Beknopte handleiding voor machinebouwers

Echt of nep: hoe herken je een geldig cybersecuritycertificaat?

Waarom het belangrijk is om het verschil te kennen

In de huidige industriële omgeving is cybersecurity niet langer een concurrentievoordeel, maar een vereiste vanuit de markt en regelgeving. Toch zijn niet alle documenten die op een certificaat lijken ook daadwerkelijk officiële certificeringen. Het verschil begrijpen helpt je om betrouwbare leveranciers te kiezen en technische, juridische en reputatierisico's te vermijden.

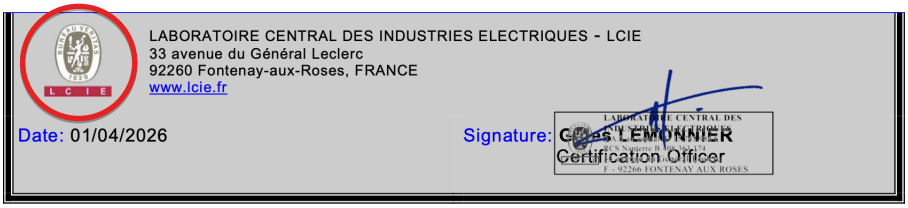
Algemene certificeringen zoals ISO 27001 hebben betrekking op de organisatie van een bedrijf, maar bieden geen garantie dat een specifiek product beschermd is tegen cyberaanvallen. Daarom is een **specifieke productcertificering (IEC 62443-4-2)** vereist.

Ga er dus niet automatisch van uit dat een product veilig is omdat een leverancier ISO 27001 gecertificeerd is. Controleer altijd of het betreffende component beschikt over een **specifieke IEC 62443 certificering.**

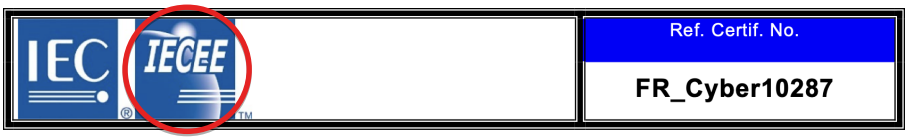
Wat is een officiële certificering?

Kijk bijvoorbeeld naar het **IEC 62443-4-2 certificaat** van de SecureEdge gateways van IXON. Hieraan zijn de kenmerken van een officiële industriële cybersecuritycertificering goed te herkennen:

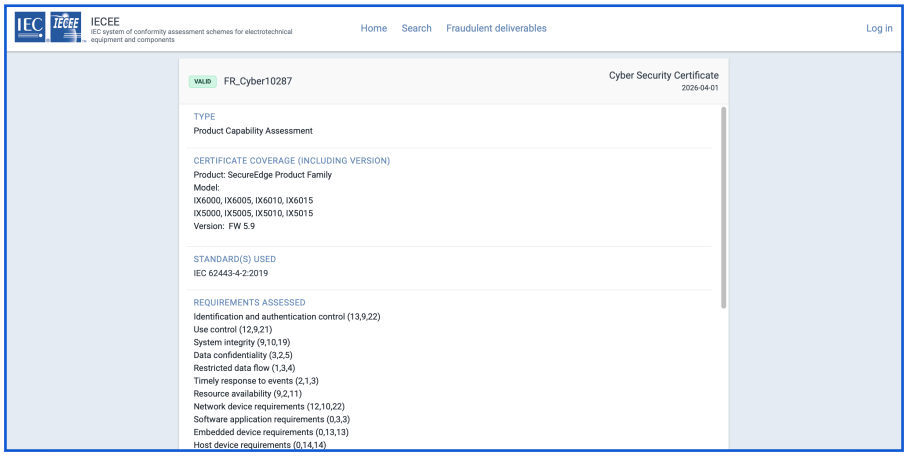
- Het certificaat wordt afgegeven door een geaccrediteerde, onafhankelijke certificeringsinstantie (zoals Bureau Veritas, TÜV of UL):



- Het certificaat is gebaseerd op een officiële internationale standaard, zoals beheerd door de **IECEE** (IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components):



- Het certificaat is openbaar te verifiëren via internationale databases:



- **Daarnaast vermeldt het certificaat duidelijk:**
  Welke standaard gecertificeerd is (bijvoorbeeld een specifiek onderdeel van de standaard) en welk Security Level of Maturity Level is behaald, afhankelijk van het type certificering:

Standard	IEC 62443-4-2:2019
Requirements Assessed *The 3-tuple represents (Passed requirements, requirements assessed as Not Applicable, Total number of requirements)*	Identification and authentication control (13,9,22) Use control (12,9,21) System integrity (9,10,19) Data confidentiality (3,2,5) Restricted data flow (1,3,4) Timely response to events (2,1,3) Resource availability (9,2,11) Network device requirements (12,10,22) Software application requirements (0,3,3) Embedded device requirements (0,13,13) Host device requirements (0,14,14) Security Level: SL2

- Op welk product of component de certificering van toepassing is:

Certificate Coverage (including Version)	Product: SecureEdge Product Family Model: IX6000, IX6005, IX6010, IX6015 IX5000, IX5005, IX5010, IX5015 Version: FW 5.9

Denk hierbij aan een rijbewijs:
Een ‘verklaring’ is te vergelijken met een vriend die zegt dat je goed kunt autorijden
Een ‘certificering’ is het officiële document dat een bevoegde instantie afgeeft na het succesvol afronden van je examen.

