



# Cyber Guru Enterprise

**Procedura di onboarding**

**Come trasformare dipendenti e collaboratori  
nella prima linea di difesa dell'organizzazione**

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

# Overview CG Awareness School

- Phishing
- Password
- Social media
- Privacy & GDPR
- Mobile Device & APP
- Fake News
- USB Device
- Email Security
- Malware & Ransomware
- Web Browsing
- Critical Scenarios
- Social Engineering
- Clean Desk
- Smart working
- Social collaboration e video conferencing
- Smishing & Vishing
- Spear Phishing
- Ransomware
- Multi-factor authentication
- IoT Device
- Bluetooth & WIFI
- Information Classification
- Data Protection
- Social Engineering 2
- Real Scam
- Phone Scam
- Social & Cyberbullying
- Privacy
- Legal Aspect
- Physical Security
- E-commerce
- Holiday & Business trip
- Cyber Hygiene
- Backup & Restore
- Best practice
- Social Engineering 3



**50 DOMANDE**  
superamento  
certificazione con  
il 60% di risposte  
esatte



**CAMPUS**  
Aggiornamento e  
mantenimento  
conoscenza

**CGA livello 1**  
1<sup>a</sup> annualità

**CGA livello 2**  
2<sup>a</sup> annualità

**CGA livello 3**  
3<sup>a</sup> annualità

**Certificazione**

**Campus**

# Overview CG Awareness - School

Awareness 

## Articolazione singole annualità

### 12 MODULI

Lo sblocco standard dei moduli è: **un modulo al mese** nel corso dell'annualità; il modulo è fruibile in formato lezione video o pdf

### 36 LEZIONI

Ogni modulo è composto da 3 lezioni della durata di 5-7 minuti ciascuna

### 36 TEST DI APPRENDIMENTO

Dopo ogni lezione un test, superabile con 3 risposte esatte su 4 per accedere alla lezione successiva, ripetibile

### 4 TEST DI CONSOLIDAMENTO

Ogni 3 moduli un test, superabile con 10 risposte esatte su 10, non ripetibile; il risultato non preclude l'accesso al modulo successivo

### 1 ATTESTATO PARTECIPAZIONE

Al completamento dei moduli per ogni annualità, l'utente può scaricare l'attestato



#### Gamification

La **medaglia** si ottiene superando i test di fine lezione <4 risposte esatte su 4>  
La **coppa** si ottiene superando il test dopo ogni 3 moduli < 10 risposte esatte su 10>



#### Contenuti extra in piattaforma:

Micro-pillole (video)



#### Sezioni speciali:

Area Interna

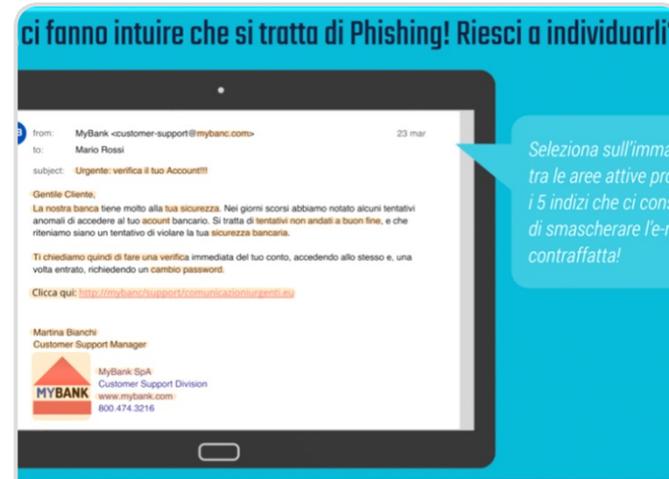
# Campus - Maintenance & Update



## Lifelong Learning



Warm-Up



DidActive



Serious Game



Cyber Insights

MANTENIMENTO

AGGIORNAMENTO

# Overview CG Awareness - Campus



- Context
- Clean & Secure
- E-Commerce
- Cyber Hygiene
- Backup
- Travel
- Mobile
- Email Investigate
- Phishing recap
- Malware recap
- Email Investigate
- Personal data
- Ramsonware
- Password Recap
- Social Media
- Social Engineering
- Una trasferta difficile
- La congiura di Kalasya
- Rischi tutto cyber
- L'arte dell'inganno
- SMS Spoofing
- Password Manager
- Juice Jacking
- Keylogger
- Testimonial Inconsapevoli (AI)
- Deep Fake (AI)
- Riservatezza a rischio (AI)
- Attacchi mirati (AI)

