Guida rapida per costruttori di macchine

Vero o falso: come riconoscere un certificato di cybersecurity valido

Perché è importante capire la differenza

Nel panorama industriale attuale, la cybersecurity non è più un valore aggiunto, ma un requisito di mercato e normativo. Tuttavia, non tutti i documenti che sembrano certificazioni lo sono realmente. Comprendere la differenza aiuta a scegliere fornitori affidabili ed evitare rischi tecnici, legali e reputazionali.

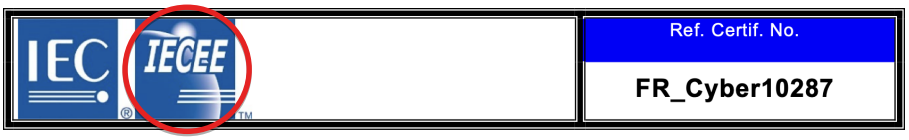
Certificazioni generali come ISO 27001 certificano l'organizzazione aziendale, ma non attestano che un prodotto specifico sia sicuro contro gli attacchi informatici. Per questo serve una **certificazione di prodotto specifica (IEC 62443-4-2).** Non bisogna quindi presumere che l'hardware sia sicuro solo perché il fornitore possiede la certificazione ISO 27001. Verificate sempre la **certificazione IEC 62443 specifica del componente.**

Che cos'è una vera certificazione

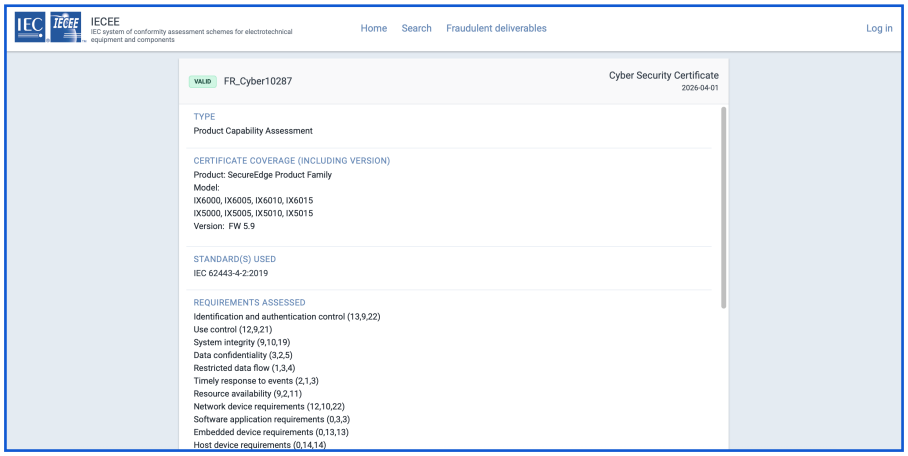
Osservando il nostro **certificato IEC 62443-4-2**, è possibile riconoscere le caratteristiche di una certificazione autentica di cybersecurity industriale:

- È rilasciata da un organismo di certificazione indipendente accreditato (ad esempio Bureau Veritas, TÜV o UL):

- Segue uno schema internazionale ufficiale, come quello gestito da **IECEE** (IEC system of conformity assessment schemes for electrotechnical equipment and components):



- Può essere verificata pubblicamente attraverso database globali:



- **Indica chiaramente:**
  lo standard certificato (ad esempio una parte specifica della norma) e il Security Level o Maturity Level raggiunto, in base al tipo di certificazione:

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

- Il prodotto o componente coperto dalla certificazione:

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

Pensiamo a una patente di guida. Una "Dichiarazione" è semplicemente un amico che dice che guidi bene. Una "Certificazione" è il documento ufficiale rilasciato dall'autorità competente dopo aver superato l'esame.

I segnali di allarme delle “autodichiarazioni”

Una dichiarazione di conformità o una dichiarazione non accreditata:

- Può essere emessa da società di consulenza o terze parti non autorizzate;
- Non prevede audit indipendenti riconosciuti;
- Spesso elenca numerosi standard (ad esempio NIST, BSI, OWASP) senza certificare realmente nessuno di essi;
- Non può essere verificata in registri ufficiali.

In breve: è una dichiarazione, non una prova.

