



Riferimenti

d.marostica@confindustriaemilia.it

[Brand ed Eventi](#)

Martedì, 5 dicembre 2023 - 16,00

"Associati per Associati": incontro "Garantire la continuità operativa nelle reti industriali. Fai in modo che i sistemi industriali garantiscano la produzione senza interruzioni"

Gli ambienti OT (**Operational Technology**) stanno cambiando con l'introduzione di nuove tecnologie e si deve tener conto delle sfide e dei rischi unici associati alle reti IoT industriali.

Le organizzazioni devono incorporare la sicurezza informatica nella strategia aziendale; occorre modellare atteggiamenti, azioni e responsabilità necessari per migliorare la protezione delle proprie reti IoT dagli attacchi, per ridurre così il rischio di interruzione dei processi produttivi e per mantenere la business continuity.

Uffici Interessati: Amministrazione, Direzione e gestione strategica, ICT, Personale e risorse umane, Produzione, Qualità, Ricerca e sviluppo, Sicurezza e ambiente

Argomenti: COMUNICAZIONE, Comunicazione - Varie

EVENTO PUBBLICO

Dove:

Webinar Zoom - [-](#)

[salva nel tuo calendario l'evento presso Webinar Zoom](#)

GARANTIRE LA CONTINUITÀ OPERATIVA NELLE RETI INDUSTRIALI

Fai in modo che i sistemi industriali garantiscano la produzione senza interruzioni



5 Dicembre
2023



Webinar



16.00 – 17.30

Gli ambienti di **Operational Technology** stanno cambiando con l'introduzione di nuove tecnologie nelle reti **IoT industriali** che controllano e monitorano i processi industriali. La digitalizzazione degli ambienti di produzione rende i sistemi industriali **vulnerabili agli attacchi informatici**. Il webinar percorrerà in dettaglio le **strategie per approcciare la sicurezza industriale** descritte nello standard per la sicurezza industriale **ISA/IEC 62443** con l'obiettivo di **mantenere la continuità aziendale** in ogni condizione operativa, anche durante un **evento di compromissione informatica**.

Interventi di:

Prof. **Franco Callegati**, Professore Ordinario Università di Bologna
◦ *Il ruolo della sicurezza nella continuità operativa di fabbrica*

Ing. **Luca Simoncini**, IT Governance, Cyber Risk Mitigation, Digital Transformation, Marposs s.p.a.
◦ *Le sfide di gestire e proteggere l'infrastruttura IT di fabbrica*

Ing. **Aldo Campi**, CEO di Stoorm5 s.r.l.
◦ *Mettere in pratica la sicurezza dei sistemi industriali*

La partecipazione all'incontro è gratuita, previa
iscrizione da effettuarsi [a questo link](#).

stoorm5

Le tecnologie operative (OT) che controllano e monitorano i processi industriali, sono vulnerabili agli attacchi informatici che sfruttano una varietà di fattori, inclusi bug del software, difetti hardware ed errori di configurazione. Gli attacchi informatici possono interrompere la produzione continua disabilitando i sistemi e corrompendo dispositivi OT, possono rubare i dati relativi a progetti e a segreti di produzione.

Mantenere la continuità operativa è l'obiettivo delle Operation Technology, la sicurezza informatica va quindi pensata per renderla gestibile dal personale delle Operations con il supporto dal team IT.

La normativa **ISA/IEC 62443** è lo standard internazionale di riferimento per la cybersicurezza industriale e fornisce un quadro completo che consente alle organizzazioni aziendali di identificare, valutare e gestire i rischi di sicurezza informatica per i propri ambienti OT.

La IEC 62443 definisce le **strategie per permettere alle aziende di mantenere la produzione costante**, senza interruzioni. Ciò è essenziale in molti settori industriali quali per esempio Industrie manifatturiere Sanità e ospitalità, Smart Cities, Trasporti e Logistica, Gestione energia, Vendita al dettaglio e magazzini, rete Finanziaria, Aerospaziale e Difesa.

Il webinar percorrerà in dettaglio le **strategie per approcciare la sicurezza industriale** con l'obiettivo di **mantenere la continuità aziendale in ogni condizione operativa**, anche durante un evento di compromissione informatica.

La partecipazione all'incontro è gratuita. Per iscriversi cliccare qui: [ISCRIVITI ORA](#)

 [Scarica il programma dell'incontro \(471.51 KB\).](#)