WARM UP

DIDACTIVE

SERIOUS GAME

CYBER INSIGHTS

# Overview CG Awareness - Campus Awareness

## Articolazione singola annualità

### 8 WARM UP

Learning Object situazionali che includono 5 interazioni per ognuna delle quali si ottengono feedback e «scudi» per le seguenti condizioni: interazione corretta, parzialmente corretta o errata.

### 8 DIDACTIVE

Learning Object didattici che includono 5 interazioni per ognuna delle quali si ottengono feedback e «scudi» per le seguenti condizioni: interazione corretta, parzialmente corretta o errata.

### 8 CYBER INSIGHTS

Sessioni di aggiornamento dedicate ad un singolo argomento, costituite da una video-pillola e da un test di quattro domande.

### 4 SERIOUS GAMES

Ogni 3 viene proposto un «gioco serio» interattivo che usa la tecnica del «game-based learning» per sviluppare apprendimento rispetto alle tematiche della Cybersecurity.

### 1 ATTESTATO PARTECIPAZIONE

Al completamento dei moduli per ogni annualità, l'utente può scaricare l'attestato



#### Gamification

La medaglia si ottiene superando in modo eccellente tutte le interazioniLea



#### Contenuti extra in piattaforma:

Micro-pillole (video)



#### Sezioni speciali:

Area Interna

# Overview CG Channel

## CGC Episodi

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

### CGC livello 1 - 1ª Stagione

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

### CGC livello 2 - 2ª Stagione

- CEO FRAUD - Sottili Connessioni
- CREDENTIAL STUFFING - Una verità scomoda
- PASSWORD SECURITY - Nessuna alternativa
- EMAIL SPOOFING - Effetto domino
- SPEAR PHISHING - Il diavolo è nei dettagli
- PRIVACY - Selfie galeotto
- SIM SWAP - Il gatto e la volpe 2.0
- WATERING HOLE - Il leone e la gazzella
- PUBLIC WIFI - Il pesce nella rete
- USB DEVICE - Chiavetta USB letale
- KEYLOGGER - Un nemico invisibile
- CYBERSECURITY - Il colpevole

### CGC livello 3 - 3ª Stagione

# Overview CG Channel

## Articolazione annualità



### 12 EPISODI

Lo sblocco standard degli episodi del Channel è: **un episodio al mese** nel corso dell'annualità; una volta rilasciati, gli episodi sono sempre visibili in piattaforma.

### STORYTELLING

Gli episodi sono caratterizzati da un **storytelling accattivante**, che cattura lo spettatore e lo immerge nei contenuti al pari delle serie televisive.

### DURATA EPISODI

**La durata** dei singoli episodi è circoscritta e ricalca lo stesso approccio della durata delle video-lezioni del Programma Awareness; in media sono episodi di circa 5 minuti.

### ACCESSO AL CHANNEL

**L'accesso** è consentito attraverso l'interfaccia della piattaforma condivisa con il Programma Awareness

# Processo Onboarding

## Aspetti Contrattuali



### ATTIVAZIONE SERVIZIO VALIDITÀ LICENZE

Il referente riceve le credenziali di primo accesso al portale di onboarding Cyber Guru

**Le licenze sono valide dal giorno dell' attivazione servizio fino alla scadenza contrattuale**



### ACCETTAZIONE T&C

Accesso al portale di onboarding e accettazione delle T&C

- **EULA**
- **Nomina responsabile trattamento dati**
- **Privacy policy**



### KNOWLEDGE BASE DOCUMENTAZIONE

All'interno del repository condiviso sarà possibile accedere e scaricare la documentazione di processo e di prodotto, caricare loghi e lista utenti necessari per il GO LIVE

