
- **CCNA Switching/Routing**, CISCO
- **Lead SCADA Security Manager,** PECB

INTERVENTIONS

- **International Speaker/Panelist (IT/OT Cybersecurity Topics):**

  - 11th Cyber & SCADA Security in Energy Sector **Amsterdam** 2024
  - ADAPT AFRICA BC & Resilience Conference **Tunisia** 2024
  - Sixth Annual Managed Security Services Forum **London** 2024
  - Cyber/physical security convergence, IFPO MENASA **Saudi Arabia** 2024
  - Cyber OT secure summit **Dubai** 2024
  - PECB **Paris** conference 2023

- PECB DataSafe Symposium 2023
- PECB **Brussels** conference 2022
- Cyber- Physical (IT/OT) security convergence seminar-ASIS **Hong-Kong** 2022
- PECB virtual conference 2021
- Cybersecurity & Cloud expo **Tunisia** 2022
- Innovation & Cyber security in civil aviation **Marrakesh** 2020
- PECB **Brussels** conference 2019
- International Datacentres Forum-**Dublin** 2019
- Security **North Africa** Expo 2018
- HSSE Conference 2017,
- Etc.

EXPERIENCE PROFESSIONNELLE (Principales missions)

■ **Depuis 02/2021 : Fortress Plus (France), Expert en cybersécurité IT/OT/des systèmes industriels**

Clients : EDF, Total Energies, ADP (Aéroport de Paris), etc.

- Aide à la définition de la feuille de route de la cybersécurité OT
- Préparation du CSMS (programme de cybersécurité OT) : périmètre, politiques, procédures, lignes directrices, évaluation des risques, sensibilisation, etc.
- Assistance à la mise en conformité avec la directive NIS 2
- Animation des sessions de formation (Intra/inter) : IEC 62443, Scada manager, installations des systèmes industriels
- Sensibilisation et formation des équipes internes et externes à la cybersécurité.
- Audit : Analyse des lacunes en matière de cybersécurité OT et plan d'actions
- Rédaction et mise en œuvre du Framework TPRM (Third Party Risk Management) et SCRM (Supply Chain Risk Management)
- Conception/conseil sur l'architecture OT sécurisée : modèle Purdue, zones et conduits, DMZ, accès à distance sécurisé, détection, surveillance, zéro trust, DAT, etc.
- Audit interne de la cybersécurité/niveau de maturité selon IEC 62443 et NIST CSF (govern, identify, protect, detect, respond and recover)
- Préparation des exigences cyber OT pour les appels d'offres, évaluation des réponses : EPCI, fournisseurs, intégrateurs, etc.
- Security by design, intégration de la sécurité dans les projets : conception du workflow et définition des activités de sécurité pour chaque phase projet
- Évaluation des risques : Inventaire des actifs, SUC, évaluation des risques de haut niveau (HLRA), évaluation détaillée des risques (DRA), zones et conduites, plan d'atténuation des risques DRA, etc.
- Examen de l'architecture de sécurité existante, identification des lacunes en matière de conception et recommandation d'améliorations de la sécurité dans le cadre d'une approche fondée sur la security by design et la protection en profondeur.
- Participer à la conception de l'architecture du réseau et de la sécurité, modèle Purdue, DMZ, VLAN, zones et conduits, cloud, communication, etc.
- Préparation des tests de cybersécurité (FAT, HAT, SAT) : analyse des vulnérabilités, détection des menaces et pentesting.

Environnement Technique : IEC 62443,NIST SP 800 82, NIST CSF, ISO 27001, ISO 27005, NIS 2, NERC-CIP, IEC 61508, ANSSI & CPNI Guidelines, Nozomi, etc.

■ **07/2022-05/2023 : Chantiers de l'atlantique (Saint-Nazaire) :** Energies Marines & Ingénierie, **Expert/Réfèrent /Architecte cybersécurité IT/OT**

Responsabilités / Projets : Expertise cybersécurité IT/OT, ISP (Intégration de la sécurité dans les projets), architecture OT, organisation de l'activité cyber OT

Client : **LEMS (Engie, EDP renewables), Ørsted** (Denmark)

Scope : Responsable de la partie cybersécurité IT/OT des projets clé en main EPCIM (Engineering, Procurement, Construction, Installation and Maintenance) et de l'organisation de la fonction cybersécurité

OT/industrielle.

