



# Company Profile



# Abbiamo una missione molto chiara

## Trasformare il comportamento degli utenti

“Solo in questo modo le organizzazioni pubbliche e private potranno affrontare la transizione digitale in piena sicurezza.

Perché ciò accada è necessario che le persone acquisiscano una corretta postura digitale, indispensabile per ridurre la componente di vulnerabilità che deriva dall'errore umano.

L'acquisizione di un approccio consapevole dei rischi cyber, trasformerà gli utenti digitali da anello debole della catena difensiva, a prima linea di difesa contro il cyber crime.”

Security Awareness Training That Works!

Gianni Baroni, Founder e CEO Cyber Guru

# Sicurezza digitale per l'umanità

Siamo convinti che le tecnologie digitali contribuiranno a migliorare molti aspetti della nostra vita.

Ma siamo anche certi che in mancanza di un corretto atteggiamento nel loro utilizzo potrebbero esserci più ombre che luci.

Per questo ci impegniamo per rendere l'umanità più cyber sicura.

# Cyber Guru in breve

## Indice

[Chi siamo](#) >

[Clienti](#) >

[Dove siamo](#) >

[Cosa dicono di noi](#) >

[Una piattaforma di training completa](#) >

[I programmi di formazione](#) >

# Cyber Guru

Nasce nel 2017 per colmare la mancanza di efficacia dei percorsi formativi di Security Awareness presenti sul mercato.

Dal 2017, Gianni Baroni è fondatore, CEO e Amministratore delegato della società.

Cyber Guru è oggi presente in Europa con la sua piattaforma di Security Awareness Training più efficace, coinvolgente e facile da gestire presente sul mercato.

## Numeri

> **500.000**

Utenti attivi

> **3,5 milioni**

Lezioni fruite

> **4 milioni**

Simulazioni effettuate

# Più di 400 organizzazioni sono già nostre clienti

## Any size, any vertical

Aiutiamo i nostri clienti a trasformare il comportamento digitale della loro forza lavoro affinché nessuno possa diventare un inconsapevole alleato del cyber crime.

Per questa ragione organizzazioni, pubbliche o private, di qualsiasi dimensione e categoria merceologica, sono diventate nostre clienti.



