WEBINAR

Sicurezza in ambito A.I.

Comprendi le implicazioni di sicurezza nell'uso dell' Intelligenza Artificiale

13 NOVEMBRE
2025

EDU TIPS
CYBERSECURITY

EDU TIPS | smeup

Sicurezza informatica,
il percorso formativo per rafforzare la tua sicurezza aziendale.

Le minacce digitali sono in continua evoluzione e affrontarle con consapevolezza è fondamentale.

Smeup ti invita a seguire un **percorso formativo gratuito** composto da **10 webinar di 30 minuti** , pensati per guidarti con soluzioni pratiche e strategie concrete nella **sicurezza aziendale** .

EDU TIPS Cybersecurity

10 webinar TIPS - 30 minuti al mese
su tematiche specifiche di Cybersecurity

DATA	DESCRIZIONE
28/1	Mese 1: **Sicurezza dell'infrastruttura**
13/2	Mese 2: **Cyber Security Awareness**
13/3	Mese 3: **Data Protection**
10/4	Mese 4: **Identità e accesso**
13/5	Mese 5: **Cloud security**
12/6	Mese 6: **Incident response**
8/7	Mese 7: **Sicurezza delle applicazioni**
11/9	Mese 8: **Analisi delle minacce e vulnerability assessment**
10/10	**Mese 9: Sicurezza delle reti industriali (OT)**
11/11	**Mese 10: Sicurezza in ambito A.I.**

👉 **SCOPRI DI PIÙ**

WEBINAR
EDU TIPS - Cybersecurity

GIANPIERO CIOLA

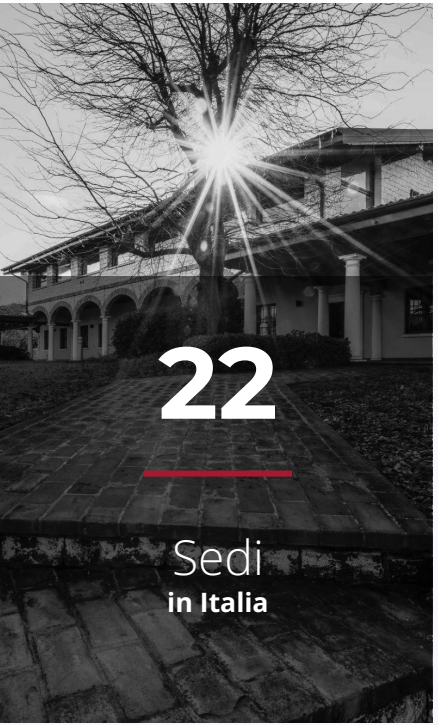
Offering Manager @smeup ICS

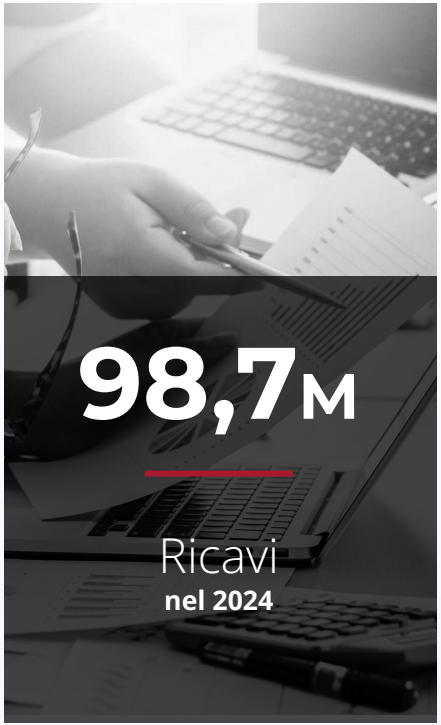
COMPANY OVERVIEW

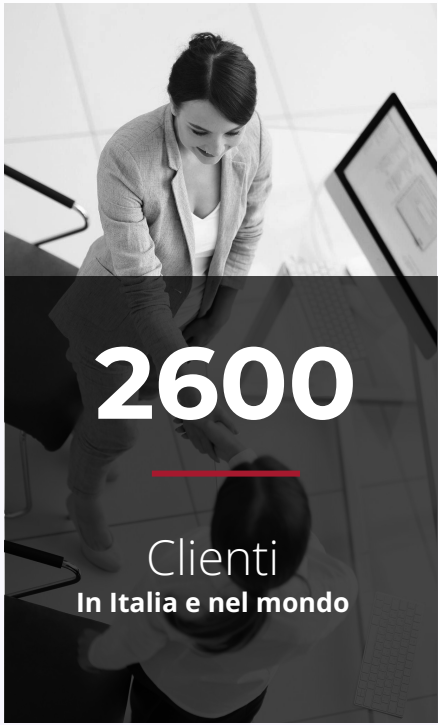
smeup in breve.

COMPANY **OVERVIEW**

smeup in Numeri.







BUSINESS SECTOR

BUSINESS SOFTWARE APPLICATION

Soluzioni **Software** per **PMI** e **grandi industrie.**

Ogni azienda è unica. smeup lo sa!
Usare la digitalizzazione per sviluppare il business e generare valore, ***insieme***.

