



Security Awareness Training That Works!

**Come trasformare i dipendenti nella prima
linea di difesa contro il Cyber Crime**

Speaker Name

www.cyberguru.io

L'anello debole



74%

**degli attacchi cyber è
riconducibile ad un errore umano**

«74% of breaches involved the human element, which includes social engineering attacks, errors or misuse.»

Verizon - 2023 Data Breach Investigations Report

La forza di una catena

“Una catena è forte, quanto il suo anello piu’ debole”

La resistenza complessiva agli **attacchi cyber** di un'organizzazione dipende dalla **resistenza del fattore umano**

La piattaforma completa Cyber Guru

Un'unica piattaforma. Tre programmi formativi.



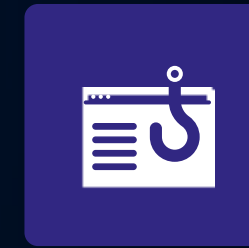
CYBER GURU AWARENESS

Formazione **Cognitiva**
Next-Gen e-learning



CYBER GURU CHANNEL

Formazione **Induttiva**
Netflix-like videos



CYBER GURU PHISHING

Addestramento **Esperienziale**
Adaptive anti-phishing

Cognizione

Percezione

Prontezza

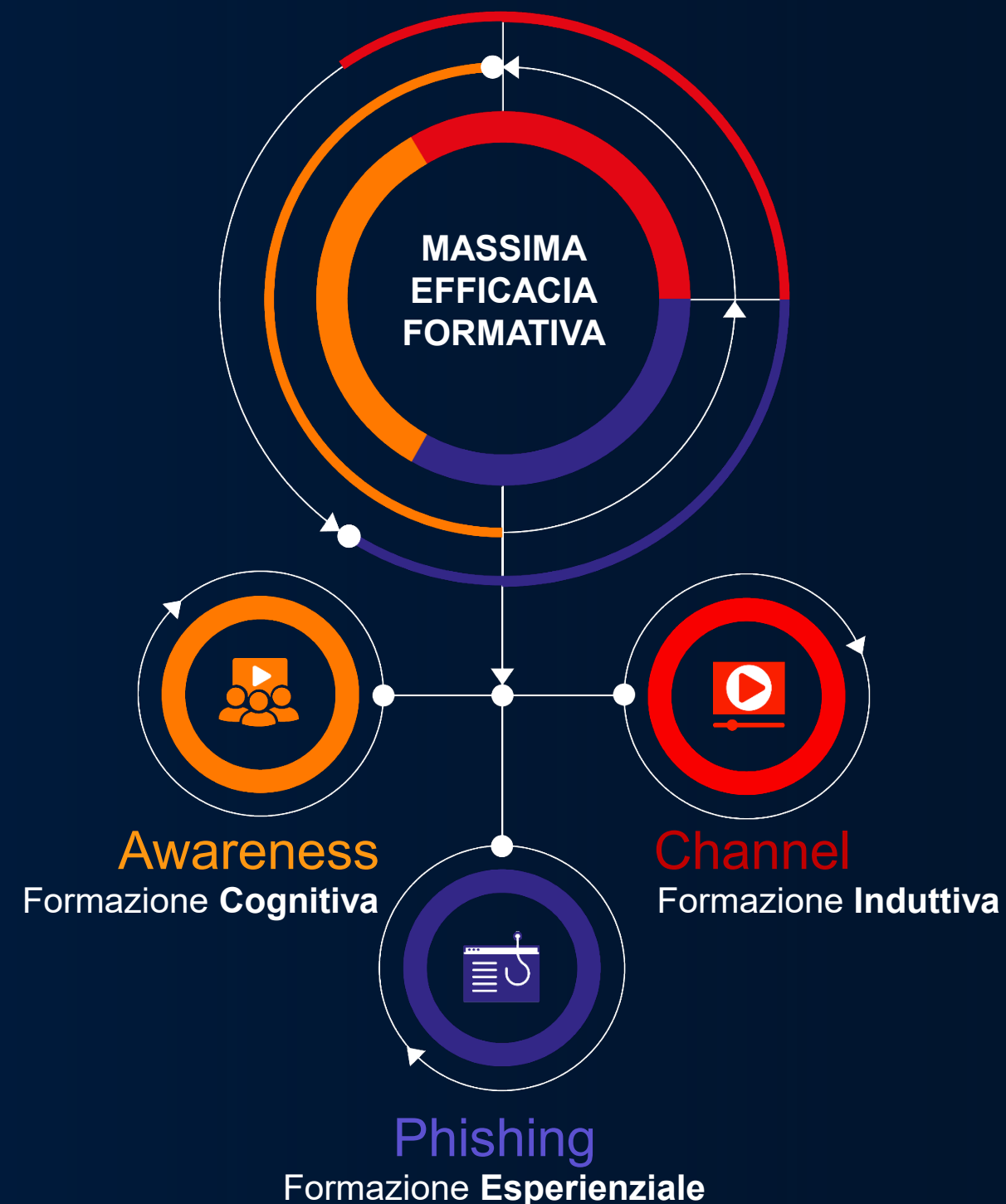
Comportamenti

Cyber Guru

Una piattaforma di formazione completa sulla Security Awareness per cambiare i comportamenti

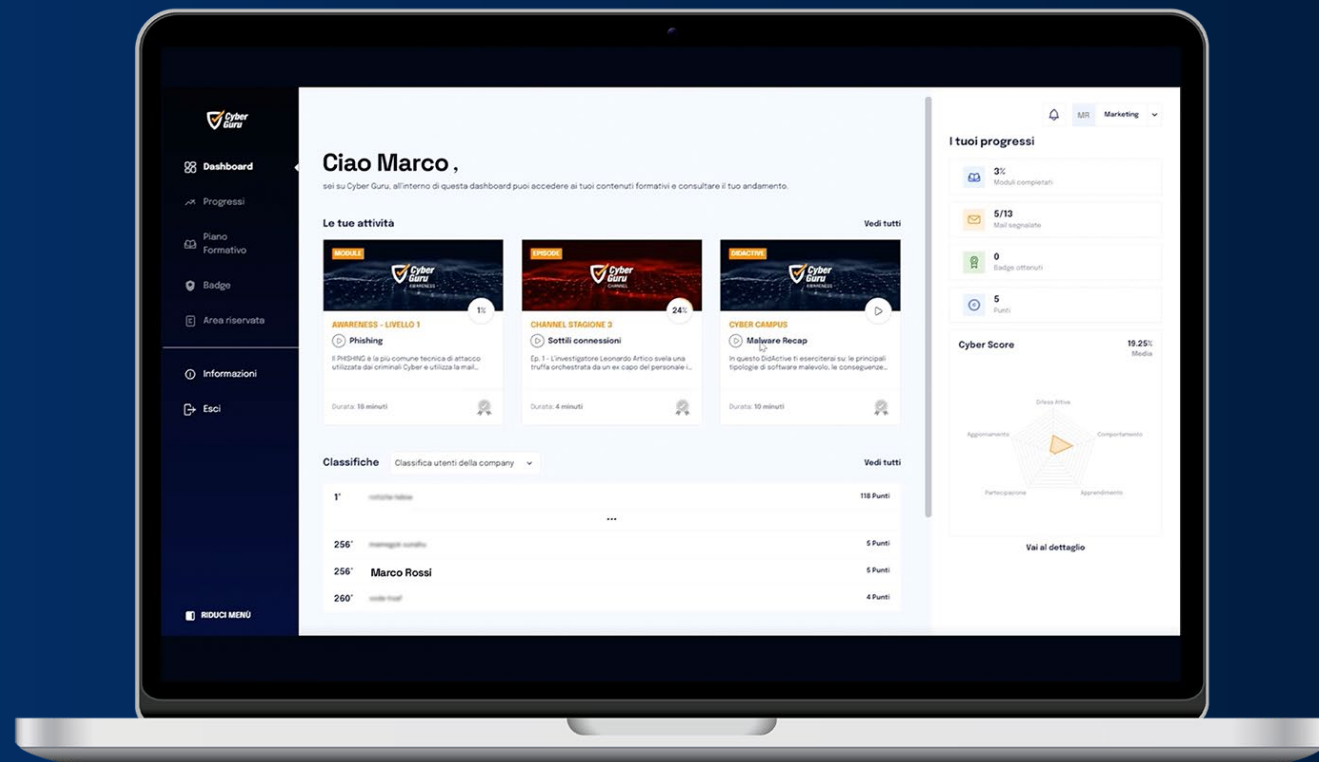
Un'unica piattaforma. Tre programmi formativi. Molti risultati consistenti:

- ▶ **Coinvolgimento** spontaneo dei tuoi dipendenti per lingua, cultura e funzione
- ▶ Massima **Efficacia** nel trasformare il comportamento dell'utente mantenendo alta la produttività
- ▶ **Efficienza** concreta e senza costi aggiuntivi grazie a un motore di ML completamente automatizzato