Manufacturing



Education



Luxury & Fashion



Power & Energy



Public Administration



Healthcare



IT Services



Telco & Media



Banking & Insurance



Transportation



Retail



Food & Beverage

# Siamo presenti

**Europa:**  
Italia  
Francia  
Spagna

## Parigi

Campus Cyber  
5 Rue Bellini  
92800 Puteaux

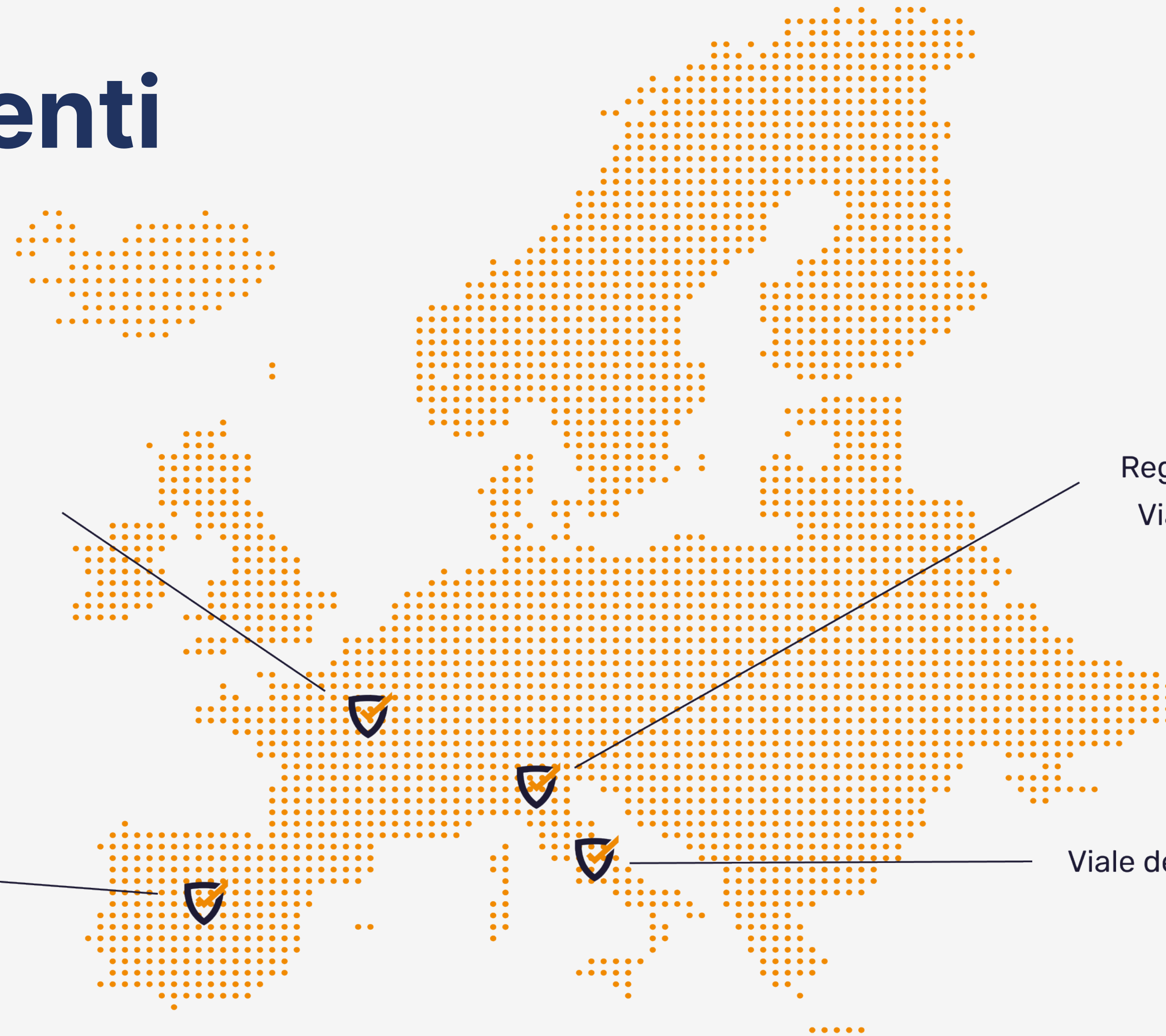
## Milano

Regus Milano Bicocca  
Via Libero Temolo 4  
20126 Milano

## Madrid

## Roma

Viale della Grande Muraglia 284  
00144 Roma



# Cosa dicono di noi

## The best Cyber training

“Great product and great team. Easy to implement and with a very proactive support team. No effort to keep it running”

CIO - Manufacturing Industry

★★★★★ - Cyber Guru Security Awareness Training

## Really Easy and Effective

“Intuitive solution, easy to use and designed to maximize user attention”

Chief Information Officer - Consumer Goods Industry

★★★★★ - Cyber Guru Security Awareness Training

## Cyber Guru is the best solution for Cyber Risk Awareness

“Kind and competent, they are very supportive especially in configuration and optimization activities of IT security solutions”

IT Manager and PMO - Banking Industry

★★★★★ - Cyber Guru Security Awareness Training

## Very good product in contents and user experience

“Very good product in contents and user experience. Move the effort regarding awareness from internal team to the product”

Chief Information Security Officer - Energy and Utilities Industry

★★★★★ - Cyber Guru Security Awareness Training

## Everything worked perfectly

“All people involved are skilled, committed and available. Our goal - to increase - employees awareness - seems reached”

Manager, IT Security and Risk Management - Manufacturing Industry

★★★★★ - Cyber Guru Security Awareness Training

## Great product and support

“We subscribed all the training channels of Cyber Guru platform. It's the perfect training: short and effective lessons, once a month, funny gamification”

