OT-Knight
An RBJCS brand

PORTFOLIO DIENSTEN EN OPLEIDINGEN



OT/ICS-CYBERSECURITY · FUNCTIONELE VEILIGHEID

In OT en kritieke infrastructuur wordt cybersecurity een veiligheidsfunctie.

Beschermen wat uw installatie draaiende houdt. Mensen, processen en technologie, van de eerste tekening tot de laatste ploegendienst, met één verantwoordelijke partner.

Concept en FEED	Gedetailleerd ontwerp	Bouw, FAT en SAT	Inbedrijfstelling	Bedrijfsvoering en onderhoud	Wijziging en vernieuwing

OT-cybersecuritybeheer als dienst · gedurende de hele levenscyclus

VOOR EXPLOITANTEN EN FABRIKANTEN IN

Kritieke infrastructuur · Olie en gas · Petrochemie · Hernieuwbare energie · BESS · Elektriciteitsproductie, -transmissie en -distributie

information@ot-knight.com
België · Europa · Midden-Oosten

DE UITDAGING

Uw installatie moet veilig, beveiligd, betrouwbaar en productief werken.

NIS 2 en de CRA maken de regelgeving strenger. Wij brengen OT-cybersecurity en functionele veiligheid samen in programma's die passen bij uw controlekamer, onderhoudsstops en veiligheidsdossier.

ONS ANTWOORD

Veiligheid is het vertrekpunt

IEC 62443 ontmoet IEC 61511 en ISA TR84.00.09. Cyberdreigingen voor uw veiligheidsfuncties horen thuis in hetzelfde gesprek als procesrisico's.

Governance die werkt in OT

IEC 62443 en ISO/IEC 27001 in één managementsysteem, opgebouwd rond de mensen die uw assets bedienen en onderhouden.

Ervaring achter het advies

Gecertificeerde competenties en echte praktijkervaring, met een zetel in het technisch comité van ISASecure ACSSA.

80+ jaar gecombineerde OT-praktijkervaring

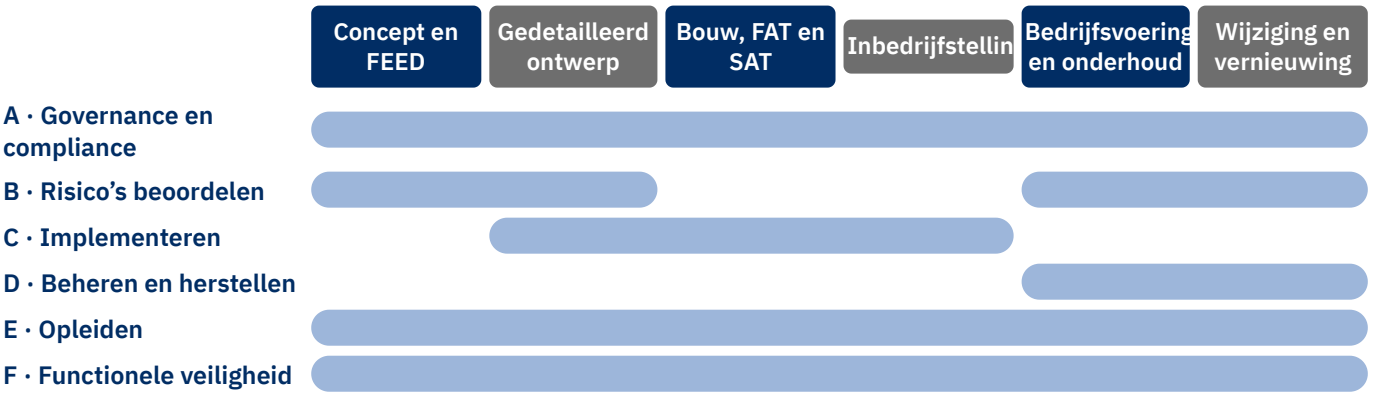
6 levenscyclusfasen, van FEED tot vernieuwing

6 dienstengroepen, één partner

ML1–3 ACSSA-certificeringstraject

Eén partner in elke fase van de levenscyclus

Waar elke dienstengroep bijdraagt



Mensen

Bewustwording, competentie en heldere rollen voor iedereen.

Processen

Governance, risicobeheer en procedures die werken op de site.

Technologie

Veilige architectuur, maatregelen en verificatie in reële omstandigheden.

A Governance en compliance

Eén managementsysteem voor IT en OT, en één compliance-aanpak in al uw landen.