- Évaluation de la maturité cybersécurité (auto-évaluation) : périmètre, évaluation de l'état actuel, identification d'un profil cible, évaluation et hiérarchisation des lacunes, remédiation et feuille de route.
- Elaboration de la politique globale de la cybersécurité OT et des politiques thématiques
- Définition et ajustement des procédures de cybersécurité OT : hardening, patch management, log et event management, backup & restore, malware protection, account management, etc.
- Évaluation de la maturité cybersécurité des fournisseurs : gestion des risques liés aux tiers et gestion des risques liés à la chaîne d'approvisionnement) sur la base des normes IEC 62443, NIST SP800 82 r2/3, NIS 1/2 et ISO 27001.
- Responsable de l'intégration de la sécurité dans les projets ISP/security by design : Planification et lancement du projet, acquisition, analyse et conception, mise en œuvre/intégration, vérification et validation, exploitation, maintenance et déclassement.
- Conformité NIS 2 du périmètre identifié
- Négociation avec les clients les objectifs à atteindre en termes de cybersécurité, et qualification des moyens à mettre en oeuvre en fonction des normes associées au projet (IEC 62443, NERC-CIP...).
- Sensibilisation et coaching de l'équipe projet (au sujet de la cybersécurité des systèmes OT/IIOT (mythes et réalités)
- Développement des outils adaptés, et définition des exigences cybersécurité auprès des partenaires et fournisseurs
- Identification et gestion des risques IT/OT/IIOT : identification des SUC (system under consideration), High level risk assessment, définition des zones et conduits, Detailed risk assessment, définition des risk mitigation plan
- Suivi, coordination, respect et mise en place des mesures de cybersécurité avec les fournisseurs et proposition des mesures compensatoires si nécessaire
- Conception d'une architecture sécurisée : protection en profondeur, zéro trust, zones et conduits, perdue model, NIST CSF, etc.
- Support technique aux partenaires et fournisseurs dans l'application de nos exigences
- Orientation des équipes internes dans les choix techniques à mettre en oeuvre pour garantir l'atteinte des performances.
- Préparation des tests cybersécurité durant le FAT, HAT et SAT
- Vérification et analyses des tests d'intrusion (pentesting et scan de vulnérabilités) avant la livraison de la sous station

Environnement Technique : IEC 62443, NIST SP 800 82, NIST CSF, ISO 27001, ISO 27005, NIS 2, NERC-CIP, IEC 61508, ANSSI & CPNI Guidelines, Nozomi, CyberArk, SEL, Qradar, etc.

- **05/2020-07/2022 : Groupe Faurecia (Forvia), Conseiller cybersécurité IT/OT**, Nanterre-France :

Responsabilités / Projets :

- Analyse des risques sécurité (nouveaux projets IT/OT/IIOT/IoT du groupe) : High level risk assessment, définition des zones et conduits, detailed risk assessment et de risk mitigation plan
- Évaluation/audit cybersécurité des systèmes industriels existants : audit technique/organisationnel et audit d'architecture
- Évaluation de la sensibilité des projets selon les priorités cybersécurité (DICT) et la conformité SOC 2, ISO, TISAX, NIST, IEC 62443, etc.
- Conception et exploitation du Framework « Third Party Risk Management TPRM » du groupe
- Analyse de la documentation cybersécurité, évaluation, validation (Go/no Go) des nouvelles solutions/applications/services et des prestataires/fournisseurs.
- Évaluation de la maturité cybersécurité des Third Parties, évaluation des risques liés à la chaine logistique (supply chain risk management)
- Responsable de l'intégration de la sécurité dans les projets ISP/security by design : projets cloud,