Piattaforma Cyber Guru v2.0

Novità



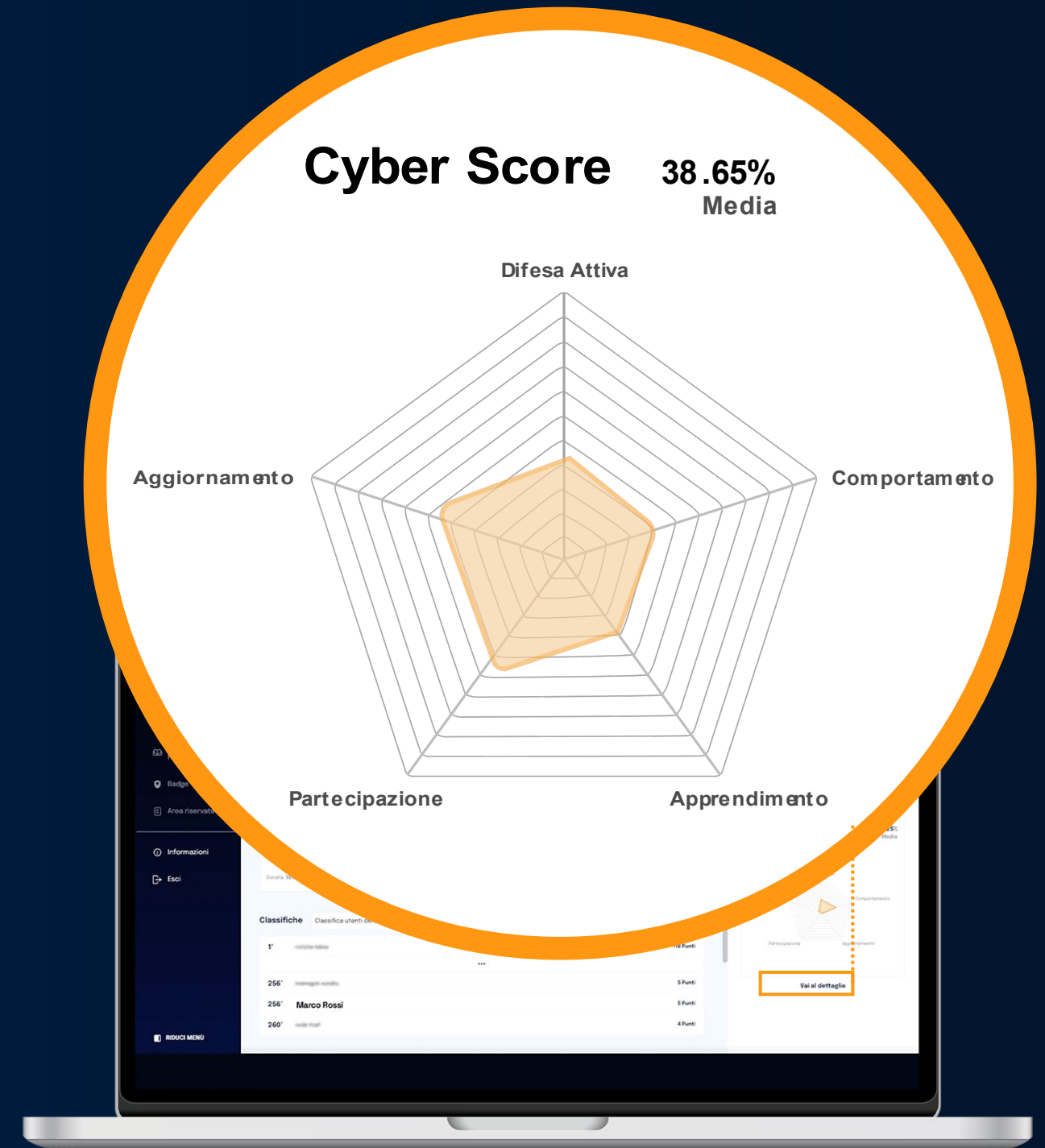
- ▶ Un'unica piattaforma, tre programmi formativi
- ▶ Un modello esclusivo e innovativo di Machine Learning per la formazione phishing
- ▶ Un'esperienza utente unificata e un'interfaccia utente all'avanguardia
- ▶ Dashboard personalizzate per persona
- ▶ Reporting avanzato
- ▶ Architettura aperta e scalabile con interoperabilità SCORM
- ▶ Gamification unificata per i 3 programmi formativi
- ▶ Automatizzata e a bassa manutenzione

Cyber Guru

Cyber Score

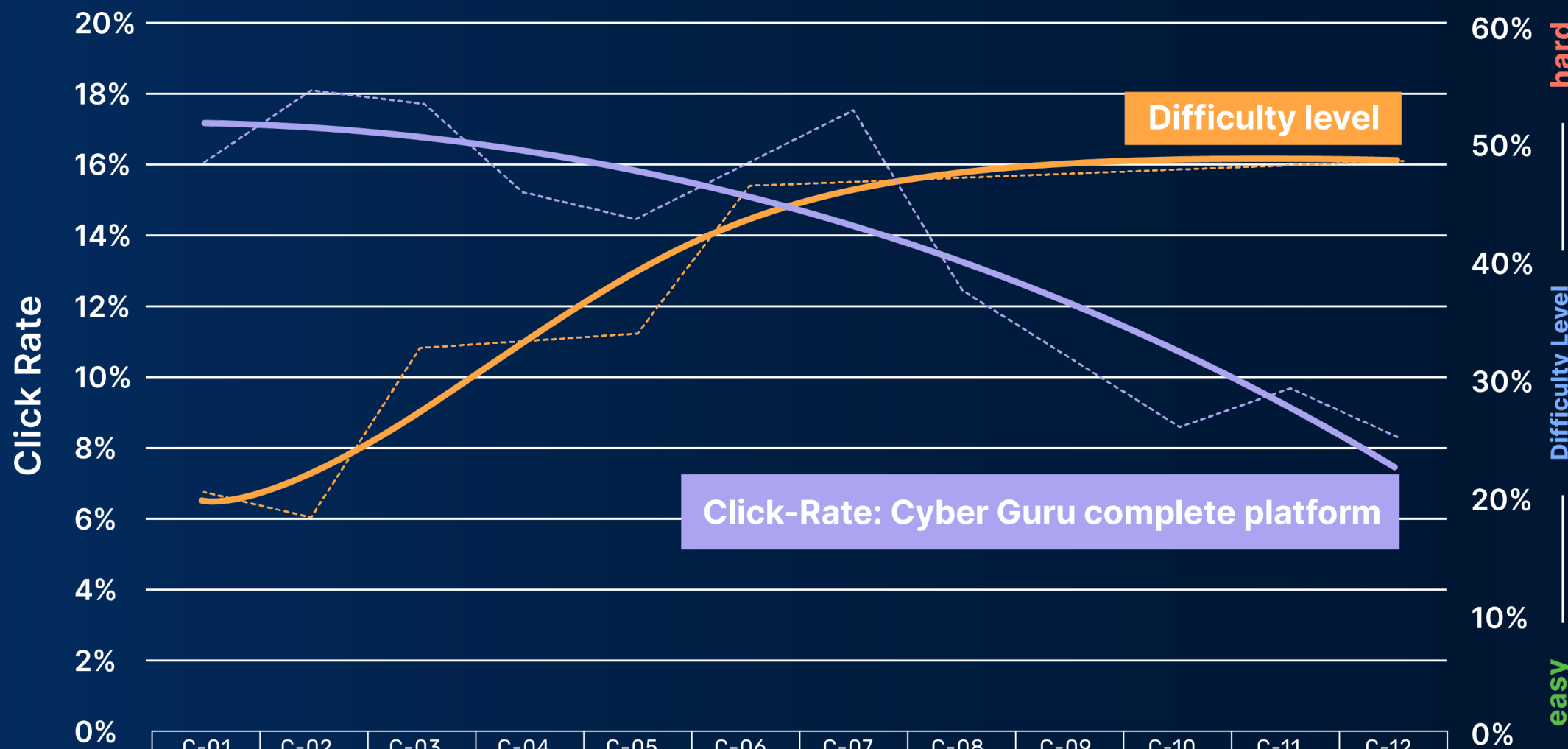
Il Cyber Score mostra i risultati raggiunti per cinque dimensioni chiave

- ▶ Difesa Attiva
 - ▶ Comportamento
 - ▶ Apprendimento
 - ▶ Partecipazione
 - ▶ Aggiornamento
- Valutazione del comportamento raggiunto sul riconoscimento degli attacchi phishing
- Valutazione dei risultati raggiunti sulla base dei test CGA
- Allineamento e regolarità con il piano formativo



