OT-Knight
An RBJCS brand

PORTFOLIO DE SERVICES ET FORMATIONS



CYBERSÉCURITÉ OT/ICS · SÉCURITÉ FONCTIONNELLE

Dans l'OT et les infrastructures critiques, la cybersécurité devient une fonction de sécurité.

Protéger ce qui fait fonctionner votre site. Les personnes, les processus et la technologie, de la première esquisse au dernier poste, avec un partenaire responsable.

Concept et FEED	Conception détaillée	Construction, FAT et SAT	Mise en service	Exploitation et maintenance	Modification et renouvellement

Gestion de la cybersécurité OT en tant que service · sur tout le cycle de vie

POUR LES EXPLOITANTS ET FABRICANTS DE

Infrastructures critiques · Pétrole et gaz · Pétrochimie · Renouvelables · BESS · Production, transport et distribution d'électricité

information@ot-knight.com
Belgique · Europe · Moyen-Orient

LE DÉFI

Sécurité fonctionnelle, cybersécurité, fiabilité et productivité.

NIS 2 et le CRA durcissent la réglementation. Nous réunissons cybersécurité OT et sécurité fonctionnelle dans des programmes adaptés à la salle de contrôle, aux arrêts programmés et au dossier de sécurité.

NOTRE RÉPONSE

La sécurité comme point de départ

IEC 62443 rejoint IEC 61511 et ISA TR84.00.09 : les cybermenaces sur vos fonctions de sécurité se traitent avec les risques de procédé.

Une gouvernance adaptée à l'OT

IEC 62443 et ISO/IEC 27001 réunies dans un système de management, construit autour des personnes qui exploitent et entretiennent vos actifs.

L'expérience au service du conseil

Des compétences certifiées et une réelle expérience industrielle, avec une participation au comité technique ISASecure ACSSA.

80+ années cumulées d'expérience OT

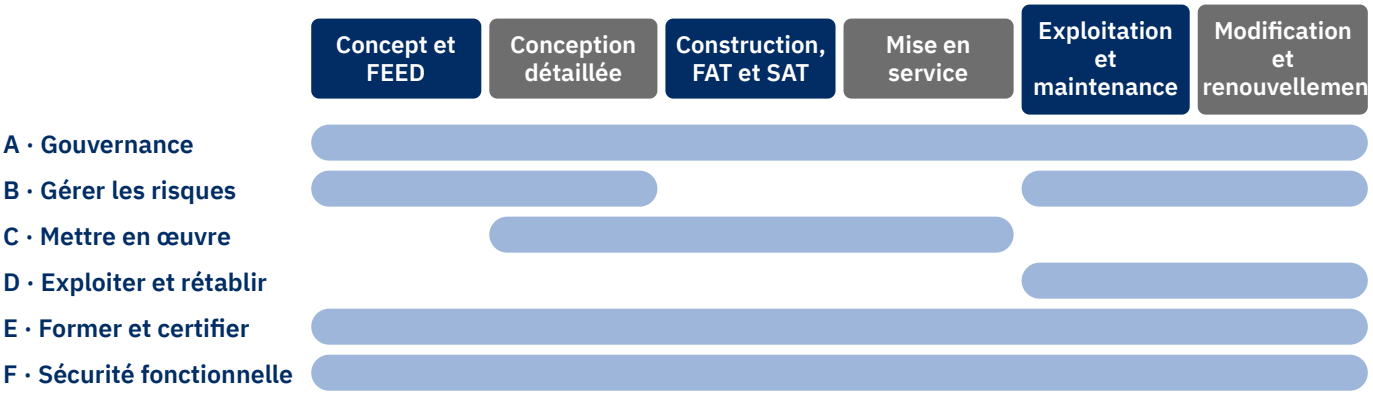
6 étapes, du FEED au renouvellement

6 familles, un partenaire responsable

ML1–3 parcours de certification ACSSA

Un partenaire responsable à chaque étape

Où intervient chaque famille de services



Personnes

Sensibilisation, compétences et rôles clairs, de l'opérateur au conseil.

Processus

Gouvernance, gestion des risques et procédures adaptées au terrain.

Technologie

Architecture sécurisée, mesures et vérification en conditions réelles.

A Gouvernance et conformité

Un système de management pour l'IT et l'OT, et une approche de conformité commune dans tous vos pays.