IT/OT/ICS

- SSDLC, intégration de la cybersécurité dans les systèmes embarqués/IOT : parties hardware/software
- Préparation des exigences sécurité (internal cybersecurity requirements) selon la criticité et la sensibilité du chaque projet pour l'équipe interne (architecte sécurité, équipe infra, …)
- Conception des solutions/architectures OT/IIOT sécurisées : purdue model, découpage en zones et conduits et selon NIST CSF
- Préparation des exigences de la configuration sécurisée (Input) pour l'architecte sécurité : firewall, IDS/IPS, Proxy, IAM, PAM, jump host …
- Représentant de l'équipe Advisory Cybersecurity dans les steering committee meetings (suivi des projets avec réserves cybersécurité)
- Conseil, assistance et support des équipes métiers : présentation des risques sécurité en comité projet, plan d'actions, risques résiduels, acceptation des risques…, en s'appuyant sur les méthodologies, normes et bonnes pratiques, EBIOS RM, ISO 27001/27005, IEC 62443, NIST, CSA, etc. ;
- Analyse et mise à jour des dossiers de sécurité et de la base documentaire (politique, procédures, guidelines, standard, DAT, etc.)
- Présentation (aux différents acteurs du projet) des risques résiduels en adaptant les résultats des audits et des analyses de risques aux contextes métiers, en identifiant des plans de mitigation des risques
- Sensibilisation et coaching cybersécurité IT/OT
- Préparation/ présentation des KPIs cybersécurité de notre activité (Advisory) dans le comité cybersecurité mensuel et reporting au CISO groupe

Environnement Technique : NIST SP 800 XX, IEC 62443, TISAX, Claroty, Cloud Security Alliance, SDLC, ISO 27001, ISO 27005, OWASP TOP 10, Mitre Att & CK, ICS Security, COBIT, Claroty, CyberArk, CMMI, ITIL, CPNI guidelines, Microsoft Azure, VMware, etc.

■ **11/2018-04/2020 : SFR Business, Consultant senior Cyber sécurité/Responsable SMSI** « des systèmes industriels : (06 Datacenters/France) »

- **06 Datacenters :** Courbevoie, Val de Reuil, Bordeaux, Venissieux, Trappes, Strasbourg
- **Certification des Infrastructures Physiques et Industriels des Datacenters :** Systèmes Industriels, Energie, Climatisation, Sécurité Physique, etc.

Responsabilités / Projet :

- Elaboration de la politique cybersécurité industrielle spécifique aux infrastructures physiques des datacenters avec les personnes concernées
- Garant de l'alignement de politique cyber sécurité avec les objectifs business
- Réalisation de l'analyse des risques SI industriel selon ISO27005/EBIOS (identification, analyse, évaluation, et traitement), NIST SP 800 82, IEC 62443, IEC 61508, Guides ANSSI
- Préparation de la cartographie des risques des systèmes d'informations industriels des 06 sites
- Coordinateur/réfèrent sécurité pour les responsables sites, la maintenance, l'ingénierie, responsable contrat, mainteneurs, prestataires, etc.
- Préparation, MAJ et élaboration du programme SI, DDA, manuel sécurité, procédures, etc.
- Préparation à la certification de 02 nouveaux DC Trappes et Strasbourg)
- Garant du maintien de la certification ISO27001 en 2019 et préparation pour le renouvellement 01/2020 pour 04 Datacenters (Audit AFNOR)
- Intégration de la sécurité dans les projets (ISP) : Phases Build et Run (sécurité de bout en bout)
  EXP : Projet GTC/Supervision centralisée, Projet contrôle des accès physiques, Projet de changement de la redondance d'un site Tier I à Tier III (Taux de disponibilité : 99,982 %, 1,6 heure (moyenne) d'interruption par an).
- Analyse des impacts (BIA) et appréciation des risques, implémentation PCA Datacenter
- Identification des scénarii d'incidents/plan de remédiation et proposition des exercices de test : perte d'un site, perte réseau EDF, Perte fournisseur critique, perte prestataire critique, etc.
- Scan de vulnérabilités et pentesting (SI industriel)
- Coordination des projets RGPD/PIA pour le périmètre Datacenter et Cloud V3/Services manages
- Animation de sessions de sensibilisation sécurité de l'information des collaborateurs (interne et