Efficacia in azione

Una piattaforma completa per migliorare la **sicurezza della postura digitale**



50%
click-rate
reduction
over 12
months

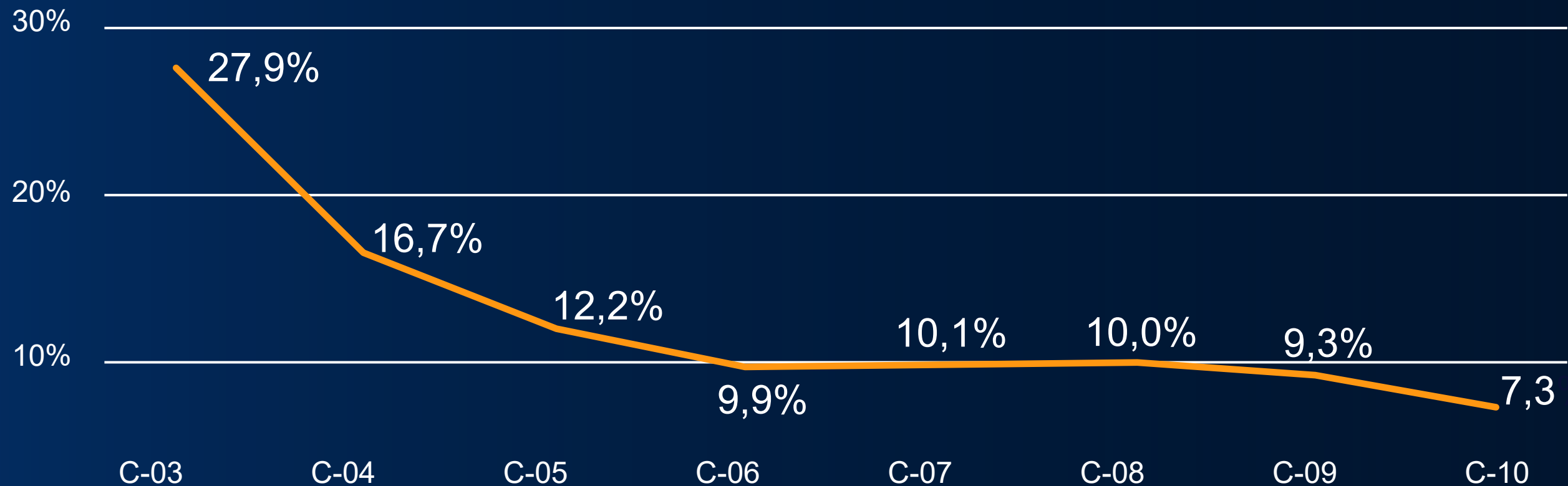
Source: Data analysis from 173 clients and 162K users that have received 1.9M simulated phishing attacks on the Cyber Guru platform over 12 months (Oct 21 to Oct 22)

	C-01	C-02	C-03	C-04	C-05	C-06	C-07	C-08	C-09	C-10	C-11	C-12
---- Click Rate	16%	18%	18%	15%	14%	15%	18%	12%	11%	9%	10%	8%
---- Difficulty Level	20%	18%	32%	32%	34%	46%	47%	47%	48%	48%	48%	48%

Riduzione del rischio phishing

Serial Clickers

Tasso di click ad alto rischio



Formazione

La formazione dei dipendenti è una **misura necessaria**

Sviluppare negli utenti una chiara consapevolezza del **rischio Cyber**

- ▶ Trasformare i **comportamenti**
- ▶ Aumentare la **resistenza agli attacchi**
- ▶ Conformità alle **normative**

Efficacia Formativa

È necessario superare gli
errori del passato

La formazione tradizionale ha
evidenziato chiari limiti di efficacia

Coinvolgere il discente

Il contesto

Se l'utente digitale è l'anello debole della catena difensiva, la formazione degli utenti è una misura di sicurezza necessaria



L'UTENTE È
L'ANELLO DEBOLE

Il 74% degli attacchi cyber è riconducibile ad un errore umano



INVESTIRE SUL
FATTORE UMANO

È necessario formare il personale dipendente rendendolo consapevole dei rischi Cyber

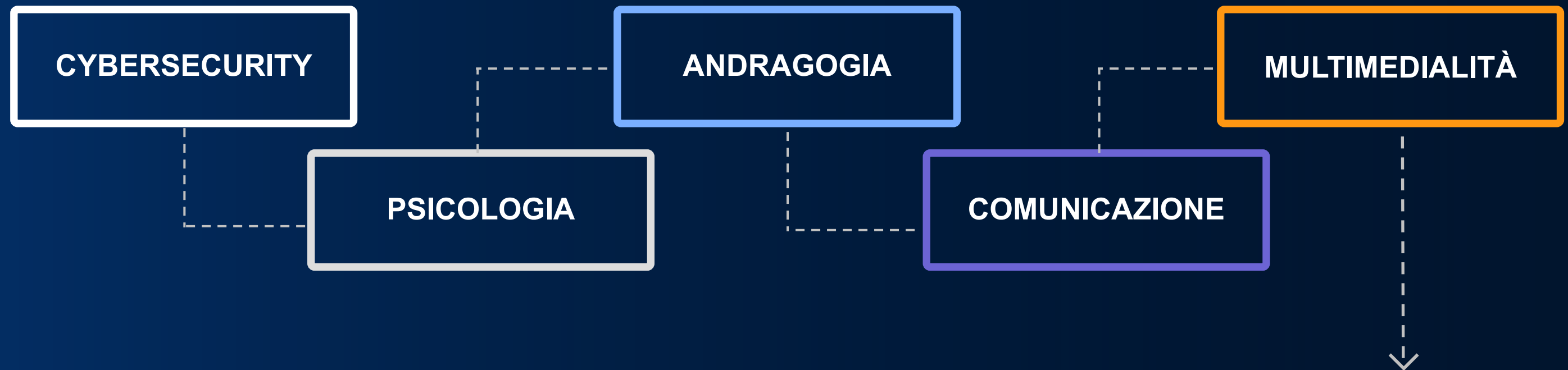


TRASFORMARE I
COMPORAMENTI

La formazione deve essere efficace, rendendo i comportamenti adeguati al livello della minaccia

Come produciamo i contenuti

Un processo di trasformazione collaudato, con una metodologia orientata al risultato

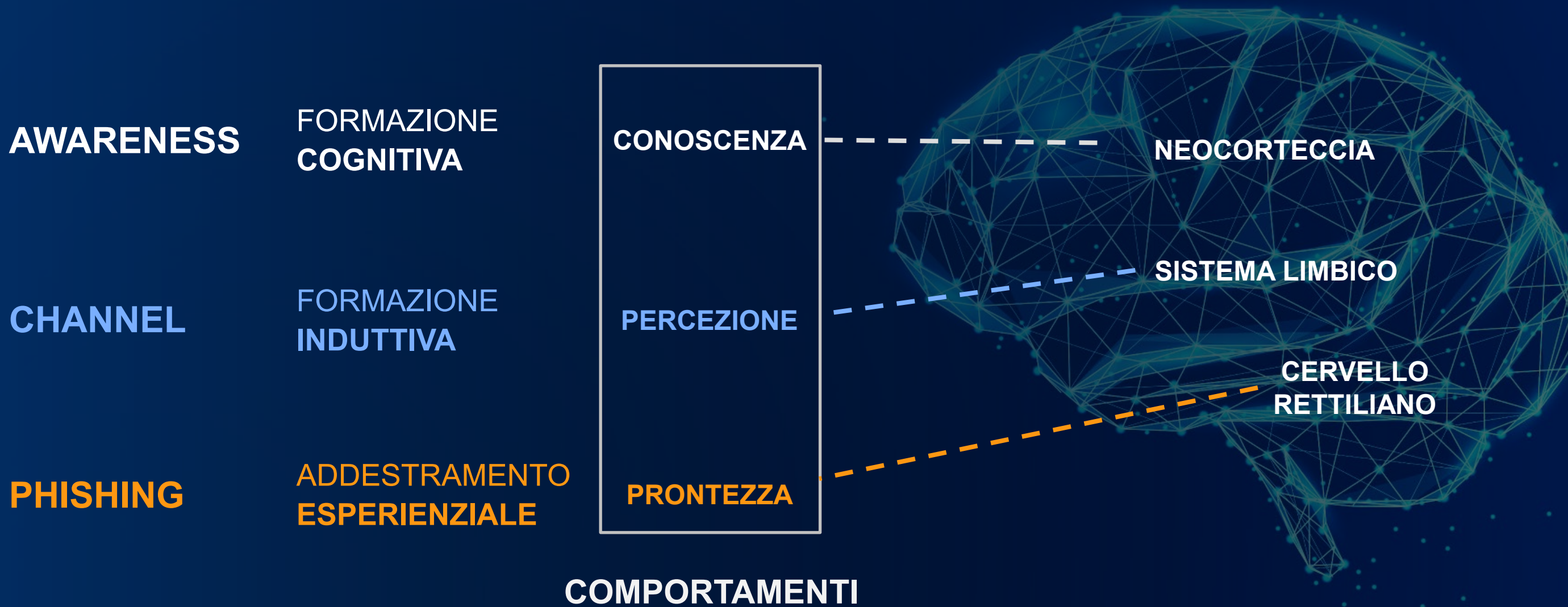


Fruizione su **piattaforme tecnologiche innovative**

Contenuto tecnologico → Contenuto apprenditivo

Metodologia

Agisce sui **processi di apprendimento**, sviluppando le difese dell'individuo



Metodologia

Per trasformare i **comportamenti** è necessario agire efficacemente sui **processi di apprendimento**