A1

Système unifié de management de la cybersécurité

IEC 62443 intégrée à ISO/IEC 27001

Un seul système de management pour l'IT et l'OT, construit côté OT pour que les mesures fonctionnent en salle de contrôle.

VOUS OBTENEZ

- Système de management combiné, Déclaration d'applicabilité (SPE IEC 62443-2-1 + Annexe A ISO/IEC 27001)
- Procédures OT pour opérateurs et équipes de maintenance
- Préparation à ISO/IEC 27001 et ISASecure ACSSA

A2

NIS 2 — mise en œuvre nationale

Conformité de tout le site, OT compris, par pays

Socle commun de groupe adapté aux exigences nationales de NIS 2, notamment en Belgique (CyFun®) et en France.

VOUS OBTENEZ

- Classification des entités et périmètre par site et pays
- Socle commun de groupe adapté aux exigences nationales
- Preuves pour les autorités de contrôle et notification des incidents

A3

Programme de cybersécurité sur le cycle de vie

Pour les entités SEVESO ou COMAH

Un plan de management de la sécurité fonctionnelle et de la cybersécurité aligné sur IEC 62443 et IEC 61511.

VOUS OBTENEZ

- FS/CSMP avec activités par phase et jalon
- Transfert EPC–exploitation et critères d'acceptation
- KPI, reporting de direction et intégration MOC

A4

Certification ISASecure ACSSA

De ML1 jusqu'à ML3

ACSSA est la certification ISASecure pour les propriétaires et exploitants qui mettent en œuvre IEC 62443. Nous vous accompagnons sur tout le parcours.

VOUS OBTENEZ

- Éligibilité, périmètre et découpage en zones
- Analyse des écarts selon IEC 62443-2-1, -3-2, -2-4 et -3-3
- Audit à blanc puis soutien jusqu'à la certification

A5

Cybersécurité de la chaîne d'approvisionnement

Une même exigence pour chaque fournisseur

EPC, intégrateurs, OEM et prestataires soumis aux mêmes exigences, de l'appel d'offres à la réception.

VOUS OBTENEZ

- Exigences IEC 62443-2-4 dans les appels d'offres et contrats
- Registre des tiers et évaluation des fournisseurs
- Exigences de conformité CRA pour vos achats

A6

Règlement européen sur la cyberrésilience

Pour fabricants et intégrateurs

Nous combinons la norme horizontale EN 40000, les normes verticales et IEC 62443-4-1 / -4-2 : un seul jeu de preuves pour toutes.

VOUS OBTENEZ

- Classification du produit et voie de conformité
- Risques produit et cycle de développement sécurisé
- Gestion des vulnérabilités, notification, dossier technique

B Évaluer et gérer les risques

Connaître vos risques avant d'investir : un langage commun du risque, de la direction à la salle de contrôle.

B1 Cadre de gestion des risques

Fondé sur ISO 31000, il relie les exigences organisationnelles IEC 62443-2-1, l'analyse de risques OT IEC 62443-3-2 et ISO/IEC 27005, sur votre matrice HSE.

LIVRABLES · méthodologie, critères, registre et traitement des risques

B2 Évaluations des risques IEC 62443-3-2

Système considéré, zones et conduits, analyse initiale et détaillée, et un niveau de sécurité cible par zone.

LIVRABLES · modèle zones et conduits, SL-T, rapport de risques, CRS

B3 Alignement cybersécurité–sécurité fonctionnelle

Cybermenaces sur votre SIS évaluées comme l'exige IEC 61511, selon ISA TR84.00.09, et intégrées aux HAZOP et LOPA.

LIVRABLES · risques cyber du SIS, interface BPCS/SIS, apports à la SRS

B4 Analyses des écarts

Votre position vis-à-vis d'IEC 62443, ISO/IEC 27001, des exigences nationales de NIS 2, du CRA ou des critères ACSSA.

LIVRABLES · rapport d'écarts, maturité, feuille de route selon vos arrêts

C Mettre en œuvre et vérifier

Traiter les écarts. Puis le démontrer.

C1 Exigences et spécifications

Les exigences IEC 62443-3-3 pour votre SL cible deviennent la base de conception des livraisons EPC et fournisseurs.

LIVRABLES · TRS (spécification des exigences techniques), segmentation, accès distant, reprise

C2 Gestion de la cybersécurité OT en tant que service

Nous assurons votre fonction cybersécurité OT, des objectifs et projets jusqu'aux audits.