# Processo Onboarding

## Aspetti Operativi



### USER LIST Lista Utenti

Lista degli utenti che andranno a fruire del servizio



### PERSONALIZZAZIONE Loghi ad alta risoluzione

Personalizzazione della piattaforma con loghi del Cliente



### WHITELISTING Test tecnico

Valutare la piena fruibilità della piattaforma



### ANNUNCIO PROGRAMMA Comunicazione interna

Piano di comunicazione per avvio e mantenimento della fruizione



### AVVIO PROGRAMMA Go Live

GO LIVE del programma e inizio formazione

OWNER

CLIENTE

CLIENTE

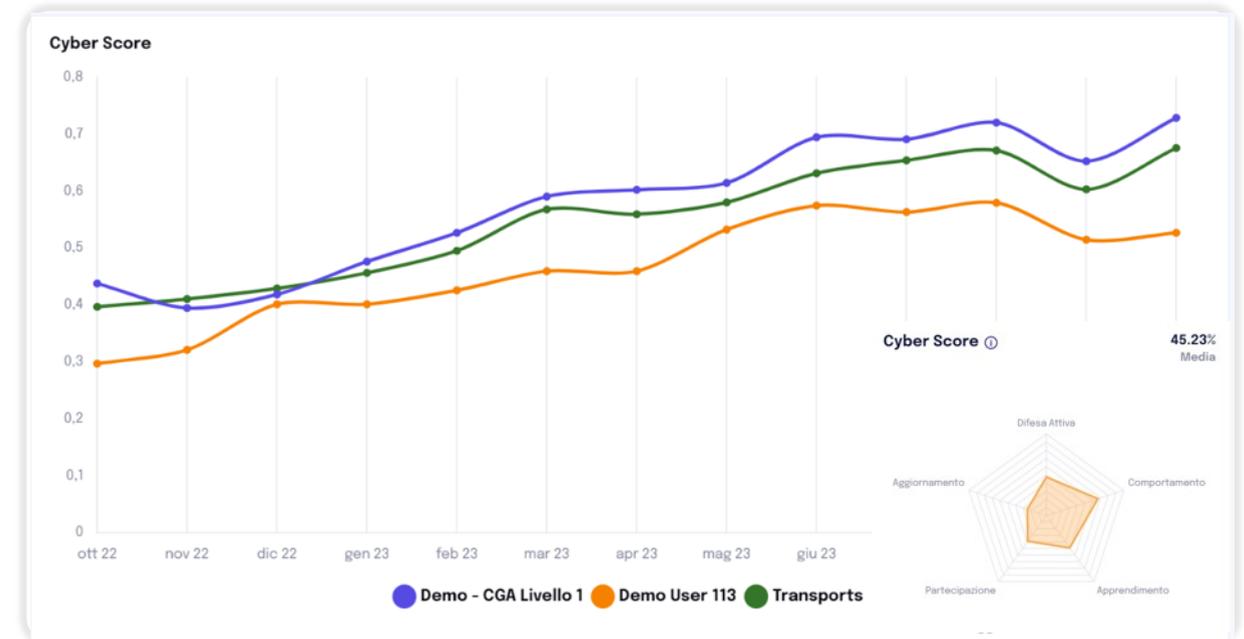
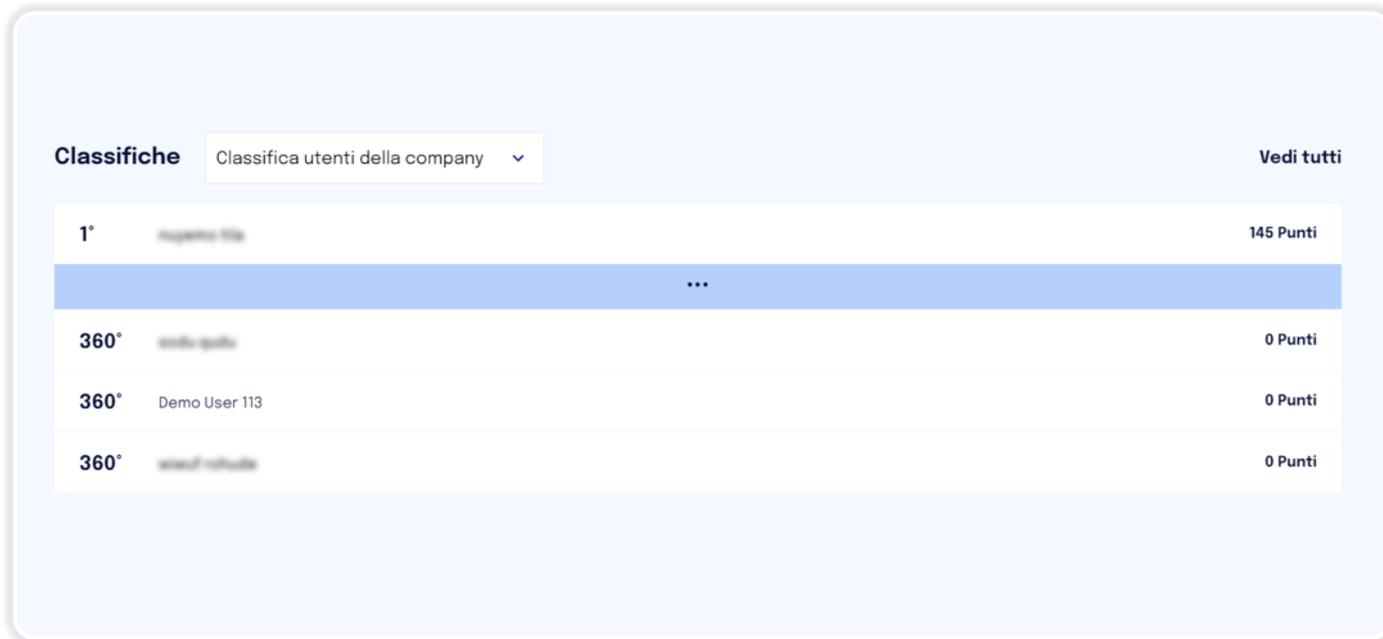
CLIENTE