A1

Geïntegreerd beveiligingsmanagementsysteem

IEC 62443 geïntegreerd met ISO/IEC 27001

Eén managementsysteem voor bedrijfs-IT en installatie-OT, opgebouwd vanuit OT zodat de maatregelen werken in de controlekamer.

U KRIJGT

- Gecombineerd managementsysteem, Verklaring van Toepasselijkheid (SPE's IEC 62443-2-1 + Annex A ISO/IEC 27001)
- OT-procedures voor operators en onderhoudsteams
- Klaar voor ISO/IEC 27001 en ISASecure ACSSA

A2

NIS 2 — België en Nederland

Compliance voor de hele site, inclusief OT, per land

Een groepsbaseline afgestemd op de nationale NIS 2-eisen. Wij ondersteunen de lokale toepassing van NIS 2 in elk rechtsgebied, waaronder België (CyFun®) en Nederland.

U KRIJGT

- Entiteitsclassificatie en scope per site en land
- Eén groepsbaseline voor de nationale NIS 2-eisen
- Bewijsvoering voor toezichthouders en incidentmelding

A3

Beveiligingsprogramma voor de levenscyclus

Voor SEVESO- of COMAH-entiteiten

Een Cybersecurity Management Plan afgestemd op IEC 62443 en de levenscyclus van functionele veiligheid (IEC 61511): wie doet wat bij elke gate.

U KRIJGT

- FS/CSMP met activiteiten per fase en gate
- Overdracht EPC–exploitatie en acceptatiecriteria
- KPI's, managementrapportage en MOC-integratie

A4

ISASecure ACSSA-certificering

Van ML1 tot ML3

ACSSA is de nieuwe ISA-certificering (ISASecure) voor asseteigenaren en exploitanten die IEC 62443 implementeren. Wij begeleiden u langs de hele roadmap, vanuit onze zetel in het ACSSA Technical Committee.

U KRIJGT

- Geschiktheid, scope en zone-indeling
- Gap-analyse volgens IEC 62443-2-1, -3-2, -2-4 en -3-3
- Proefbeoordeling en ondersteuning tot aan certificering

A5

Beveiliging van de toeleveringsketen

Eén norm voor elke leverancier

EPC's, integratoren, OEM's en dienstverleners met dezelfde securityeisen, van aanbesteding tot overdracht.

U KRIJGT

- IEC 62443-2-4-eisen in aanbestedingen en contracten
- Register van derden en leveranciersbeoordelingen
- CRA-conformiteitseisen voor wat u aankoopt

A6

EU Cyber Resilience Act

Voor fabrikanten en integratoren

Wij combineren de horizontale EN 40000, verticale normen en IEC 62443-4-1 / -4-2: één set bewijs voor alle.

U KRIJGT

- Productclassificatie en conformiteitsroute
- Productrisico's en veilige ontwikkelcyclus
- Kwetsbaarheidsbeheer, meldplicht, technisch dossier

B Risico's beoordelen en beheren

Ken uw risico's voordat u investeert: één gemeenschappelijke risicotaal, van directie tot controlekamer.

B1 Kader voor risicomanagement

Gebaseerd op ISO 31000, verbindt de organisatorische eisen van IEC 62443-2-1, de OT-risicoanalyse van IEC 62443-3-2 en ISO/IEC 27005, op uw HSE-matrix.

RESULTATEN · methodiek, criteria, register en behandelworkflow

B2 IEC 62443-3-2-risicobeoordelingen

System under consideration, zones en conduits, initiële en gedetailleerde analyse, en een beoogd securityniveau per zone.

RESULTATEN · zone- en conduitmodel, SL-T, risicorapport, CRS

B3 Cybersecurity en veiligheid

Cyberdreigingen voor uw SIS beoordeeld zoals IEC 61511 vereist, volgens ISA TR84.00.09, en verwerkt in HAZOP en LOPA.

RESULTATEN · cyberrisico's SIS, interface BPCS/SIS, input voor de SRS

B4 Gap-analyses

Uw positie tegenover IEC 62443, ISO/IEC 27001, de nationale NIS 2-eisen in België en Nederland, CRA of ACSSA.

RESULTATEN · gaprapport, volwassenheidsscore, stappenplan rond uw onderhoudsstops

C Implementeren en verifiëren

Verhelp tekortkomingen. Toon het resultaat aan.