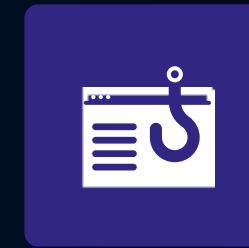
CYBER GURU **AWARENESS**

Cognitive Training
Next-Gen e-learning



CYBER GURU **CHANNEL**

Inductive Training
Netflix-like videos



CYBER GURU **PHISHING**

Experiential Learning
Adaptative anti-phishing

Cognizione

Percezione

Prontezza

Comportamenti

Le nostre soluzioni

Una piattaforma completa di Cyber Security Awareness, per tutta la forza lavoro



CYBER GURU AWARENESS

E-learning based program

Programma didattico/cognitivo che garantisce lo sviluppo graduale della consapevolezza



CYBER GURU CHANNEL

Web-series based program

Programma induttivo che sfrutta la forza della narrazione e della produzione video



CYBER GURU PHISHING

Adaptive anti-phishing training

Programma di addestramento esperienziale automatizzato e adattivo

Cyber Guru Awareness

E-learning based program



Formazione cognitiva realizzata con un programma didattico in
“**formazione continua**” (Smart-School)

L'apprendimento è garantito dall'adozione dei più avanzati **principi multimediali** e della formazione degli adulti, che massimizzano efficacia e coinvolgimento

Progress, Maintenance & Update

Un percorso graduale di apprendimento per sviluppare il giusto grado di conoscenza, per poi lavorare al mantenimento e all'aggiornamento delle competenze acquisite



Caratteristiche



APPRENDIMENTO COGNITIVO EFFICACE

- FORMAZIONE CONTINUA
- MODULI AUTO-CONSISTENTI
- MICRO-LEARNING
- VIDEO CON ATTORI COACH
- TEST A FINE LEZIONE



MASSIMO COINVOLGIMENTO DEL DISCENTE

- OTTIMIZZAZIONE CARICO COGNITIVO
- LEVA INDIVIDUALE
- GAMIFICATION INDIVIDUALE
- GAMIFICATION A SQUADRE



SUPERVISIONE A IMPATTO ZERO

- PIATTAFORMA IN SaaS
- SERVIZIO CHIAVI IN MANO
- PIANI FORMATIVI PRECOSTITUITI
- STUDENT CARING AUTOMATICO
- REPORTISTICA ESAURIENTE

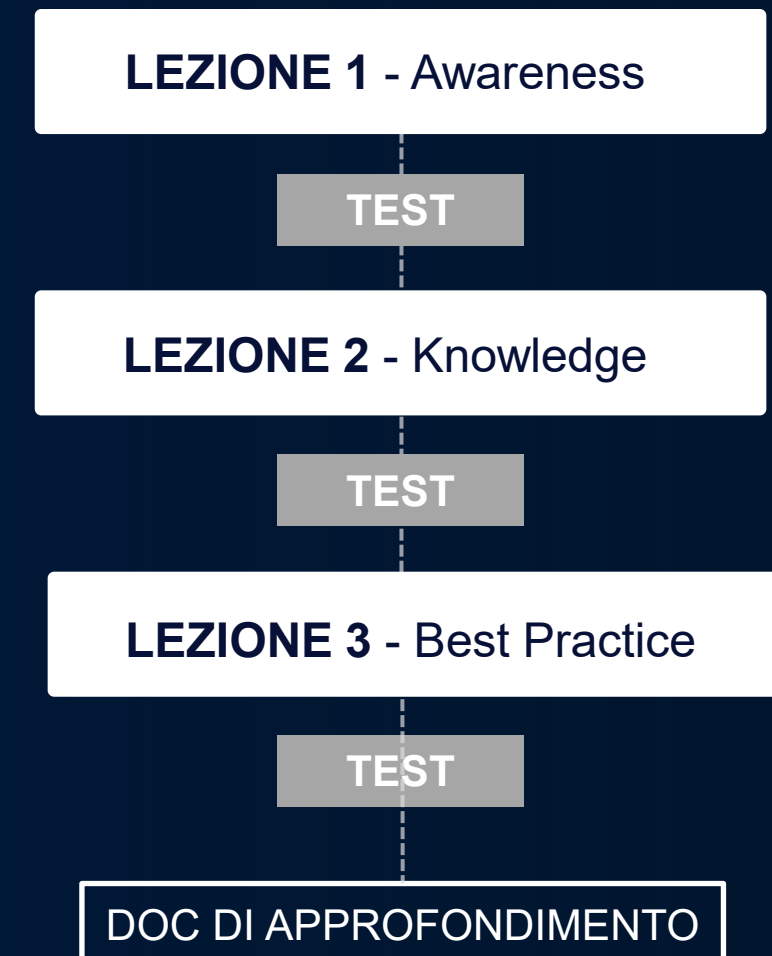
Cyber School

Offerta formativa di **primo livello**

PERCORSO FORMATIVO ANNUALE COSTITUITO DA 12 MODULI
AUTOCONSISTENTI



STRUTTURA DEL MODULO
IN 3 LEZIONI



Caratteristiche

Offerta formativa **secondo e terzo livello**

LEVEL 2

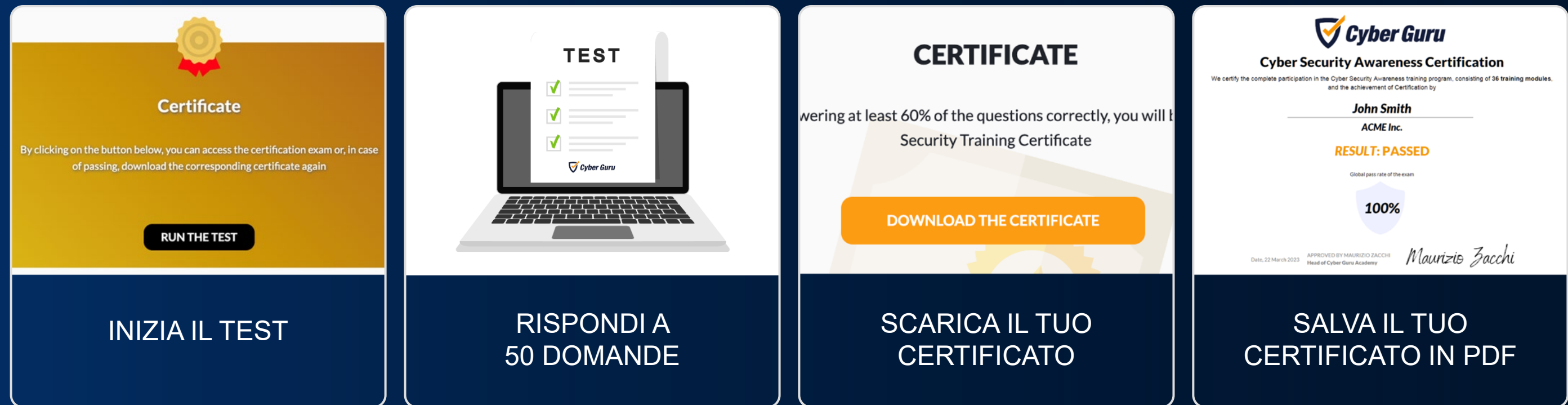
CLEAN DESK	SMART-WORKING	SOCIAL COLLABORATION & VIDEO	SMISHING & VISHING	SPEAR PHISHING	RANSOMWARE
MULTI-FACTOR AUTHENTICATION	IoT DEVICE	BLUETOOTH & WI-FI	INFORMATION CLASSIFICATION	DATA PROTECTION	SOCIAL ENGINEERING 2

LEVEL 3

REAL SCAM	PHONE SCAM	SOCIAL & CYBERBULLYING	PRIVACY	LEGAL ASPECT	PHYSICAL SECURITY
E-COMMERCE	HOLIDAY & BUSINESS TRIPS	CYBER HYGIENE	BACKUP & RESTORE	TOP BEST PRACTICE	SOCIAL ENGINEERING 3

Certificazione

Certificazione al termine del terzo livello



PROCESSO DI CERTIFICAZIONE

Cyber Campus

Formazione permanente

Awareness 


Learning object interattivi che hanno l'obiettivo di **allenare la memoria** per:

- ▶ **Richiamare e consolidare la conoscenza acquisita**
- ▶ **Riorientare la conoscenza**
- ▶ **Colmare eventuali lacune**
- ▶ **Mantenere un costante aggiornamento sull'evoluzione dei rischi cyber**

**Uso intensivo
del feedback**

Maintenance & Update

Lifelong Learning



Wow una super offerta! Corso di inglese "professional" a 20€ al mese!

1

2

Prima devo inserire i dettagli sulla mia azienda e sul mio ruolo professionale...

3

4

QUALCHE ORA DOPO...

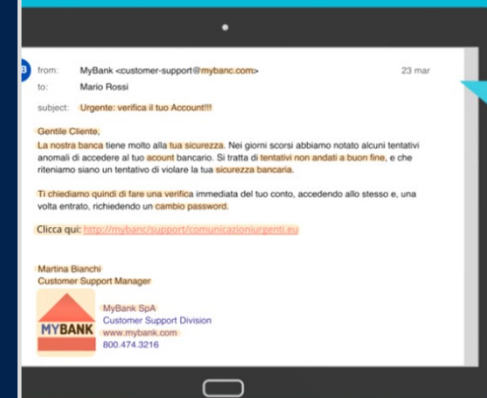
Ecco fatto!