Waarschuwingssignalen van ‘zelfverklaringen’

Een conformiteitsverklaring of niet-geaccrediteerde verklaring:

- Kan afkomstig zijn van adviesbureaus of onbevoegde derde partijen.
- Bevat geen erkende onafhankelijke audits.
- Vermeldt vaak meerdere standaarden (zoals NIST, BSI of OWASP) zonder daadwerkelijke certificering.
- Kan niet worden gecontroleerd via officiële registers.

Kortom: het gaat om een verklaring, niet om aantoonbaar bewijs.

Hoe controleer je snel een leverancier?

Wanneer een leverancier aangeeft gecertificeerd te zijn, vraag dan altijd om de volgende gegevens. Deze gegevens staan bijvoorbeeld vermeld in IXON’s **IEC 62443-4-1** certificaat voor veilige softwareontwikkeling:

- Het officiële certificaatnummer:

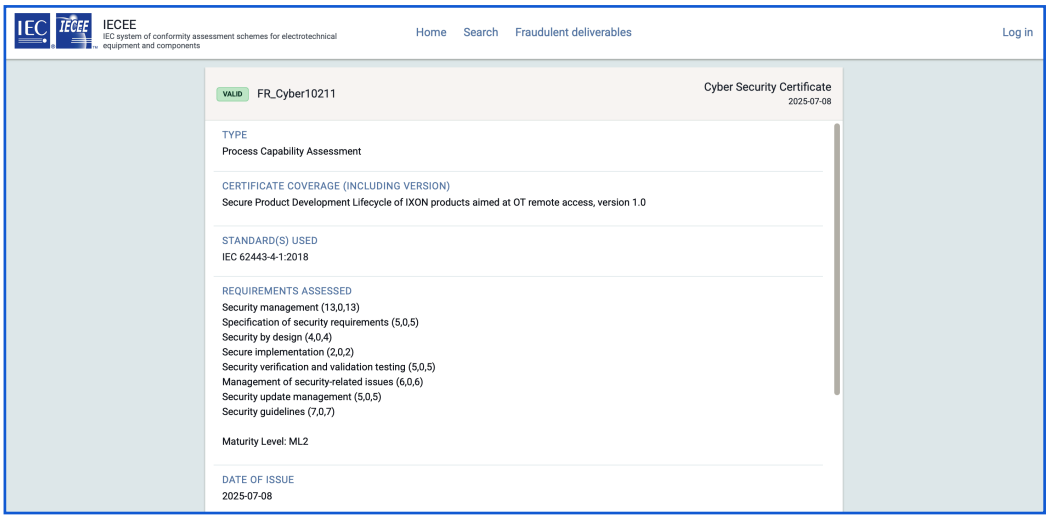
- De naam van de certificerende instantie:

- De norm en het behaalde Security Level of Maturity Level (afhankelijk van het type certificering):

Standard	IEC 62443-4-1:2018
Requirements Assessed *The 3-tuple represents (Passed requirements, requirements assessed as Not Applicable, Total number of requirements)*	Security management (13,0,13) Specification of security requirements (5,0,5) Security by design (4,0,4) Secure implementation (2,0,2) Security verification and validation testing (5,0,5) Management of security-related issues (6,0,6) Security update management (5,0,5) Security guidelines (7,0,7) Maturity Level: ML2

- Verificatie via internationale databases zoals: **certificates.iecee.org**

Voorbeeld:



Kan een leverancier deze informatie niet verstrekken, of ontbreekt een directe link naar het certificaat in het register, dan gaat het waarschijnlijk niet om een officiële certificering.

Hoe IXON machinebouwers ondersteunt

Een officiële certificering toont aan dat onafhankelijke derde partijen de conformiteit hebben gecontroleerd. De SecureEdge gateways van IXON behoren tot de eerste IEC 62443-4-2 gecertificeerde edge gateways ter wereld. Het gebruik van gecertificeerde industriële componenten vereenvoudigt bovendien het certificeringsproces volgens **IEC 62443-3-3** voor machines, iets waar eindklanten in de industrie steeds vaker om vragen.

Nieuwe Europese regelgeving verwijst bovendien steeds vaker naar IEC-eisen. Door gebruik te maken van componenten die al IEC-gecertificeerd zijn, kan sneller worden aangetoond dat wordt voldaan aan verplichtingen uit NIS2, de Cyber Resilience Act (CRA) en de nieuwe Machineverordening (EU) 2023/1230.

Meer weten over de certificeringen en producten van IXON?

Bekijk ons Trust Center of neem contact op met de accountmanager.

trust.ixon.cloud ›

IXON