LIVRABLES · responsable désigné, pilotage, outils, ToR, audits, conseil à la demande

C3 Projets de traitement des écarts

Segmentation, interface IT/OT sécurisée, accès distant, durcissement, comptes, sauvegardes et surveillance.

LIVRABLES · périmètre, choix des fournisseurs, supervision, preuves de clôture

C4 Assurance et vérification

Tests sûrs sur site en exploitation, par ceux qui le connaissent : vérification SL, FAT/SAT cyber, évaluations OT, tests d'intrusion OT et audits.

LIVRABLES · protocoles, rapports témoins, vérification SL, constats

Gestion de la cybersécurité OT en tant que service sur tout le cycle de vie

- Un responsable OT désigné à vos côtés
- Projets de cybersécurité pilotés
- Outils OT choisis avec vous
- Audits internes et externes préparés
- Objectifs de sécurité définis et suivis
- Écarts traités jusqu'à leur clôture
- Cahiers des charges
- Réponses aux questions ponctuelles

D Exploiter et rétablir

Sécurisé au quotidien. Prêt pour les jours difficiles.

D1 Évaluation de la posture opérationnelle

Au-delà des documents : architecture, accès distant, comptes, sauvegardes, supports amovibles et pratiques quotidiennes.

LIVRABLES · score par SPE (62443-2-1) et FR (62443-3-3), risques clés, plan à 90 jours

D2 Réponse aux incidents OT

Plans de réponse et scénarios opérationnels, alignés sur la réponse d'urgence du site et les obligations réglementaires de notification.

LIVRABLES · plan de réponse, playbooks, matrice d'escalade, exercices sur table

D3 Continuité et reprise après sinistre

Rétablissez vos systèmes OT dans les délais définis, en combinant IEC 62443 AVAIL, ISO 22301, ISO/IEC 27031 et les pratiques NIST.

LIVRABLES · BIA OT, RTO/RPO, procédures et tests de restauration

D4 Surveillance OT, NDR, EDR et SOC

Nous définissons ce que vos NDR, EDR, outils de supervision et OT-SOC doivent apporter, choisissons le bon prestataire et pilotons sa performance, sans lien avec aucun fournisseur de SOC.

LIVRABLES · périmètre OT-SOC, KPI, choix du prestataire

E Former et certifier

Les personnes sont la première ligne de défense.

E1 Formations certifiantes ISA et PECB

Cours certifiants ISA/IEC 62443 (IC32, IC33, IC34, IC37, IC49) et PECB (NIS 2, ISO/IEC 27001, ISO 31000), dispensés par notre ISA Qualified Instructor et PECB Certified Trainer via notre organisme de formation autorisé, en intra ou en inter.

E2 Sensibilisation et compétences

Sessions sur mesure pour opérateurs, techniciens, ingénieurs, sous-traitants et conseils, y compris la formation des organes de direction NIS 2, fondées sur une vraie expérience terrain.



« La sécurité fonctionnelle et la cybersécurité ne sont pas simplement analogues : elles se rencontrent littéralement dans le même contrôleur. »

C'est pourquoi chaque mission OT-Knight intègre la cybersécurité à votre dossier de sécurité.

F Sécurité fonctionnelle

Alignée sur le cycle de vie de sécurité IEC 61511 : sûre dès la conception, et sûre en exploitation.

F1 Management de la sécurité fonctionnelle et du cycle de vie

Nous mettons en place et pilotons le système de management qui garde votre SIS sûr toute sa vie : un système permanent pour un site en exploitation, ou un plan de sécurité fonctionnelle au sein d'un projet d'investissement. Prêt pour l'évaluation, avec une remise propre à l'exploitation.

- Planification du cycle de vie et de la validation
- Gestion des compétences
- Gestion des modifications
- Rôles propriétaire, sous-traitants et fournisseurs
- Planification vérifications et FSA
- Maîtrise documentaire

F2 Évaluations de sécurité fonctionnelle

FSA indépendantes à chaque étape du cycle de vie, de l'analyse des dangers et des risques et de la SRS à la mise en service, l'exploitation et les modifications, ainsi que des audits qui vérifient l'application de vos procédures.