C1 Eisen en specificaties

IEC 62443-3-3-eisen voor uw beoogde SL worden de ontwerpbasis voor alle leveringen van EPC's en leveranciers.

RESULTATEN · TRS (technische eisenspecificatie), segmentatie, remote access, herstel

C2 OT-cybersecuritybeheer als dienst

Wij zijn uw OT-cybersecurityfunctie gedurende de hele levenscyclus, van doelstellingen en projecten tot audits.

RESULTATEN · vaste verantwoordelijke, projectsturing, tools, ToR, audits, advies op afroep

C3 Projecten om tekortkomingen te verhelpen

Segmentatie, veilige IT/OT-interface, remote access, hardening, accounts, back-ups en monitoring: afgebakend, beheerd en afgesloten.

RESULTATEN · scope, leverancierskeuze, toezicht, afsluitbewijs

C4 Borging en verificatie

Veilig getest in draaiende installaties, door mensen die ze kennen: SL-verificatie, cyber-FAT/SAT, OT-assessments, OT-pentesten en audits.

RESULTATEN · testprotocollen, getuigenrapporten, SL-verificatie, bevindingen

OT-cybersecuritybeheer als dienst gedurende de hele levenscyclus

- Een vaste OT-verantwoordelijke naast u
- Cybersecurityprojecten aangestuurd
- OT-tools samen met u gekozen
- Interne en externe audits voorbereid
- Securitydoelstellingen bepaald en opgevolgd
- Tekortkomingen verholpen tot afronding
- Opdrachtomschrijvingen en aanbestedingsspecificaties
- Antwoord op ad-hocvragen

D Beheren en herstellen

Elke dag beveiligd. Voorbereid op moeilijke dagen.

D1 Beoordeling van de beveiligingsstatus

Hoe veilig is uw site zoals hij vandaag echt draait? Wij kijken verder dan documenten: architectuur, remote access, accounts, back-ups, media en dagelijkse praktijk.

RESULTATEN · score per SPE (62443-2-1) en FR (62443-3-3), toprisico's, 90-dagenplan

D2 OT-incidentrespons

Responsplannen en scenariodraaiboeken, afgestemd op de noodplannen voor de installatie en wettelijke meldplichten.

RESULTATEN · responsplan, playbooks, escalatiematrix, tabletop-oefeningen

D3 Continuïteit en herstel na calamiteiten

Herstel uw OT-systemen binnen vastgelegde doelen, met IEC 62443 AVAIL, ISO 22301, ISO/IEC 27031 en NIST-praktijken.

RESULTATEN · OT-BIA, RTO/RPO, herstelprocedures en -tests

D4 OT-monitoring, NDR, EDR en SOC

Wij bepalen wat uw NDR, EDR, monitoringtools en OT-SOC moeten leveren, kiezen de juiste aanbieder en sturen zijn prestaties, onafhankelijk van elke SOC-leverancier.

RESULTATEN · scope OT-SOC, KPI's, keuze van de aanbieder

E Opleiden en certificeren

Mensen vormen de eerste beheersmaatregel: wij bouwen de competentie achter elke maatregel op.

E1 Gecertificeerde ISA- en PECB-opleidingen

Certificerende ISA/IEC 62443-cursussen (IC32, IC33, IC34, IC37, IC49) en PECB-cursussen (NIS 2, ISO/IEC 27001, ISO 31000), gegeven door onze ISA Qualified Instructor en PECB Certified Trainer via onze erkende opleidingspartner, in-company of open.

E2 Bewustwording en competentie

Sessies op maat voor operators, technici, ingenieurs, aannemers en directies, inclusief NIS 2-opleiding voor bestuursorganen, vanuit echte praktijkervaring.



'Functionele veiligheid en cybersecurity zijn niet analoog: ze komen letterlijk samen in dezelfde controller.'

Daarom behandelt OT-Knight cybersecurity bij elke opdracht als onderdeel van uw veiligheidsdossier.

F Functionele veiligheid

Afgestemd op de veiligheidslevenscyclus van IEC 61511: veilig ontworpen, en veilig in bedrijf.

F1 Functional Safety Management en levenscyclusplanning

Wij bouwen en beheren het managementsysteem dat uw SIS zijn hele levensduur veilig houdt: een permanent systeem voor een site in bedrijf, of een plan voor functionele veiligheid binnen een investeringsproject. Klaar voor beoordeling, met een nette overdracht naar bedrijfsvoering.