Manager, IT Security and Risk Management - Transportation Industry

★★★★★ - Cyber Guru Security Awareness Training



Gartner® and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose



# Security Awareness Training: una piattaforma completa

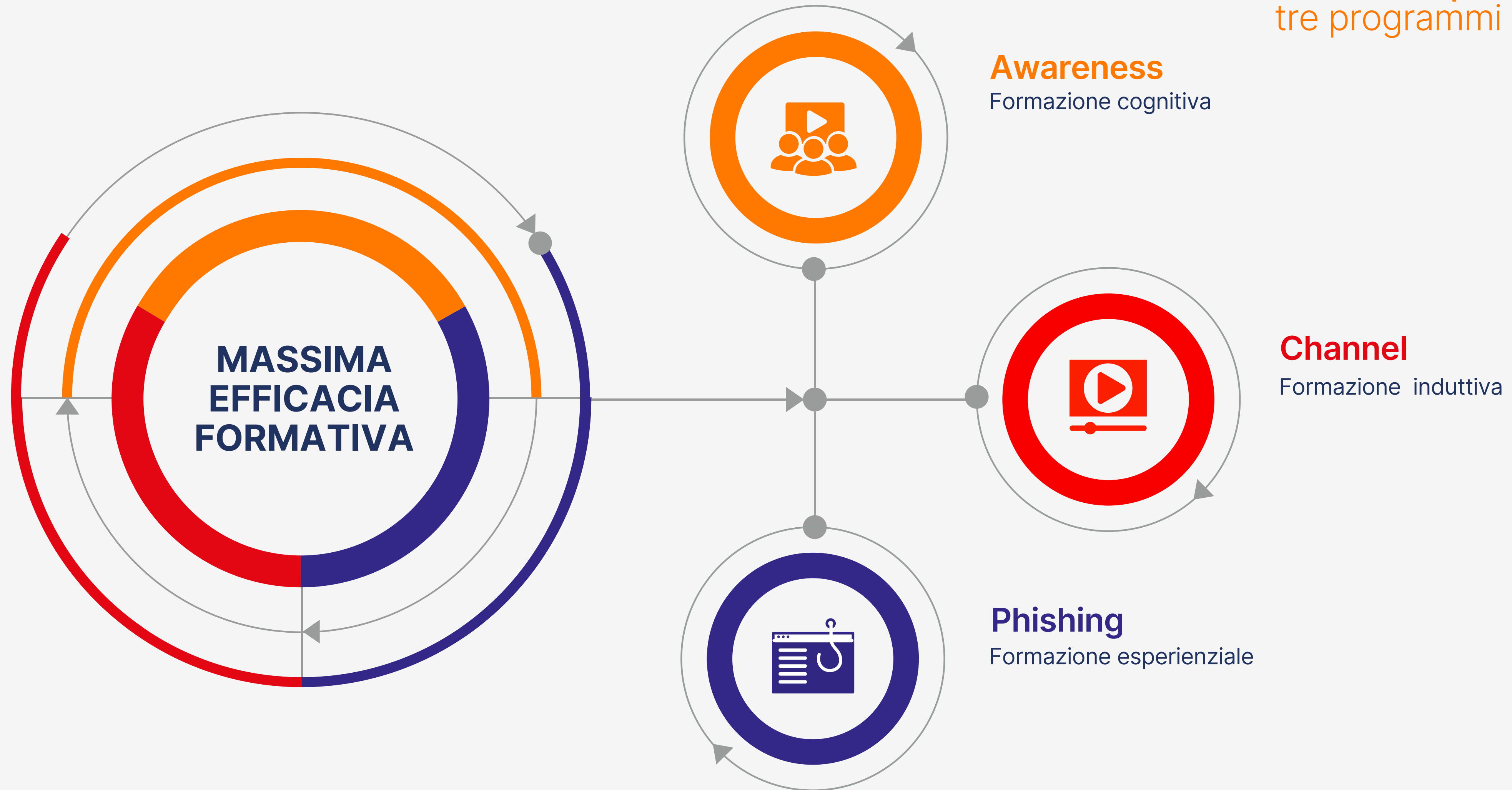
La piattaforma Cyber Guru è progettata per massimizzare l'efficacia dei processi di apprendimento e consolidare nel tempo la consapevolezza necessaria ad affrontare la continua evoluzione delle tecniche utilizzate dal cyber crime.

L'obiettivo principale dei programmi formativi è quello di incidere sui comportamenti degli utenti sviluppando le tre principali caratteristiche difensive di ogni individuo: la conoscenza, la percezione del pericolo, la prontezza.

Solo lavorando contemporaneamente su queste caratteristiche è possibile attivare quel processo di trasformazione dei comportamenti, essenziale in un programma di formazione realmente efficace.

Per questa ragione la piattaforma offre un training completo basato su tre programmi metodologici: **COGNITIVO, INDUTTIVO, ESPERIENZIALE.**

## Una piattaforma, tre programmi formativi



# Metodologie formative

## Formazione **Cognitiva** La conoscenza

La conoscenza viene sviluppata attraverso un programma di formazione cognitiva, Awareness Training, basato su un approccio principalmente didattico che agisce sulla parte del cervello più razionale. In questo programma vengono spiegate le principali tipologie di minacce, come si concretizzano e quali sono le logiche comportamentali più adeguate da seguire.

## Formazione **Induttiva** La percezione del pericolo

La capacità di percepire il pericolo, necessaria per riconoscere una minaccia, viene sviluppata attraverso un programma di formazione induttiva. Il Channel Training usa la narrazione di situazioni reali per incidere sulla componente emotiva del nostro cervello. Il discente, immedesimandosi nella storia, può comprendere come chiunque possa diventare vittima del cyber crime.