LIVRABLES · rapports FSA, audits de sécurité fonctionnelle, registre des constats

F3 Exigences de sécurité (SRS)

Nous rédigeons ou revoyons la SRS de chaque fonction instrumentée de sécurité : état sûr, seuils de déclenchement, temps de réponse, SIL cible, règles d'inhibition et de réarmement, exigences de tests périodiques.

LIVRABLES · SRS, liste des SIF, commentaires de revue

F4 Vérification SIL

PFD, tolérance aux fautes matérielles, contraintes d'architecture et capacité systématique vérifiées pour chaque SIL cible : un calcul indépendant, défendable lors d'une évaluation.

LIVRABLES · rapport de vérification SIL, recommandations

F5 Appui exploitation et maintenance

Procédures de tests périodiques et optimisation des intervalles, suivi des sollicitations et des défaillances, gestion des inhibitions et revue des modifications du SIS en exploitation.

LIVRABLES · procédures de tests périodiques, revues de performance du SIS, revues MoC

F6 Certifiez votre FSMS

Nous vous guidons dans le choix de l'organisme de certification et tout au long du processus. Nous avons mené un système de management de la sécurité fonctionnelle jusqu'à la certification exida : nous connaissons le parcours de l'intérieur.

+ Sécurité et cybersécurité réunies

Un SIS nécessite sa propre analyse des risques de cybersécurité selon IEC 61511. Nous la réalisons en même temps que nos travaux de sécurité fonctionnelle (voir B3) et formons vos équipes aux deux (pages 7–9).

À vos côtés sur tout le cycle de vie de sécurité IEC 61511

De l'analyse des dangers au démantèlement

Analyse des dangers et des risques	Allocation SIL et SRS	Conception et ingénierie	Installation, FAT et validation	Exploitation et maintenance	Modification et démantèlement

Portfolio de formations

Des connaissances qui reviennent sur le terrain.

Huit programmes spécialisés, adaptés à votre équipe, vos actifs et votre maturité. Le contenu, le niveau de détail et les exercices peuvent être adaptés à votre contexte réglementaire : ateliers sur site, formations sur plusieurs jours et séances pour dirigeants, en anglais, français ou espagnol.

FORMAT D'UN JOUR — T1 et T2 peuvent devenir un atelier d'une journée sur site avec un exercice pratique condensé. Durées indicatives.

PARCOURS CERTIFIANTS

Formations ISA et PECB autorisées · supports PECB en français

- **IC32** Using the ISA/IEC 62443 Standards to Secure Your Control Systems
- **IC33** Assessing the Cybersecurity of New or Existing IACS Systems
- **IC34** IACS Cybersecurity Design & Implementation
- **IC37** IACS Cybersecurity Operations & Maintenance
- **IC49** ISASecure Automation and Control System Security Assurance (ACSSA) for Evaluators
- **PECB** Cours NIS 2, ISO/IEC 27001, ISO 31000

T1 Sécurité fonctionnelle et cybersécurité dès la conception

3 JOURS · OPTION 1 JOUR

IEC 61511 · IEC 62443 · ISO/IEC 27001 · ISA-TR84.00.09-2024 · ISASecure ACSSA, pour les exploitants

- Là où les deux cycles de vie se croisent : analyse de risques cyber IEC 61511 (8.2.4), exigences cyber du SIS et impact sur la SRS
- Gouvernance combinée : MoC, compétences, audits et tests périodiques avec la vérification cyber
- Atelier : dossier sécurité fonctionnelle et cyber d'une unité
- ISA-TR84.00.09-2024 en pratique : le cyber comme cause de perte de couches de protection, et l'indépendance SIS/BPCS dans le zonage
- Préparer un site en exploitation à ISASecure ACSSA

T2 Fondamentaux d'IEC 62443 : le langage de la cybersécurité industrielle

1 JOUR

Fondamentaux · Rôles · Panorama des normes

- Structure de la série et rôle de chacun : propriétaire, prestataire, intégrateur, fournisseur de produits
- La feuille de route : 2-1 (programme), 3-2 (risque), 3-3 (système) et 4-1/4-2 (produit)
- Schémas ISASecure (CSA, SSA, SDLA, ACSSA)
- Concepts clés : éléments du programme, zones et conduits, niveaux SL-T, SL-C et SL-A, exigences FR 1–7, défense en profondeur
- Liens avec ISO/IEC 27001 et NIST CSF 2.0