- Planning van levenscyclus en validatie
- Competentiebeheer
- Management of change
- Rollen eigenaar, aannemers en leveranciers
- Verificatie- en FSA-planning
- Documentbeheer

F2 Functionele veiligheidsbeoordelingen

Onafhankelijke FSA's in elke levenscyclusfase, van gevaren- en risicoanalyse en de SRS tot inbedrijfstelling, bedrijfsvoering en wijzigingen, plus audits die nagaan of uw procedures worden gevolgd.

RESULTATEN · FSA-rapporten, functionele veiligheidsaudits, bevindingenregister

F3 Veiligheidseisenspecificatie

Wij schrijven of beoordelen de SRS voor elke veiligheidsinstrumentfunctie: veilige toestand, trippunten, responstijden, SIL-doel, overbruggings- en resetregels, proeftesteisen.

RESULTATEN · SRS, SIF-lijst, reviewopmerkingen

F4 SIL-verificatie

PFD, hardwarefouttolerantie, architectuurbeperkingen en systematische capaciteit getoetst aan elk SIL-doel: een onafhankelijke berekening die u in een beoordeling kunt verdedigen.

RESULTATEN · SIL-verificatierapport, aanbevelingen

F5 Ondersteuning bij bedrijfsvoering en onderhoud

Proeftestprocedures en intervaloptimalisatie, opvolging van demands en falen, beheer van overbruggingen en review van SIS-wijzigingen zodra het SIS in bedrijf is.

RESULTATEN · proeftestprocedures, SIS-prestatiereviews, MoC-reviews

F6 Certificeer uw FSMS

Wij begeleiden u bij de keuze van de certificatie-instelling en door het hele proces. Wij hebben een managementsysteem voor functionele veiligheid naar exida-certificering geleid en kennen de weg uit eigen ervaring.

+ Waar safety en security samenkomen

Een SIS vraagt een eigen security-risicobeoordeling volgens IEC 61511. Wij voeren die uit naast ons functionele-veiligheidswerk (zie B3) en trainen uw teams in beide (pagina's 7–9).

Met u over de hele IEC 61511-veiligheidslevenscyclus

Van gevarenanalyse tot ontmanteling

Gevaren- en risicoanalyse	SIL-toewijzing en SRS	Ontwerp en engineering	Installatie, FAT en validatie	Bedrijfsvoering en onderhoud	Wijziging en ontmanteling

Opleidingsportfolio

Kennis die terugkeert naar de installatie.

Acht specialistische programma's, afgestemd op uw team, assets en volwassenheid. Inhoud, diepgang en oefeningen kunnen worden afgestemd op uw team en de toepasselijke regelgeving: workshops op locatie, meerdaagse opleidingen en managementbriefings, in het Engels, Frans of Spaans.

EENDAAGS FORMAT T1 en T2 kunnen een eendaagse workshop ter plaatse worden, met een beknopte praktijkoefening. Duur is indicatief.

GECERTIFICEERDE LEERTRAJECTEN Erkende ISA- en PECB-opleidingen · via onze erkende opleidingspartner

- **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** Cursussen NIS 2, ISO/IEC 27001, ISO 31000

T1 Veiligheid en beveiliging vanaf het ontwerp

3 DAGEN · OPTIE 1 DAG

IEC 61511 · IEC 62443 · ISO/IEC 27001 · ISA-TR84.00.09-2024 · ISASecure ACSSA, voor asseteigenaren

- Waar beide levenscycli samenkomen: cyberrisicoanalyse IEC 61511 (8.2.4), cybereisen voor het SIS en impact op de SRS
- Gecombineerde governance: MoC, competentie, audits en proof testing naast securityverificatie
- Workshop: gecombineerde safety/security case voor één procesunit
- ISA-TR84.00.09-2024 in de praktijk: cyber als oorzaak van verlies van beschermingslagen, en SIS/BPCS-onafhankelijkheid in het zone-ontwerp
- Een draaiende site voorbereiden op ISASecure ACSSA

T2 Basiskennis IEC 62443: de taal van industriële cybersecurity

1 DAG

Basiskennis · Rollen · Normenoverzicht

- Opbouw van de reeks en wie welk deel bezit: asseteigenaren, dienstverlener, integrator, productleverancier
- De roadmap: 2-1 (programma), 3-2 (risico), 3-3 (systeem) en 4-1/4-2 (product)
- ISASecure-schema's (CSA, SSA, SDLA, ACSSA)
- Kernbegrippen: programma-elementen, zones en conduits, SL-T, SL-C en SL-A, Foundational Requirements FR 1–7, defence in depth
- Relatie met ISO/IEC 27001 en NIST CSF 2.0