Ma perché mi fa così comodo? Oh Noooooo!

VAI ALL'ESERCIZIO

Warm-Up

ci fanno intuire che si tratta di Phishing! Riesci a individuarli?



from: MyBank <customer-support@mybank.com> 23 mar
to: Mario Rossi
subject: Urgente: verifica il tuo Account!!!

Gentile Cliente:
La nostra banca tiene molto alla tua sicurezza. Nei giorni scorsi abbiamo notato alcuni tentativi anomali di accedere al tuo account bancario. Si tratta di tentativi non andati a buon fine, e che riteniamo siano un tentativo di violare la tua sicurezza bancaria.

Ti chiediamo quindi di fare una verifica immediata del tuo conto, accedendo allo stesso e, una volta entrato, richiedendo un cambio password.


Clicca qui: <http://mybank.com/customer-support/gentile>

Martina Bianchi
Customer Support Manager

MYBANK
MyBank SpA
Customer Support Division
www.mybank.com
800.474.3216

Seleziona sull'immagine tra le aree attive proprie i 5 indizi che ci consentono di smascherare l'e-mail contraffatta!

DidActive



Clicca su un punto e trascina l'immagine per esplorare l'ambiente. Quando trovi le aree sensibili clicca sopra.

Serious Game

Password Manager

avanzato conosciuto referenziato



LOGIN
Username: mariorossi
Password: *****



Cyber Insights

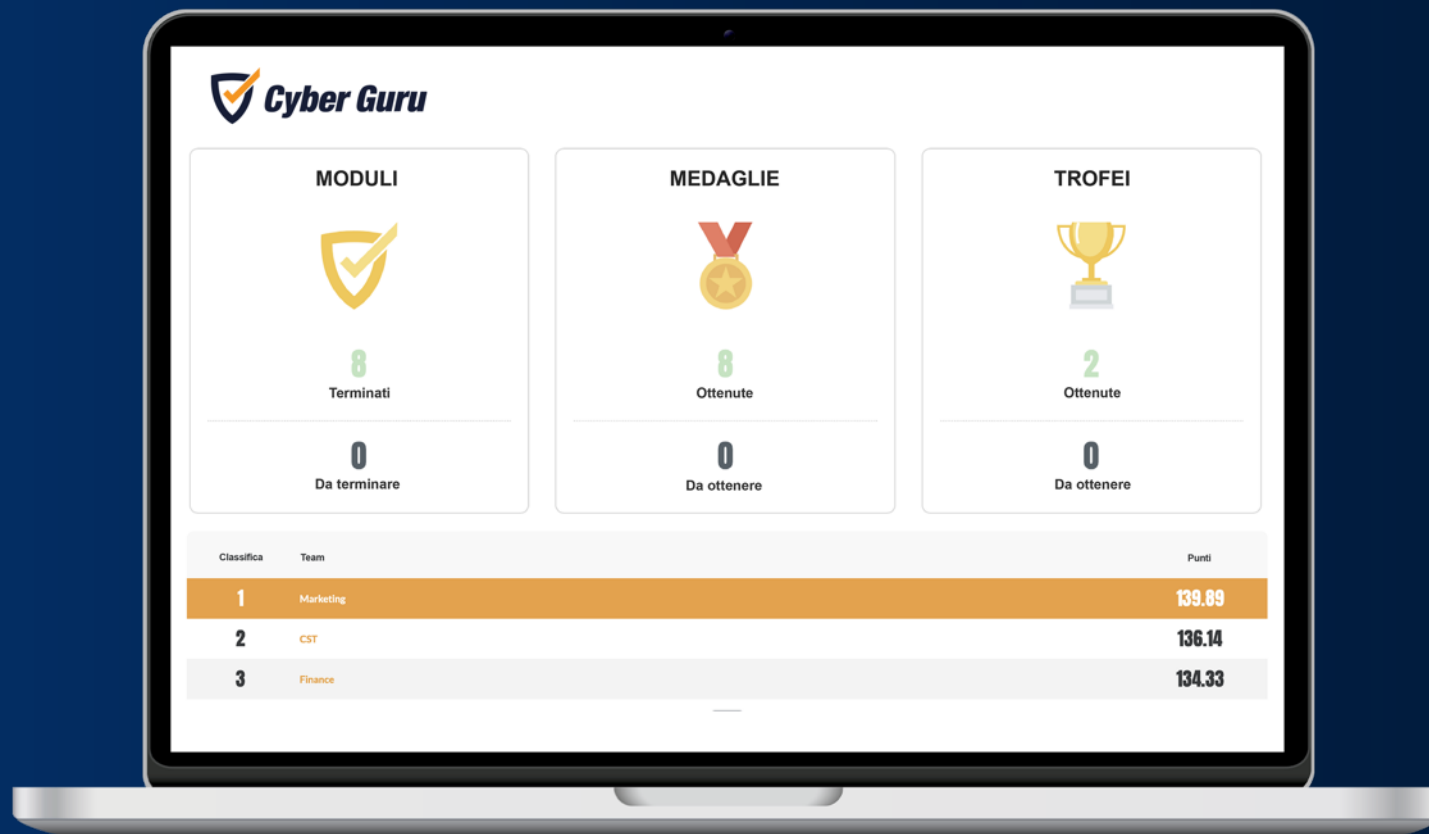
MANTENIMENTO

AGGIORNAMENTO

Gamification

Awareness 

Il gioco rafforza il grado di coinvolgimento negli utenti, aumentando l'efficacia dei processi di apprendimento



- ▶ È coinvolgente e motivante
- ▶ È decisiva in un percorso non obbligatorio
- ▶ Attiva processi di comunicazione interna
- ▶ Sviluppa una sana competizione
- ▶ Rafforza il senso di appartenenza
- ▶ Si sviluppa su tempistiche adeguate

Cyber Guru Channel

Web-series based program

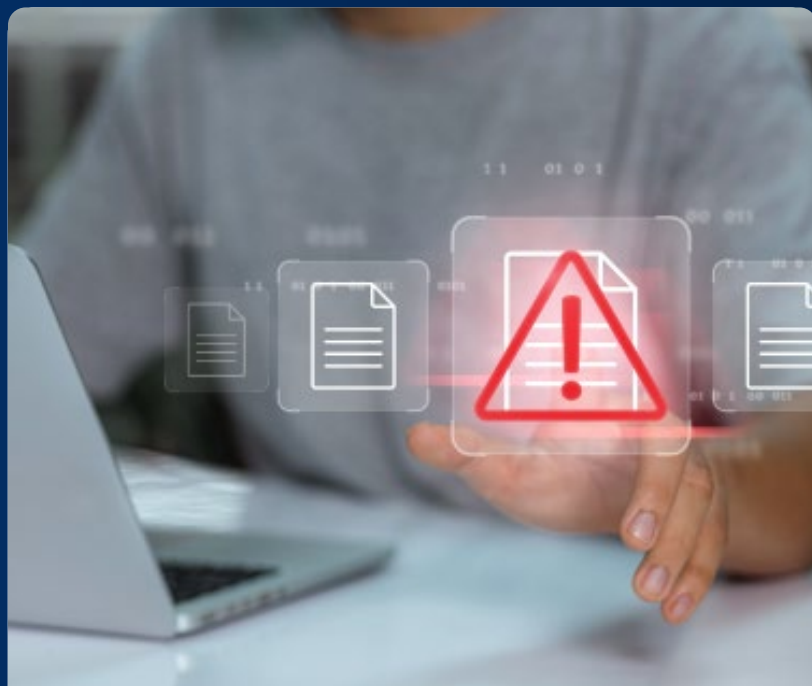


Formazione induttiva realizzata secondo lo schema narrativo delle serie televisive, che favorisce un processo di auto-identificazione del discente

Il discente **apprende attraverso la narrazione**, superando un retropensiero molto pericoloso: “a me non può accadere”

Formazione induttiva

Immergere un individuo in una **situazione reale**, resta il metodo più efficace per sviluppare un'adeguata percezione del pericolo