T3 Construire votre programme de cybersécurité IEC 62443

3 JOURS

Pour les propriétaires d'actifs et les exploitants

- IEC 62443-2-1:2024 et ses 8 SPE : ORG, CM, NET, COMP, DATA, USER, EVENT, AVAIL
- Gouvernance, rôles, politiques et procédures réellement utilisés
- KPI et amélioration continue
- Analyse des écarts, niveaux de maturité et feuilles de route priorisées
- Gérer les prestataires avec IEC 62443-2-4

T4 Un cyberrisque qui a du sens : gestion des cyberrisques OT

3 JOURS

IEC 62443-3-2 · ISO/IEC 27005 · ISO 31000

- ISO 31000 comme cadre général, ISO/IEC 27005 pour le risque informationnel et IEC 62443-3-2 pour l'IACS
- Analyse fondée sur les conséquences : lien avec HAZOP et LOPA, calibrage sur la matrice de risques
- ZCR 1 à ZCR 7 : système considéré (SuC), analyse initiale et détaillée, zones et conduits, SL-T et spécification des exigences (CRS)
- Étude de cas, du SuC à la CRS

T5 Un SMSI, deux mondes : unifier IEC 62443 et ISO/IEC 27001

2 JOURS

SMSI · Correspondance des mesures · Programmes d'audit

- Étendre un SMSI de l'IT à l'OT sans rien casser
- Périmètre, Déclaration d'applicabilité (SoA) et traitement des risques OT
- Mesures de l'Annexe A ISO/IEC 27001 face aux exigences IEC 62443-2-1 et aux SR 62443-3-3
- Un seul programme d'audit pour les deux certifications

T6 Sécuriser du cahier des charges au site

3 JOURS

Pour EPC, intégrateurs, fabricants et équipes projet de l'exploitant

- Capacités du prestataire selon IEC 62443-2-4 en intégration et maintenance
- Développement sécurisé IEC 62443-4-1 (SM, SR, SD, SI, SVV, DM, SUM, SG) et passage des exigences composant 4-2 aux capacités système 3-3
- Cybersécurité à chaque phase : FEED, ingénierie de détail, FAT, SAT, réception, exploitation et maintenance
- Livrables et exigences contractuelles : CRS, plans de zones et conduits, durcissement de référence, documentation

T7 Faire confiance, mais vérifier : assurance cybersécurité OT, de l'évaluation des risques au démantèlement

2-3 JOURS

Audit · Vérification · Essais de cybersécurité sûrs

- Plan d'assurance sur tout le cycle de vie : quoi vérifier, quand, comment et avec quelle indépendance
- Tests sûrs en OT : tests FAT/SAT, analyse de vulnérabilités, cadrage de tests d'intrusion sur site en exploitation
- Démantèlement sécurisé : effacement des données, identifiants, gestion du changement
- Auditer les programmes selon IEC 62443-2-1 et 2-4, et vérifier SL-A face à SL-T (3-3)
- Preuves, constats et rapports à la manière des évaluateurs ISASecure

T8 Durcissement et essais pratiques pour les environnements ICS

2 JOURS TRAVAUX PRATIQUES

Avec un expert en tests d'intrusion OT · débutant à intermédiaire

- Un processus de durcissement pratique, indépendant de l'OS : pourquoi, quand, comment et quoi, et ses liens avec IEC 62443
- Vos propres scripts et politiques de durcissement, plus durcissement réseau, physique et utilisateurs
- Durcissement des IHM et serveurs Windows, Linux, équipements réseau et automates, autonomes ou en domaine, avec environnements opérateur restreints
- Vérifier le durcissement avec des outils courants, en labs inspirés de sites réels

F Formation en sécurité fonctionnelle

Compétence IEC 61511 de la salle de contrôle au bureau de projet, construite autour de votre site et de vos procédures.