externe) en SSI et prestataires (VINCI, DALKIA, SNEF : sécurité des systèmes industriels)
- Elaboration de l'annexe de sécurité des systèmes industriels ajoutée au contrat de prestation de services (Maintenance corrective et préventive)
- Suivi de l'avancement de la maintenance préventive des actifs industriels/infrastructures physiques avec les responsables des sites et les prestataires : DALKIA, VINCI, SEIMENS, TOSHBA, MITSUBISHI, SOCOMEC, SCHNEIDER, etc.
- Garant du niveau de sécurité sur le périmètre Datacenter
- Garant de l'applicabilité des procédures SSI génériques (IT) et spécifiques (OT) sur le périmètre DC, rédaction de procédures SSI sur le périmètre DC
- Suivi et reporting : PTR (Plan de Traitement des Risques) et PCSO (Plan de Surveillance et Contrôle Obligatoire)
- Référent SSI sur les projets dans le périmètre certifié
- Garant de la réalisation et de la consolidation des kpi SSI sur le périmètre DC
- Garant du suivi de mise en œuvre des actions correctives et préventives identifiées suite aux audits interne et externe
- Garant du suivi de remédiation à la suite des audits techniques

Environnement Technique : ISO 27001, ISO 27005, EBIOS, NIST SP 800 82, IEC 62443, IEC 61508, ANSSI, CPNI Guidelines, ISO 22301

■ **06/2015-09/2018 : PANTHERA, Directeur bureau Maghreb/Consultant sénior en sécurité, Rhône-Alpes, France**

Secteurs : Industries (Fabrication pièces techniques Auto, électronique, chimique, pharmaceutique, etc.)

Responsabilités / Projet :

- Pilotage des projets, et assurance de la bonne conduite des missions dans leurs ensembles
- Préparation et animation des réunions avec le client (Kick-off, COPIL, Réunion d'avancement)
- Réponses et préparation des offres cyber sécurité (IT et OT), sécurité physique et continuité des activités
- Management d'une équipe de consultants sur les projets : gestion de la qualité, coûts, délais, risques, communication vers les clients et reporting interne
- Inventaire (Infrastructures IT et systèmes industriels, OT) et étude de l'existant (Gap Analysis)
- Scan de vulnérabilités et pentesting (systèmes, réseaux, applicatif et installations industrielles)
- Elaboration : recommandations, schéma directeur, Feuille de route, Plan d'action avec priorité, Quick wins, procédures de sécurité
- Définition de politique de sécurité, de gestion de crise et de continuité d'activités
- Audit de la Sécurité du Système d'Information (IT et Industriel) en conformité avec la norme ISO 27001, Annexe A, ISO27002 (Cyber sécurité IT) et IEC 61508 (sécurité fonctionnelle), IEC 62443 (cyber sécurité des installations industrielles)
- Gestion des risques selon la norme ISO 27005 / EBIOS / HAZOP
- Analyse des impacts (BIA) et appréciation du risque, Assistance à l'implémentation PCA et PRA
- Identifications des scénarii, mise en place de projets, de procédures, des d'exercices de simulation pour améliorer les dispositifs de continuité d'activité
- Accompagnement à la réalisation du plan de gestion de crise : Niveau d'incident, Equipe de gestion d'incident, cellule de crise, type d'incident : malveillance, IT, OT, cyber, incendie, etc.
- Formation à la gestion et à la communication de crise (niveau d'incident, PC sécurité, cellule de crise, communication, SOC, coordination interne et externe, etc.)
- Préparation des Scénarii de crise, Mise en place du plan d'urgence
- Conception des systèmes de sécurité physique/solutions convergentes

Environnement Technique : ISO 27001, ISO 27005, EBIOS, NIST SP 800 82, IEC 62443, IEC 61508, Guides ANSSI, CPNI Guideline, AMDEC, HAZOP, ISO 22301, Guidelines ASIS, CNPP APSAD, ISO 31000

■ **12/2013 -11/2015 : BUSINESS SHIELD, Consultant Continuité d'Activité et Gestion de Crise**