T3 Uw IEC 62443-beveiligingsprogramma opbouwen

3 DAGEN

Voor asseteigenaren en exploitanten

- IEC 62443-2-1:2024 en de 8 SPE's: ORG, CM, NET, COMP, DATA, USER, EVENT, AVAIL
- Governance, rollen, beleid en procedures die operations echt gebruikt
- KPI's en continue verbetering
- Gap-analyse, maturiteitsniveaus en geprioriteerde roadmaps
- Dienstverleners beheren met IEC 62443-2-4

T4 Cyberrisico's die ertoe doen: OT-cyberrisicomanagement

3 DAGEN

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

- ISO 31000 als overkoepelend kader, ISO/IEC 27005 voor informatierisico's en IEC 62443-3-2 voor het IACS
- Analyse vanuit gevolgen: koppeling met HAZOP en LOPA, kalibratie op de risicomatrix
- ZCR 1 tot ZCR 7: System under Consideration (SuC), initiële en gedetailleerde analyse, zones en conduits, SL-T en eisenspecificatie (CRS)
- Praktijkcase, van SuC tot CRS

T5 Eén ISMS, twee werelden: IEC 62443 en ISO/IEC 27001 samenbrengen

2 DAGEN

ISMS · Koppeling van beheersmaatregelen · Auditprogramma's

- Een ISMS uitbreiden van IT naar OT zonder iets te breken
- Scope, Verklaring van Toepasselijkheid (SoA) en risicobehandeling OT
- Annex A-maatregelen van ISO/IEC 27001 naast de eisen van IEC 62443-2-1 en de SR's van 62443-3-3
- Eén auditprogramma voor beide certificeringen

T6 Beveiligd van specificatie tot site

3 DAGEN

Voor EPC's, integratoren, leveranciers en projectteams van de asseteigenaren

- Capaciteiten van de dienstverlener volgens IEC 62443-2-4 voor integratie en onderhoud
- Veilige ontwikkeling IEC 62443-4-1 (SM, SR, SD, SI, SVV, DM, SUM, SG) en hoe componenteisen 4-2 doorwerken in systeemcapaciteiten 3-3
- Cybersecurity in elke fase: FEED, detailontwerp, FAT, SAT, overdracht, bedrijf en onderhoud
- Deliverables en contracteisen: CRS, zone- en conduittekeningen, hardening-baselines, gebruikersdocumentatie

T7 Vertrouw, maar verifieer: borging van OT-cybersecurity, van risicobeoordeling tot buitenbedrijfstelling

2-3 DAGEN

Audits · Verificatie · Veilige beveiligingstests

- Assuranceplan over de hele levenscyclus: wat, wanneer, hoe en met welke onafhankelijkheid verifiëren
- Veilig testen in OT: securitytests in FAT/SAT, kwetsbaarheidsanalyse, scope van pentesten in draaiende installaties
- OT-assets veilig uit dienst nemen: data wissen, credentials intrekken, wijziging beheren
- Securityprogramma's auditen volgens IEC 62443-2-1 en 2-4, en SL-A tegenover SL-T verifiëren (3-3)
- Bewijs, bevindingen en rapporten zoals ISASecure-evaluatoren werken

T8 Praktische hardening en tests voor ICS-omgevingen

2 DAGEN | PRAKTIJKOEFENINGEN

Samen verzorgd met een specialist in OT-penetratietests · beginner tot gevorderd

- Een praktisch, OS-onafhankelijk hardeningproces: waarom, wanneer, hoe en wat, en de link met IEC 62443
- Eigen hardeningscripts en systeembeleid, plus netwerk-, fysieke en gebruikershardening
- Hardening van Windows-HMI's en -servers, Linux, netwerkapparatuur en PLC's, standalone of in een domein, met afgeschermde operatoromgevingen
- Hardening verifiëren met gangbare tools, in labs gebaseerd op echte installaties

F

Opleiding functionele veiligheid

IEC 61511-competentie van controlekamer tot projectkantoor, afgestemd op uw installatie en procedures.

Alle opleidingen functionele veiligheid worden gegeven in het Engels, Frans en Spaans.