- **e** GESTIONALI ERP
- **b** BUSINESS ANALYTICS
- **d** DOCUMENTALE
- **w** WEB & MOBILE APPLICATION
- **f** IOT E INTEGRAZIONE INDUSTRIALE
- **l** LOGISTICA E TRASPORTI

BUSINESS SECTOR

INFRASTRUCTURE, CLOUD & SECURITY

Soluzioni per **Architetture IT** e **servizi gestiti.**

Innovazione e **sicurezza** per rispondere ai bisogni delle aziende.

- i INFRASTRUTTURA
- c CLOUD
- cs CYBER SECURITY
- ps IBM POWER SYSTEMS

LA NOSTRA **MISSIONE**

Obiettivi e percorso.

In questo webinar esploreremo il **mondo dell'Intelligenza Artificiale**: dalle sue applicazioni ai rischi intrinseci, per fornirvi un percorso chiaro verso un'implementazione sicura.

IL **NOSTRO OBIETTIVO** È GUIDARVI ATTRAVERSO I SEGUENTI **PUNTI CHIAVE**:

- Comprendere l'Intelligenza Artificiale e le sue applicazioni principali
- Approfondire l'A.I. Generativa e i suoi componenti
- Analizzare l'architettura dei sistemi A.I. moderni
- Identificare le best practice di sicurezza specifiche per l'A.I.

IL **CONTESTO**

Cos'è l'Intelligenza Artificiale.

L'A.I. simula l'intelligenza umana attraverso algoritmi e modelli computazionali, ed è l'innovazione che sta ridefinendo il business moderno.

IL CONCETTO

L'A.I. simula l'intelligenza umana attraverso algoritmi e modelli computazionali. Capire come funziona è il primo passo per implementare misure di sicurezza efficaci.

APPLICAZIONI CHIAVE

- Assistenti virtuali
- Analisi predittiva
- Riconoscimento immagini
- Automazione processi

EVOLUZIONE E TENDENZE

- Machine Learning avanzato
- Deep Learning
- Natural Language Processing
- A.I. Generativa

L' **INTELLIGENZA ARTIFICIALE**

A.I. Generativa.

L'A.I. Generativa è la tecnologia che sta rivoluzionando il business, ma la sua rapida adozione crea nuovi e complessi vettori di rischio che dobbiamo comprendere e gestire.

Sistemi A.I. capaci di creare nuovi contenuti (testo, immagini, codice) basandosi su pattern appresi da enormi dataset.

Tecnologie chiave:

- **LLM** (Large Language Models): GPT, Claude, Gemini
- **Text-to-Image:** Nano Banana, Midjourney
- **Code Generation:** GitHub Copilot

CASI D'USO E APPLICAZIONI

- **Content creation:** generazione di articoli, riassunti e testi di marketing.
- **Customer support:** chatbot avanzati e assistenti virtuali.
- **Software development:** creazione e debugging automatico di codice (es. Copilot).
- **Data analysis:** sintesi e interpretazione di grandi volumi di dati.

Architettura di un sistema A.I.

UTENTE

Interagisce
tramite interfaccia
o Chatbot.

LLM

Large Language Model.
Il "motore" che elabora la richiesta.
Spesso risiede su cloud.

DOCUMENTI

Dati sensibili su cui l'AI si basa
per rispondere *(RAG - Retrieval Augmented Generation).*

Flusso dei dati: dove si genera il rischio

Il flusso dei dati è una sequenza di passaggi dove è necessario garantire sicurezza e privacy:

- **L'utente invia una richiesta tramite chatbot.** (*Inizio del flusso*)
- **L'LLM elabora la query e recupera informazioni dal RAG.** (*L'LLM accede ai dati sensibili*)
- **Risposta generata e inviata all'utente.** (*Rischio di data leakage se la risposta contiene dati non autorizzati*)

STRATEGIE DI **DIFESA**

Best Practice di sicurezza.

La **sicurezza nell'A.I.** non è un optional, ma una **necessità strategica nell'era dell'A.I.** Per integrare l'Intelligenza Artificiale in modo resiliente e a norma, è necessario agire su sei aree fondamentali:

01 **Protezione dei dati:** cifratura end-to-end, gestione chiavi API, conformità GDPR.

02 **Controllo accessi:** autenticazione multi-fattore, gestione ruoli, audit log.

03 **Validazione input:** sanitizzazione prompt, filtri anti-injection, rate limiting.

04 **Monitoraggio continuo:** detection anomalie, logging richieste, alert sospetti.

05 **Modelli sicuri:** versioning modelli, testing bias, aggiornamenti regolari.

06 **Governance:** policy aziendali, formazione, compliance normativa (NIS2, AI Act).


EDU TIPS
Q&A

Thank you!

GIANPIERO **CIOLA**

Offering Manager @smeup ICS

gianpiero.ciola@smeup.com

EDU TIPS CYBERSECURITY