## Formazione **Esperienziale** La prontezza

Per reagire velocemente adottando il giusto comportamento di fronte al manifestarsi di un pericolo, è necessario mantenere allenata la prontezza attraverso simulazioni di attacco phishing o smishing. Il programma formativo di Phishing Training è realizzato per addestrare quella parte del cervello che è per sua natura predisposto ad attivare i meccanismi di azione-reazione.

# I tre programmi formativi



## Cyber Guru Awareness

Il programma didattico cognitivo, basato su una metodologia di formazione permanente, che garantisce lo sviluppo graduale della consapevolezza attraverso la conoscenza delle minacce della rete e dei comportamenti da adottare per prevenire gli attacchi.



## Cyber Guru Channel

Il programma di formazione induttiva che grazie alla forza di uno schema narrativo tipico delle serie TV, genera nel discente la capacità di apprendere attraverso l'identificazione all'interno di situazioni reali.



## Cyber Guru Phishing

Il programma di addestramento esperienziale automatico e adattivo, con funzione anti-phishing, che consente un allenamento personalizzato sulla base delle esperienze individuali e del singolo livello di resistenza agli attacchi.

# Cyber Guru Awareness

Cyber Guru Awareness è la componente didattica della piattaforma, in modalità e-learning, che si occupa di sviluppare una formazione prettamente cognitiva. L'obiettivo principale di questo programma formativo è quello di sviluppare la conoscenza delle minacce cyber. Un processo di apprendimento graduale, seguito dal mantenimento delle conoscenze e dall'aggiornamento delle competenze.



Moduli formativi auto-consistenti ad attivazione mensile



Impegno settimanale minimo, compatibile con qualsiasi funzione



Micro-lezioni video in formato multimediale



Utilizzo di attori professionisti con funzioni di coach



Linguaggio altamente divulgativo



Approccio interattivo con continua alternanza tra micro lezioni e test



Test di valutazione a risposta multipla



Metodologia di gamification, con organizzazione in team



Piattaforma multilingua



Contenuti aggiuntivi e costantemente aggiornati

# Cyber Guru Channel

La metodologia induttiva utilizzata si basa sull'immersione dell'utente all'interno di una situazione reale e su un processo di auto-identificazione con la minaccia Cyber, che assume così una forma concreta. L'utente assume consapevolezza non attraverso una nozione, ma attraverso una narrazione, la quale agisce, prima, sulla percezione del pericolo, e successivamente sull'elemento nozionistico, superando un retropensiero molto pericoloso: "a me non può capitare". Le tre principali caratteristiche sono l'apprendimento induttivo efficace, il massimo coinvolgimento del discente e la supervisione ad impatto zero.



Formazione continua



Produzioni video avanzate



Più formati video con storytelling diversi



Episodi brevi



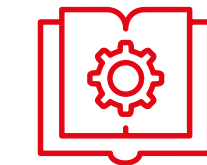
Ritmo narrativo elevato



Auto-identificazione in situazioni realistiche



Approccio Netflix-Like



Documentazione di approfondimento per ogni episodio



Reportistica esaustiva sul livello di fruizione



Funzioni di student caring automatico, per motivare la partecipazione

# Cyber Guru Phishing

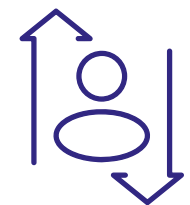
Cyber Guru Phishing è stato progettato per addestrare la forza lavoro a resistere agli attacchi phishing, attraverso campagne di attacchi simulati, che vengono personalizzati sulla base del profilo comportamentale del singolo utente, grazie a un processo automatico e adattativo, guidato dall'uso di tecnologie di intelligenza artificiale. Il discente aumenta la resistenza agli attacchi attraverso l'esperienza, sia quella negativa dell'errore che quella positiva del riconoscimento dell'attacco. Le tre principali caratteristiche sono l'addestramento esperienziale efficace, l'allenamento personalizzato e la supervisione a impatto zero.



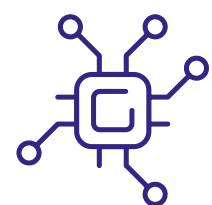
Addestramento esperienziale efficace e continuativo



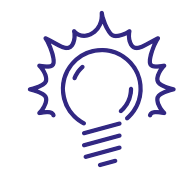
Allenamento personalizzato tramite processo adattivo



Livelli di difficoltà e simulazioni personalizzate



Campagne di attacco automatizzate



Errore > Formazione istantanea



Procedura di segnalazione



Template pre-caricati



Reportistica analitica e manageriale attraverso una dashboard avanzata



Gruppi di rischio



Politiche di remediation



# Security Awareness Training That Works!

[www.cyberguru.io](http://www.cyberguru.io)