T9 Bewustwording functionele veiligheid: waarom het SIS ertoe doet

HALVE DAG TOT 1 DAG

Voor operators, onderhoudsteams, aannemers en managers

- Wat een veiligheidsinstrumentsysteem doet en hoe het verschilt van het controlesysteem
- Waarom overbruggingen, overrides en niet-beoordeelde wijzigingen de beveiliging in gevaar brengen
- De IEC 61511-veiligheidslevenscyclus in gewone woorden, en wie elke stap beheert
- Wat elke rol moet doen, en nooit mag doen, rond een SIF

T10 IEC 61511 in de praktijk: van gevarenanalyse tot de SRS

3 DAGEN

Voor ingenieurs, procesveiligheidsspecialisten en projectteams

- De veiligheidslevenscyclus en hoe de fasen aansluiten: gevaren- en risicoanalyse, toewijzing, SRS, ontwerp, validatie, bedrijfsvoering
- De SRS opstellen: veilige toestand, trippunten, responstijden, overbruggings- en resetregels, proeftesteisen
- Het SIL-doel bepalen met HAZOP en LOPA, en afstemmen op de risicomatrix van het bedrijf
- Workshop: van een gevarenscenario tot een volledige SRS voor één SIF

T11 SIL-verificatie: aantonen dat het ontwerp zijn doel haalt

2 DAGEN

Voor SIS-ontwerpingenieurs, EPC's en leveranciers

- PFD-berekening voor typische architecturen, en de data en aannames erachter
- Het proeftestinterval bepalen en vastleggen waarvan het resultaat afhangt
- Hardwarefouttolerantie, architectuurbeperkingen en systematische capaciteit
- Workshop: één SIF verifiëren en het resultaat verdedigen in een beoordeling

T12 Het SIS in bedrijf houden: proeftesten, overbruggingen en management of change

2 DAGEN

Voor teams bedrijfsvoering, onderhoud en engineering

- Proeftestprocedures opstellen en uitvoeren, en testintervallen optimaliseren
- Demands en falen opvolgen, en de data gebruiken om de ontwerpaannames te toetsen
- Beheer van overbruggingen en de operationele regels in de SRS
- SIS-wijzigingen beoordelen binnen management of change

T13 Functional Safety Management: het FSM-systeem laten draaien

2 DAGEN

Voor managers, verantwoordelijken functionele veiligheid en projecteigenaren

- Het plan voor functionele veiligheid, de levenscyclus- en validatieplannen, en de rollen van eigenaar, aannemers en leveranciers
- Beoordelingen en audits functionele veiligheid: waar beoordelaars op letten, in elke fase
- Competentiebeheer, verificatieactiviteiten en documentbeheer
- Uw FSM-systeem voorbereiden op beoordeling en op FSMS-certificering

Coaching op echte projecten

wij werken samen met uw team aan uw eigen projecten

Wij helpen uw team de competentie op te bouwen die IEC 61511 vereist, op het werk dat voorligt. Ook: T1, functionele veiligheid en OT-cybersecurity in één cursus (3 dagen of een workshop van één dag).

ONZE AANPAK

Een duidelijk traject. Een praktische volgende stap.

1 **Ontdekken**
Uw installatie, verplichtingen en prioriteiten

2 **Beoordelen**
Risico's, tekortkomingen en maturiteit, ter plaatse

3 **Plannen**
Geprioriteerd stappenplan rond uw onderhoudsstops

4 **Implementeren**
Specificeren, sturen en tekortkomingen verhelpen

5 **Verifiëren en borgen**
Testen, auditen, opleiden en blijven verbeteren

VOOR KRITIEKE BEDRIJFSVOERING

- Kritieke infrastructuur
- Olie en gas
- Petrochemie
- Hernieuwbare energie
- BESS
- Elektriciteitsopwekking
- Transmissie
- Distributie

WAAR WIJ WERKEN

Projecten in **Europa en het Midden-Oosten**, waaronder NIS 2-programma's in meerdere landen. Gevestigd in Brussel, België.

Werktalen: Engels, Frans, Spaans.

GECERTIFICEERDE COMPETENTIE

Lid van het ISASecure ACSSA Technical Committee

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

Samen uw installatie beveiligen.

Vertel ons over uw installatie, uw verplichtingen en uw volgende project. Wij reageren met een duidelijke scope en een praktische eerste stap.

information@ot-knight.com

Brussel, België · Europa en Midden-Oosten

In OT en kritieke infrastructuur wordt cybersecurity een veiligheidsfunctie.