T9 Sensibilisation à la sécurité fonctionnelle : pourquoi le SIS compte

DEMI-JOURNÉE À 1 JOUR

Pour opérateurs, équipes de maintenance, sous-traitants et managers

- Ce que fait un système instrumenté de sécurité et en quoi il diffère du système de contrôle
- Pourquoi les inhibitions, les forçages et les modifications non revues mettent la protection en danger
- Le cycle de vie de sécurité IEC 61511 en termes simples, et qui est responsable de chaque étape
- Ce que chaque rôle doit faire, et ne doit jamais faire, autour d'une SIF

T10 IEC 61511 en pratique : de l'analyse des dangers à la SRS

3 JOURS

Pour ingénieurs, spécialistes de la sécurité des procédés et équipes projet

- Le cycle de vie de sécurité et l'enchaînement de ses phases : analyse des dangers et des risques, allocation, SRS, conception, validation, exploitation
- Rédiger la SRS : état sûr, seuils de déclenchement, temps de réponse, règles d'inhibition et de réarmement, exigences de tests périodiques
- Détermination du SIL cible avec HAZOP et LOPA, et calage sur la matrice de risque de l'entreprise
- Atelier : d'un scénario de danger à une SRS complète pour une SIF

T11 Vérification SIL : prouver que la conception atteint sa cible

2 JOURS

Pour ingénieurs de conception SIS, EPC et fournisseurs

- Calcul de la PFD pour des architectures types, et les données et hypothèses sous-jacentes
- Fixer l'intervalle de test périodique et documenter ce dont dépend le résultat
- Tolérance aux fautes matérielles, contraintes d'architecture et capacité systématique
- Atelier : vérifier une SIF et défendre le résultat lors d'une évaluation

T12 Exploiter le SIS : tests périodiques, inhibitions et gestion des modifications

2 JOURS

Pour les équipes d'exploitation, de maintenance et d'ingénierie

- Rédiger et exécuter les procédures de tests périodiques, et optimiser les intervalles
- Suivi des sollicitations et des défaillances, et usage des données pour revoir les hypothèses de conception
- Gestion des inhibitions et règles d'exploitation de la SRS
- Revue des modifications du SIS dans le cadre de la gestion des modifications

T13 Management de la sécurité fonctionnelle : piloter le système FSM

2 JOURS

Pour managers, responsables de sécurité fonctionnelle et maîtres d'ouvrage de projet

- Le plan de sécurité fonctionnelle, les plans de cycle de vie et de validation, et les rôles du propriétaire, des sous-traitants et des fournisseurs
- Évaluations et audits de sécurité fonctionnelle : ce que cherchent les évaluateurs, à chaque étape
- Gestion des compétences, activités de vérification et maîtrise documentaire
- Préparer votre système FSM à l'évaluation et à la certification du FSMS

Coaching sur projets réels

nous travaillons aux côtés de votre équipe sur vos propres projets

Nous aidons votre équipe à développer les compétences qu'exige IEC 61511, sur le travail qu'elle a devant elle. Aussi : T1, sécurité fonctionnelle et cybersécurité OT en un cours (3 jours ou 1 jour).

NOTRE MÉTHODE

Un chemin clair. Une prochaine étape concrète.

1 — Découvrir
Votre site, vos obligations et vos priorités

2 — Évaluer
Risques, écarts et maturité, sur site

3 — Planifier
Feuille de route priorisée selon vos arrêts

4 — Mettre en œuvre
Spécifier, piloter et traiter les écarts

5 — Vérifier et pérenniser
Tester, auditer, former et améliorer en continu

CONÇU POUR LES OPÉRATIONS CRITIQUES

- Infrastructures critiques
- Pétrole et gaz
- Pétrochimie
- Énergies renouvelables
- BESS
- Production d'électricité
- Transport d'électricité
- Distribution

OÙ NOUS INTERVENONS

Projets en **Europe et au Moyen-Orient**, dont des programmes NIS 2 multi-pays. Basés à Bruxelles, Belgique.

Langues de travail : anglais, français, espagnol.

COMPÉTENCES CERTIFIÉES

Membre du Comité technique ISASecure ACSSA

ISA/IEC 62443 Cybersecurity Expert (ISA) · ISASecure ACSSA for Evaluators Specialist · ISA Qualified Instructor · PECB ISO/IEC 27001 Senior Lead Implementer · PECB ISO/IEC 27001 Senior Lead Auditor · PECB NIS 2 Directive Senior Lead Implementer · PECB ISO 31000 Senior Lead Risk Manager · TÜV SÜD · RISKNOWLOGY Certified Competency

Sécurisons ensemble votre site.

Parlez-nous de votre site, de vos obligations et de votre prochain projet. Nous vous proposerons un périmètre clair et une première étape concrète.

information@ot-knight.com

Bruxelles, Belgique · Europe et Moyen-Orient

Dans l'OT et les infrastructures critiques, la cybersécurité devient une fonction de sécurité.