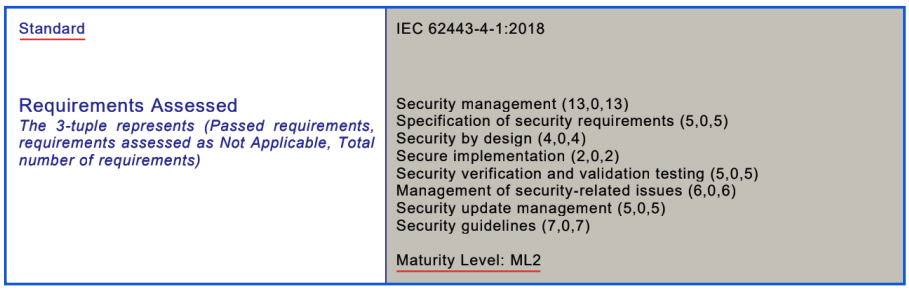
Come verificare rapidamente un fornitore

Quando un fornitore afferma di essere certificato, chiedere sempre i seguenti elementi, riscontrabili ad esempio nel nostro certificato **IEC 62443-4-1** sullo sviluppo sicuro del software:

- Numero ufficiale del certificato:

- Organismo che ha rilasciato la certificazione:

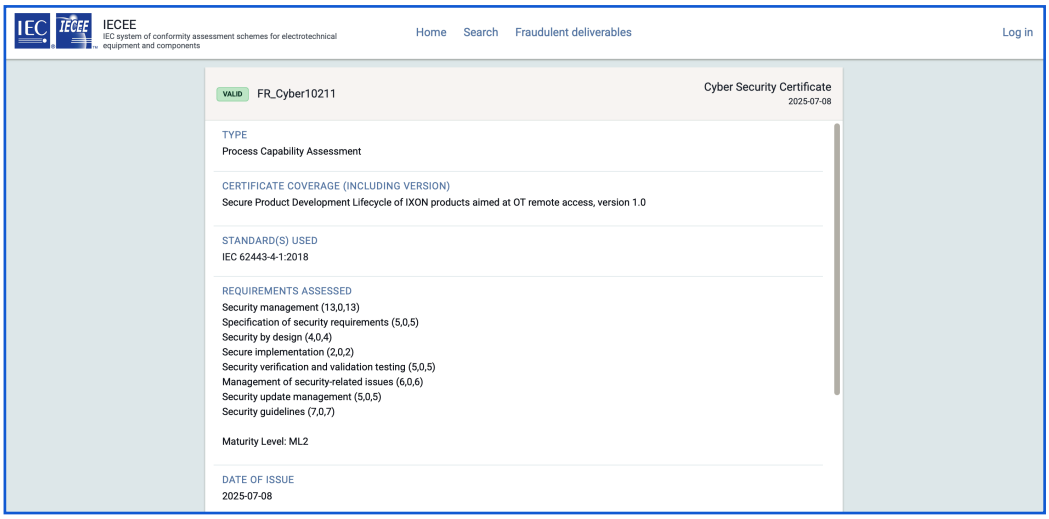
- Standard e Security Level o Maturity Level raggiunto (a seconda della certificazione):



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

- Il certificato puo essere verificato pubblicamente attraverso database globali: **certificates.iecee.org**

Esempio:



Se non sono in grado di fornire queste informazioni, o un link diretto al certificato nel registro, probabilmente non si tratta di una vera certificazione.

IXON è al fianco dei costruttori di macchine

Una certificazione reale dimostra la conformità verificata da terze parti indipendenti. Utilizzare componenti industriali certificati facilita il processo di certificazione **IEC 62443-3-3** relativa alla macchina, sempre più richiesta dai clienti finali del settore industriale.

Infatti, le nuove normative europee fanno sempre più riferimento ai requisiti IEC. Utilizzando componenti già certificati IEC, è possibile dimostrare più rapidamente la conformità agli obblighi previsti dalla NIS2, dal Cyber Resilience Act (CRA) e dal nuovo Regolamento Macchine (UE) 2023/1230.

Per saperne di più sulle certificazioni e sui prodotti IXON

È possibile visitare il nostro Trust Center o contattare l'account manager di riferimento.

trust.ixon.cloud ›

IXON