AVVERTIMENTO



DIDATTICA



ESPERIENZA IMMERSIVA



CYBER GURU CHANNEL



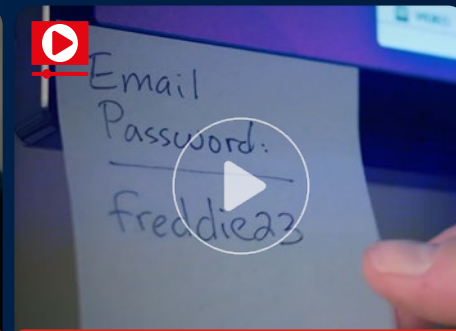


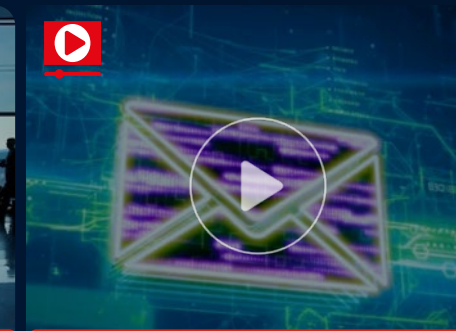



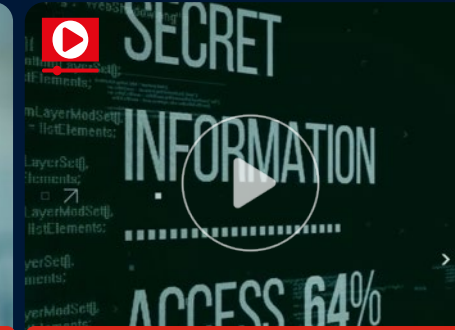

Struttura dei percorsi formativi

Channel 

Offerta formativa del **primo anno**, costituita da **12 episodi narrativi**

Serie ▼

Trappole in rete

 <p>Dal paradiso all'inferno in un clic - CEO FRAUD</p>	 <p>La tempesta perfetta SMART WORKING</p>	 <p>È solo un gioco! PASSWORD</p>	 <p>Per un "pugno" di canzoni USB DEVICE</p>	 <p>Impigliata nella rete PUBLIC WI-FI</p>	 <p>Il peggiore affare di sempre SOCIAL ENGINEERING</p>
 <p>Le vie dei truffatori sono infinite DEEPFAKE</p>	 <p>Impara a leggere! RANSOMWARE</p>	 <p>L'insostenibile leggerezza del conto in banca - SIM SWAP</p>	 <p>In troppi vogliono essere nei vostri panni - IDENTITY THEFT</p>	 <p>La tecnica del cocodrillo SCAM WEBSITES</p>	 <p>Rimborso fatale SMISHING</p>


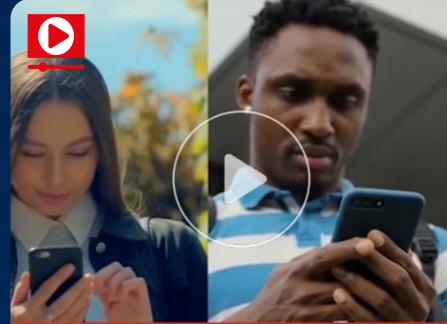










 Ogni episodio narrativo è comprensivo di un **documento didattico di approfondimento**

Struttura dei percorsi formativi

Offerta formativa del **secondo anno**, costituita da **12 episodi narrativi**

Serie ▼

Cybersecurity Breaking News

 Tutti pazzi per gli sconti WATERING HOLE	 Una pesca fruttuosa WHATSAPP SCAM	 Se telefonando VISHING & DATA THEFT	 Parcheggi "pericolosi" QISHING	 Provare, ma senza dimenticare FAKE WEBSITE	 Copia con troppa conoscenza CEO FRAUD
 Foto ricordo...da dimenticare DATA PROTECTION	 Galeotta fu l'e-mail SPEAR PHISHING	 Oltre le apparenze FAKE NEWS	 Una donazione "sbagliata" PHARMING	 Post Pericolosi PRIVACY	 Una vacanza molto "costosa" DISPOSITIVI CONDIVISI

 Ogni episodio narrativo è comprensivo di un **documento didattico di approfondimento**

Struttura dei percorsi formativi

Offerta formativa del **terzo anno**, costituita da **12 episodi narrativi**

Serie ▼

Indagini in rete, operazione Money Run

 <p>Sottili connessioni CEO FRAUD</p>	 <p>Una verità scomoda CREDENTIAL STUFFING</p>	 <p>Nessuna alternativa PASSWORD SECURITY</p>	 <p>Effetto domino PISHING (EMAIL SPOOFING)</p>	 <p>Il diavolo è nei dettagli SPEAR PHISHING</p>	 <p>Selfie galeotto PRIVACY VIOLATION</p>
 <p>Il gatto e la volpe 2.0 SIM SWAP</p>	 <p>Il leone e la gazzella WATERING HOLE</p>	 <p>Il pesce nella rete PUBLIC WI-FI</p>	 <p>Chiavetta USB letale USB DEVICE</p>	 <p>Key Logger (un nemico invisibile) MALWARE (KEYLOGGER)</p>	 <p>Il colpevole CYBERSECURITY</p>

 Ogni episodio narrativo è comprensivo di un **documento didattico di approfondimento**

Caratteristiche



APPRENDIMENTO INDUTTIVO EFFICACE

- FORMAZIONE CONTINUA
- EPISODI NARRATIVI BREVI
- AUTO-IDENTIFICAZIONE
- MATERIALI DI APPROFONDIMENTO



MASSIMO COINVOLGIMENTO DEL DISCENTE

- PRODUZIONI VIDEO AVANZATE
- RITMO NARRATIVO ELEVATO
- SITUAZIONI REALISTICHE
- APPROCCIO NETFLIX-LIKE



SUPERVISIONE A IMPATTO ZERO

- PIATTAFORMA IN SaaS
- SERVIZIO CHIAVI IN MANO
- SERIE PRECOSTITUITE
- STUDENT CARING AUTOMATICO
- REPORTISTICA ESAURIENTE

Cyber Guru Phishing

Adaptive anti-phishing training



Apprendimento esperienziale basato su simulazioni di attacco Phishing/Smishing guidate da un motore automatico che utilizza algoritmi di Intelligenza Artificiale

Il discente **aumenta la resistenza agli attacchi attraverso l'esperienza**, sia quella negativa dell'errore sia quella positiva del riconoscimento dell'attacco

Personal training

Per sviluppare **maggiore resistenza** è necessario adattare l'addestramento alle caratteristiche specifiche del singolo individuo (resistenza agli attacchi)



SERIAL CLICKERS



INTERMEDIATE USERS



STRONG USERS



CYBER DEFENDER

Phishing adattivo e continuo

Senza sforzo per il team di Security

IL NOSTRO PHISHING ENGINE AI/ML SELEZIONERÀ I MODELLI DI ATTACCO DI SIMULAZIONE E LA FREQUENZA IN BASE A:

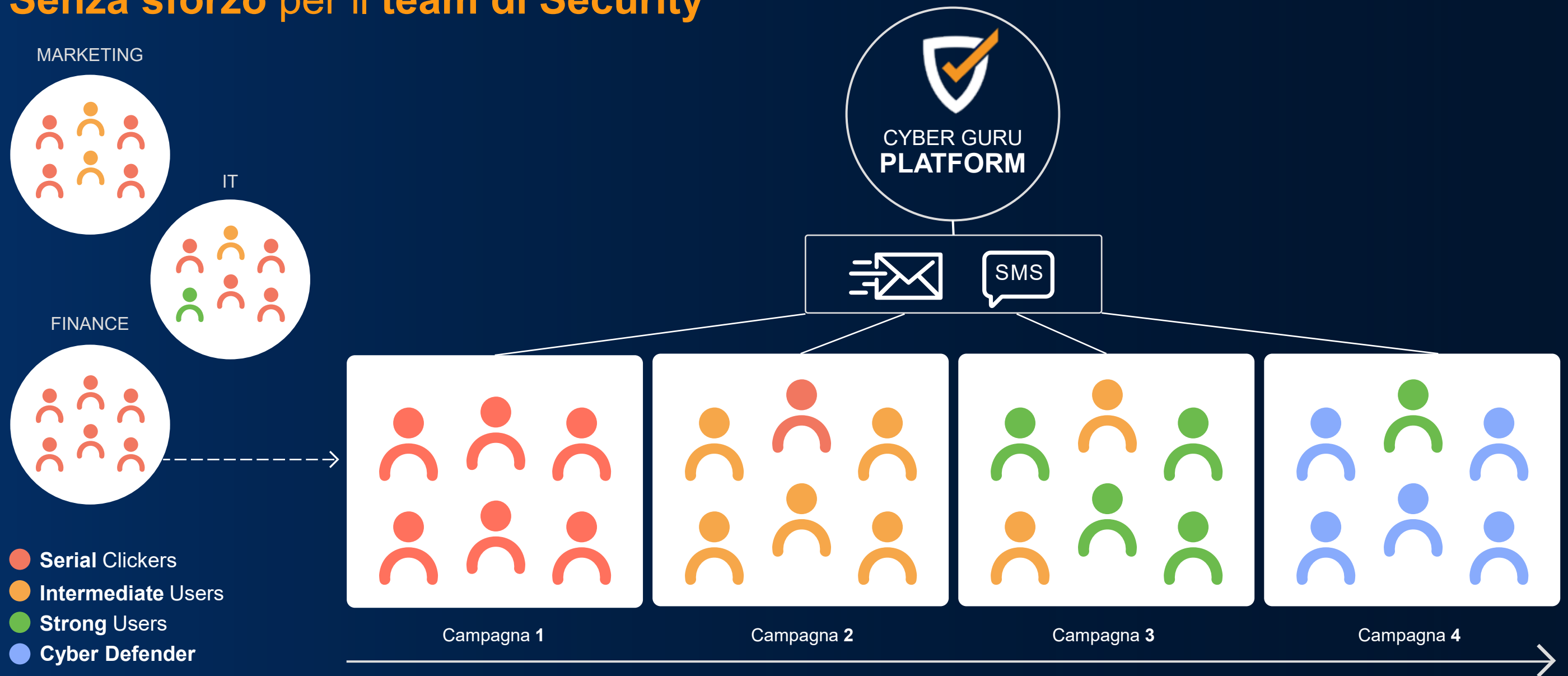
- **Segmentazione degli utenti** (lingua, luogo, reparto)
- **Capacità dell'utente di resistere agli attacchi** (regolazione continua del livello di difficoltà a ogni iterazione)
- **Canali disponibili/configurati dall'amministratore** (e-mail o SMS)

LA FREQUENZA, IL VOLUME E IL SETUP DEGLI ATTACCHI DI PHISHING HANNO UN IMPATTO BASSO O NULLO SUL TEAM DI SICUREZZA.

