

Rassegna ALIMENTARE

PACKAGING
BEVANDE

Novità e panorama dei fornitori
di macchine, impianti, prodotti e
attrezzature per l'industria alimentare



Let CodeMeter inspire you with new license-driven business models

- Protect your digital assets from piracy and reverse engineering
- Secure the integrity of your endpoints from tampering
- Implement license-based readily adaptable business models

Customer centric approach

From the cloud down to FPGAs

Digital global marketplace

Software, firmware, and sensitive data

Brown field and green field



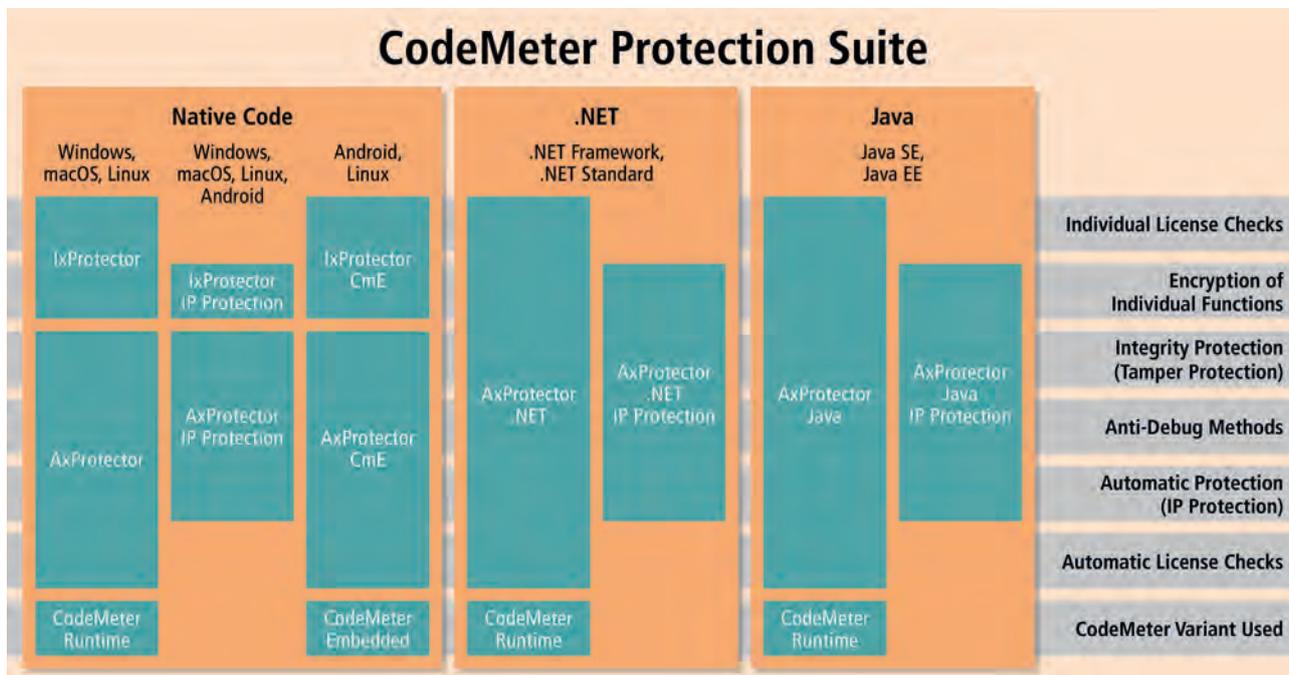
Don't wait any longer
Start protecting your IP now!
s.wibu.com/sdk-cm

+49 721 931720
sales@wibu.com
www.wibu.com



SECURITY
LICENSING
PERFECTION IN PROTECTION

CYBERSICUREZZA IIOT come raggiungere la maturita'