Secteurs : industries, OIL & GAZ, Afrique de Nord

Responsabilités / Projet :

- Évaluation des risques de sécurité / analyse de vulnérabilité / cartographie des risques
- Conseil en gestion de crise (définition de la politique, aide à la rédaction de documents d'exploitation), Accompagnement à la réalisation du plan de gestion de crise
- Organisation de crise, Ingénierie et transfert de compétences
- Formation à la gestion et à la communication de crise
- Conception des procédures de gestion de crise, de continuité des métiers et IT
- Identification des risques et des impacts en cas de crise,
- Mise en oeuvre d'un SMCA selon l'ISO 22301
- Préparation des Scénarii de crise, Mise en place du plan d'urgence
- Organisation d'exercice de gestion de crise, de PCA et de PSI

Environnement Technique *:* ISO 27001, ISO 27005, EBIOS, ISO 22301, Guidelines ASIS, ISO 31000

■ **02/2011-01/2013 : ATFP - Conseiller/Formateur en sécurité**

- Sessions de formation en sécurité
- Mise en place des contrôle/barrières de sécurité (FW, WAF, IPS/IDS, Anti-malware, PKI, politiques de cryptage, NAC, …)
- Administration des solutions de sécurité (pare-feu, antivirus, proxy, …)
- Scan de vulnérabilités (systèmes, réseaux et applications)
- Analyse et traitement des incidents de sécurité,
- Développement des procédures de sécurité opérationnelles,
- Développement du plan de contrôle « cyber » et des tableaux de bord sécurité,
- Participation aux actions de développement de la politique de sécurité.

Environnement Technique*:* Cisco firewalls, Cisco switching, F5, Juniper firewalls, Stonesoft IPS/IDS, Mcafee, SPLUNK, …

■ **07/2008-01/2011 : CFAK Tunisie, Ingénieur Technique**

Secteurs : industries (textile, électronique, chimique)

Responsabilités / Projet :

- Etude du cahier des charges client.
- Gestion du relationnel client
- Développement et conception de nouvelles machines/lignes, conformément aux demandes clients (exp : convoyeurs pour une chaine de production)
- Programmation automate (Siemens)
- Coordination avec les équipes techniques (calculs, prototypes, essais) afin de valider les solutions
- Résolution de problèmes fonctionnels et adaptation de produits existants
- Suivi des essais et installation sur site
- Rédaction de la documentation machine
- Formation et assistance client

Environnement technologique : Api Simatic Simens, Logo, Step 7, Sql, Modebus,

■ **02/2007-06/2008 : TIMELEC-GROUPE SOCOMEC France, Chef de projet Industriel**

Responsabilités / Projet :

- Suivi d'activités des unités de production et analyse des dysfonctionnements dans les différentes étapes du processus de fabrication.
- Etude des projets d'amélioration de la production et de minimisation des pertes, avec les responsables concernés (production, qualité, maintenance, industrialisation, etc.).

- Suivi de l'intégration de nouvelles technologies, supervision des étapes de test et de mise au point des process.
- Supervision des phases de tests et de mise au point des process et étude des solutions technologiques pour réduire les risques industriels et fiabilisation des process de production.
- Participation à la définition de l'instrumentation associée aux process (sélection des technologies capteurs et pilotage des études d'intégration)
- Participation à l'obtention de certification ISO 9001
- Pilote AMDEC Process et chantiers d'améliorations continues/ Lean Manufacturing (5S, SMED, TPM)

INTERVENTIONS

- **Depuis 2018 : Formateur Agréé par PECB**, Animation de sessions de préparation à la certification : ISO 27001 LA, ISO 27005 LRM, ISO 22301 LI, MEHARI RM
- **2011➔ 2014 : Conférencier en cyber sécurité** (Vacation, 3h/Semaine), ECOLE POLYTECHNIQUE CENTRALE : Master Professionnel en sécurité système d'information
- **2011 ➔ 2014 : Cisco Instructor** (Vacation, 3h/Semaine), Université UAS : Ingénieurs IT