- **Selezione automatica degli templates di Phishing** (E-Mail/SMS)
- **Frequenza degli attacchi** (completamente automatizzata o selettiva)
- **Flusso degli attacchi completamente automatizzato**, senza alcun intervento manuale

Phishing adattivo e continuo

Senza sforzo per il team di Security



Gli utenti di gruppi diversi (segmenti) si rafforzano nel tempo, poiché la nostra piattaforma seleziona il modello giusto per ogni utente dopo ogni interazione

Processo adattivo

Delivery automatizzato delle campagne

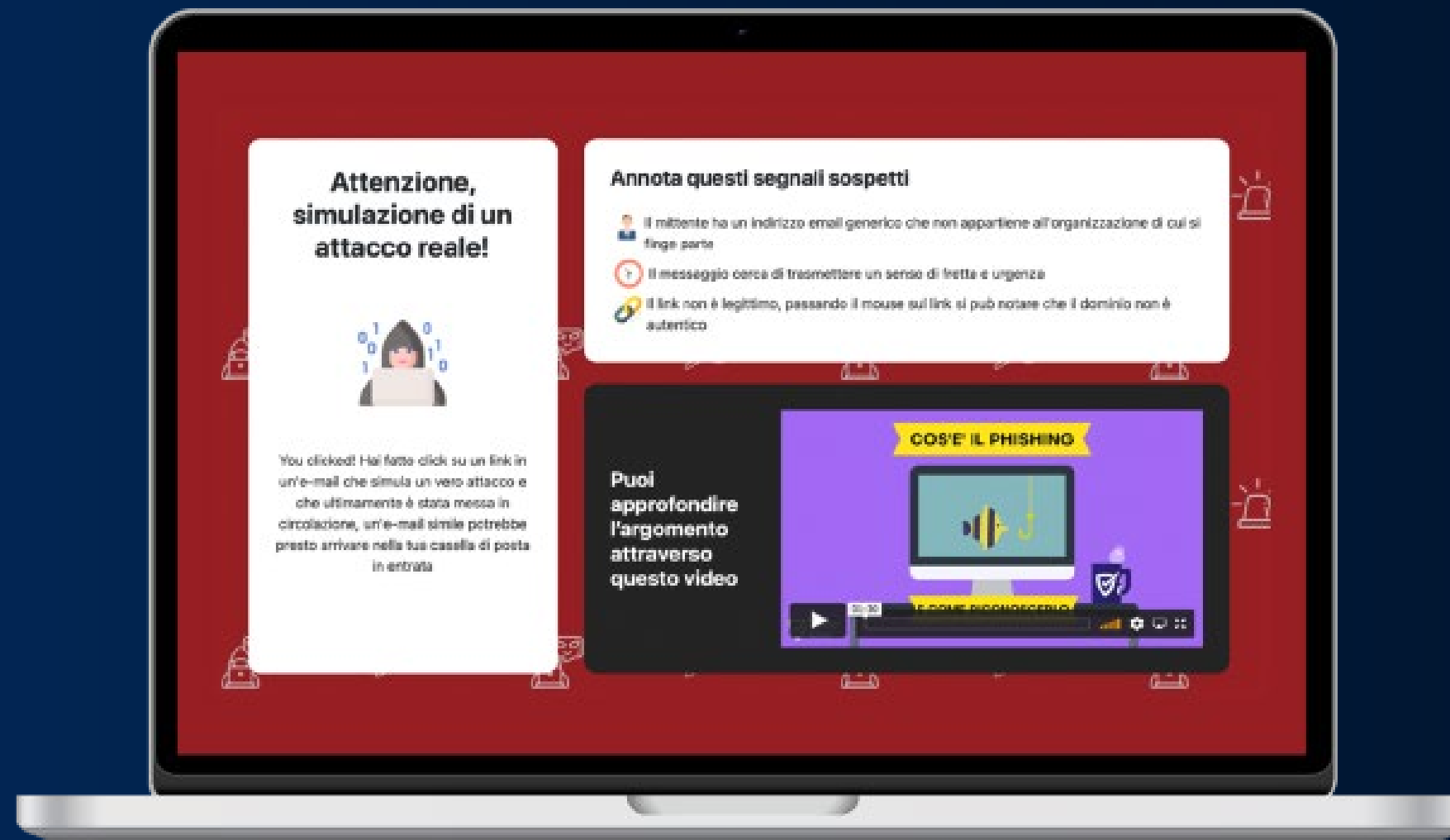


NUOVA CAMPAGNA

- ★ Il processo di approvazione dei template è opzionale e può essere completamente automatizzato

Landing Page

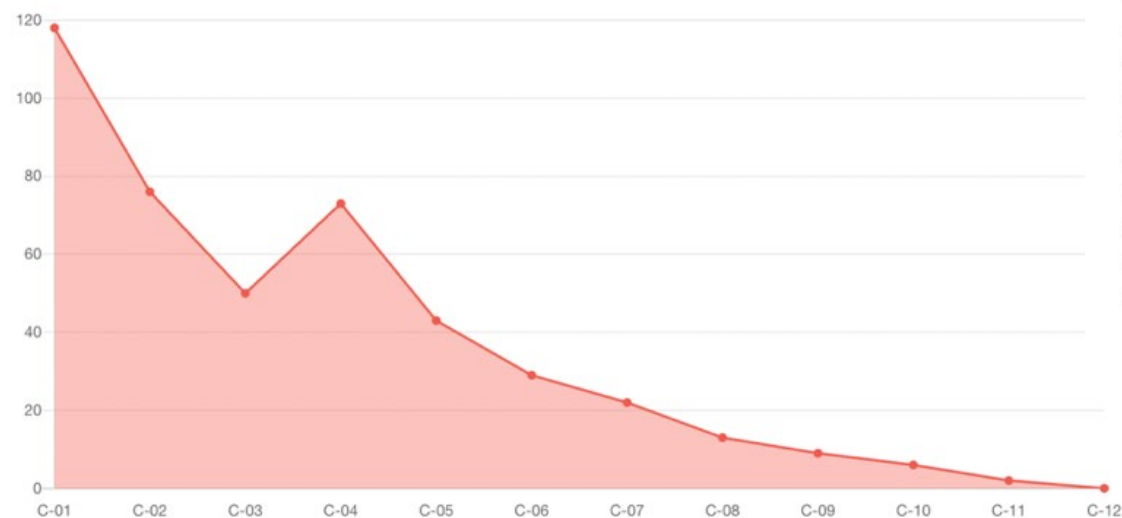
Formazione mirata per chi cade nella simulazione