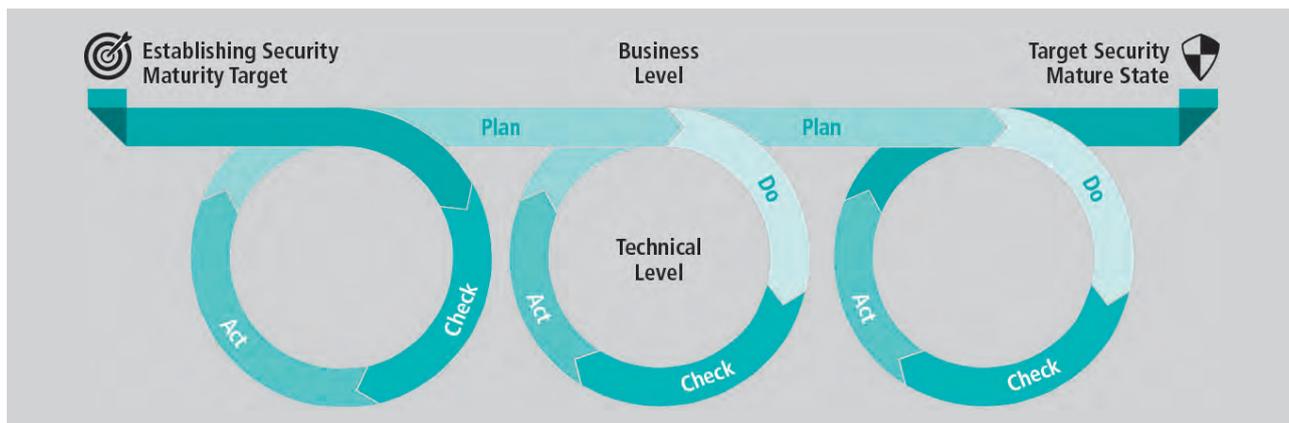


Gli ICS (Industrial Control Systems), che gestiscono e monitorano i moderni impianti di produzione e la loro evoluzione verso dispositivi intelligenti in rete, sia su base cloud che su base locale, costituiscono il fondamento per i progressi compiuti in ambito Industria 4.0. I rischi più significativi in termini di cybersicurezza di questa nuova classe di sistemi IIoT includono minacce alla sicurezza di dati e reti, alla stabilità delle infrastrutture critiche nazionali e all'integrità

delle catene di fornitura. Molti sono ormai gli approcci e gli standard di riferimento per valutare lo stato dell'arte in materia di cybersecurity, tanti dei quali partono però direttamente dal fronteggiare specifici problemi strutturali e tecnici, senza prima porre l'accento su un'analisi omnicomprensiva.

Il Security Maturity Model (SMM) creato dall'Industrial Internet Consortium (IIC), e ancora oggetto di ulteriore espansione, vuole invece coinvolgere tutti gli

stakeholder aziendali e i fornitori cui l'impresa si sia affidata, per effettuare una valutazione di merito in fatto di governance, enablement e hardening, ovvero di policies e strategie attive all'interno dell'organizzazione, attenzione alla security by design e alla sua implementazione, monitoraggio e risposte ad eventuali vulnerabilità. Tanto più è estesa questa prima fase, quanto più accurati saranno gli obiettivi che si andranno a delineare e certa la loro risoluzione.



16-17 Giugno 2021
Amburgo, Germania

La stima terrà conto non solo delle linee guida fornite dall'IIC, ma anche degli scenari del settore industriale di appartenenza e dei possibili profili legati a specificità inerenti a dispositivi e sistemi. Una volta completata l'indagine ed individuate le aree da potenziare attraverso una mappatura di indicatori di successo, azioni tangibili e best practices, l'analisi del divario tra stato attuale e stato verso il quale si è concordato di traghettare l'azienda permetterà di stabilire le priorità e raggiungere risultati effettivi.

Solo allora ci si può rivolgere a standard accreditati, come quelli NIST, ISO/IEC, ISA, cui si farà riferimento per sanare le vulnerabilità tecniche rilevate. Il processo dovrà poi essere ripetuto ciclicamente, al fine di verificare la validità delle misure correnti a fronte di tecnologie sempre in evoluzione e della costante crescita di nuove minacce.

Wibu-Systems, membro da anni dell'IIC e co-autore dell'Industrial Internet Security Framework (IISF), entra in gioco in questo secondo stadio, offrendo una serie di soluzioni di hardening sotto il nome di CodeMeter, che vanno da un accesso sicuro a piattaforme progettuali condivise, ad elementi hardware sicuri integrabili anche all'interno dei dispositivi embedded, ed ancora a suite di protezione del software, del firmware e dei dati sensibili da contraffazione, reverse engineering e manomissioni. La sicurezza di macchine ed impianti manifatturieri si estende agli strumenti di controllo e di sviluppo, all'hardware, agli ambienti di runtime e ai sistemi operativi, ai linguaggi di programmazione e alle applicazioni. L'adozione di un'opportuna tecnologia di protezione, basata sui più moderni metodi crittografici, previene il trasferimento illecito di know-how digitale alla concorrenza o anche solo al personale interno non autorizzato, e così pure la pirateria di progetto e di prodotto, aiutando le aziende a mantenere salda la quota di mercato e alta la loro reputazione. Anche gli operatori e gli utenti delle macchine ne traggono vantaggio: la salvaguardia dell'integrità dei beni digitali impedisce sabotaggi e manipolazioni accidentali o intenzionali. Il sistema può essere anche utilizzato per garantire ai clienti un'aderenza dei cicli produttivi a quanto da loro stessi ordinato e dunque una protezione contro un'illecita produzione di lotti sotto banco.

La tecnologia CodeMeter trasforma quindi strumenti di controllo, monitoraggio e restrizioni d'uso in versatilità, flessibilità e libertà per produttori di software e dispositivi intelligenti, i loro utenti e la società tutta. 🏛️

www.wibu.com

Fai crescere la tua impresa

alla fiera mondiale
per snack salati

**L'unico evento al 100% dedicato
agli snack salati e alla frutta secca**

- + Scopri le tendenze, i gusti e le tecnologie più in voga
- + Sviluppa la tua attività con i principali fornitori del settore
- + Entra in contatto con i maggiori attori del settore e trova partner commerciali internazionali e distributori
- + Incontra clienti esistenti e nuove prospettive da tutto il mondo
- + Vendi i tuoi prodotti ad un pubblico pronto per l'acquisto

**La fiera di riferimento per
il settore degli snack salati**