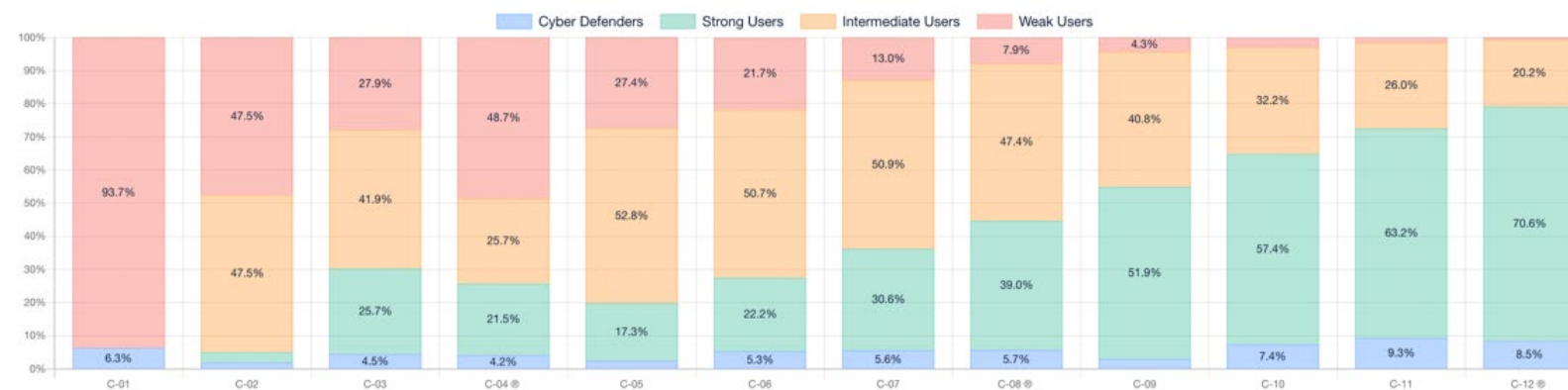
Efficacia comprovata

Riduzione del rischio Cyber e aumento della resistenza agli attacchi

Serial Clickers (Weak Users) ⓘ



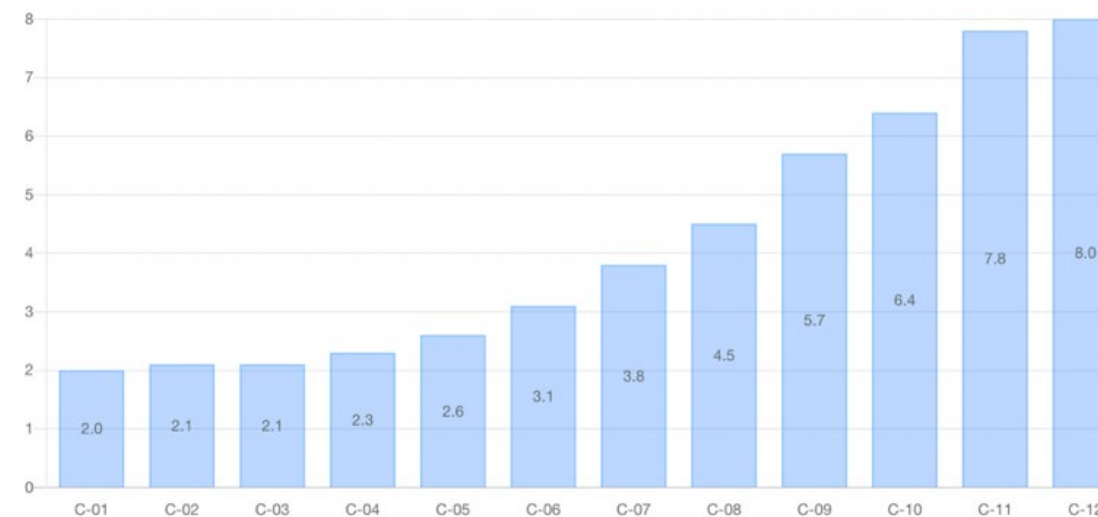
Evoluzione del rischio ⓘ



Click Rate con Difficoltà Media ⓘ



Reliability Score ⓘ



Report Phishing



CARATTERISTICHE CON MS365



- Utilizza il pulsante **"Segnala phishing"** già presente nel client di posta elettronica.
- Non è necessaria l'installazione di plugin di terze. Il **plugin MS è incluso nel pacchetto**. E mantenuto da Microsoft ed è integrato nelle procedure di installazione di Microsoft 365.
- Facile da usare per i SOC. Regole Power Automate configurabili per gestire automaticamente i tentativi di phishing simulato inviati al SOC.



CARATTERISTICHE CON GMAIL



- Script per aggiungere un pulsante "Segnala Phishing". Completamente personalizzabile (icona, nome, tooltip).
- Compatibile con il SOC. Pulsante configurabile per instradare automaticamente le mail di phishing simulato segnalate dagli utenti.



ADDESTRAMENTO ESPERIENZIALE EFFICACE

- ALLENAMENTO CONTINUATIVO
- ERRORE > FORMAZIONE Istantanea
- POLITICHE DI REMEDIATION
- PROCEDURA DI SEGNALAZIONE



ALLENAMENTO PERSONALIZZATO

- PROCESSO ADATTIVO
- SIMULAZIONI PERSONALIZZATE
- GRUPPI DI RISCHIO
- LIVELLI DI DIFFICOLTÀ



SUPERVISIONE A IMPATTO ZERO

- PIATTAFORMA IN SaaS
- SERVIZIO CHIAVI IN MANO
- CAMPAGNE AUTOMATIZZATE
- TEMPLATE PRE-CARICATI
- REPORTISTICA ANALITICA E MANAGERIALE

PhishPro Add-on

PhishPro

3 Nuove funzionalità



ATTACCO USB

Effettuare simulazioni di attacco phishing attraverso l'utilizzo di chiavette USB.



ATTACCO QR CODE

Effettuare simulazioni di attacco phishing attraverso l'utilizzo di QR Code.



ADAPTIVE LEARNING REMEDIATION

Effettuare delle azioni di Remediation **Adattivo**: offrendo agli utenti dei contenuti didattici dedicati.

Attacco USB

Obiettivo

Effettuare simulazioni di attacco phishing attraverso l'utilizzo di chiavette USB

Caratteristiche:

- I supervisori potranno ampliare l'addestramento anti-phishing attraverso la creazione di una chiavetta USB contenente un file doc "malevolo"
- Ogni apertura del file doc andrà ad alimentare un report presente nella Dashboard di Remediation, dove apparirà il numero di volte che il doc è stato aperto.
- L'esecuzione della macro di Word attiverà la cattura del nome dell'Host (verrà registrato il fatto che l'utente oltre a inserire la chiavetta USB nel dispositivo, ha anche accettato di eseguire la macro, quindi un'ulteriore esposizione al rischio cyber con un'azione particolarmente pericolosa per la sicurezza).



Attacco QRcode

Obiettivo:

Effettuare simulazioni di attacco phishing attraverso l'utilizzo di QR Code

Caratteristiche:

- I supervisor potranno ampliare l'addestramento anti-phishing attraverso la creazione di codici QR "malevoli".
- I QR Code saranno stampati e distribuiti all'interno dell'organizzazione.
- Le persone che effettueranno la scansione e accetteranno di aprire il link presente nel QR Code saranno reindirizzate a una landing page dedicata dove verrà chiesto loro di fornire informazioni sensibili come ad esempio il nome e l'email.
- Ogni QR Code scansionato andrà ad alimentare un report presente nella Dashboard di Remediation, dove verranno evidenziate le scansioni e chi ha inviato le ulteriori informazioni richieste.



Adaptive Learning Remediation

Obiettivo:

Effettuare delle azioni di Remediation adattivo: offrendo agli utenti che necessitano dei contenuti didattici dedicati e finalizzati al riconoscimento della minaccia.

Caratteristiche:

I supervisor potranno dalla Dashboard di Remediation assegnare dei contenuti dedicati a quella tipologia di utenti definiti "weak" o che soddisfano criteri simili, per fornire una formazione specifica e finalizzata al riconoscimento delle minacce di phishing.



Servizio chiavi in mano

- ▶ **Completo**
- ▶ **Scalabile**
- ▶ **Efficace**
- ▶ **Multilingua**
- ▶ **Adattivo (AI)**
- ▶ **Automatizzato (impatto zero)**
- ▶ **Erogato in SaaS**

Customer Success Team

Un servizio che va oltre la normale logica del supporto alla piattaforma, pensato per **accompagnare il cliente** verso il raggiungimento dei **risultati formativi** che sono alla base di un progetto di CSA



ON-BOARDING

Tenendo conto delle esigenze di IT/SEC, Human Resources & Internal Communication



PROGRAM CARING

Con l'obiettivo di aumentare l'efficacia del programma e ridurre l'impatto su chi lo governa



PERIODIC CHECKS

Con un'analisi condivisa degli indicatori di partecipazione, come base per decidere eventuali azioni

Customer Success Team

Cosa offriamo



PACCHETTO CST

- Incontro di avvio dell'onboarding (kick off meeting)
- Supporto per la verifica e caricamento della prima lista utenti
- Supporto all'implementazione della whitelist
- Supporto alla comunicazione interna
- Analisi della formazione e raccomandazioni - Mid Term SAL



KNOWLEDGE BASE (DOCUMENTAZIONE)

- Onboarding
- Prodotto
- Tecnica



CST MANAGER DEDICATO

Durante tutto il ciclo di vita del servizio



HELPDESK

Durante tutto il ciclo di vita del servizio
support@cyberguru.eu

Customer Success Team

CST Package per numero di licenze

SIZE	XS	S	M	L	XL
CST PACK (H)	8	16	24	48	56

- Pacchetto licenze
- Documentazione progetto
- Helpdesk
- Customer Management Service (Pacchetto CST)
- Rendicontazione periodica del Pacchetto Ore CST

LEGENDA	XS Users \leq 250	M 1001 < Users \leq 3000	XL Users > 10000
	S 251 < Users \leq 1000	L 3001 < Users \leq 10000	

Perché Cyber Guru

- ▶ Metodologia orientata al **risultato**
- ▶ Formazione **permanente**
- ▶ **Formazione – addestramento – allenamento**
- ▶ **Adattività** dei programmi
- ▶ **Automazione** (impatto zero)
- ▶ Coinvolgimento del **discente**
- ▶ Customer Success Management



SECURITY AWARENESS TRAINING THAT WORKS!

Grazie

www.cyberguru.io