CLIENTE

CYBER GURU

SUPPORTO CYBER GURU

# Gamification



## GAMIFICATION A SQUADRE (Fortemente consigliata)



User Engagement



Reward



Achievement

## GAMIFICATION INDIVIDUALE



Motivation



Learning



Challenge

# Student Caring



**Comunicazione interna a cura del Cliente**



**Notifica di GO LIVE** (post comunicazione interna)



**Notifica per il rilascio del nuovo modulo**



**Invio email massive** da parte del team leader e/o supervisore direttamente dalla piattaforma (ad esempio solleciti)



**Ciao Asia,**

di seguito trovi le credenziali per l'accesso:

**Username:**

[asia.jannetti@cyberguru.eu](mailto:asia.jannetti@cyberguru.eu)

**Password temporanea:**

K,yUR2TLdy

Ti ricordiamo che al primo accesso è necessario sostituire la password temporanea con una password scelta per la piattaforma.

**Accedi alla piattaforma**

# Template User List

COMMON				AWARENESS/CHANNEL			PHISHING						POST GO LIVE (USER LIST UPDATE)				
Email	firstname	lastname	username	Team	lang	cgrole	Org_1	Org_2	Org_3	Org_4	Org_5	Org_6	Country*	To modify	To delete	To suspend	To add
john.smith@company.com	John	Smith	John.Smith	Red Team	it	Studente	Red Team	Marketing	CFO	Dirigente	Lazio	Rome	IT	modify			
mario.rossi@company.com	Mario	Rossi	Mario.Rossi	Blue Team	it	Studente	Blue Team	Sales	CEO	Dirigente	Lazio	Rome	IT				add
marco.lucini@company.com	Marco	Lucini	Marco.Lucini	Red Team	en	Supervisore Azienda	Red Team	Production	Inbound	Impiegato	England	London	UK				
bill.gates@company.com	Bill	Gates	Bill.Gates	Red Team	de	Team Leader	Red Team	Research & Development	Developer	Quadro	Illinois	Chicago	US	modify			
elon.musk@company.com	Elon	Musk	Elon.Musk	Yellow Team	fr	Studente	Yellow Team	Research & Development	Developer	Quadro	Catalogna	Barcelons	ES		delete		
warren.buffer@company.com	Warren	Buffer	Warren.Buffer	Yellow Team	es	Studente	Yellow Team	Administration	Junior Developer	Impiegato	Lombardia	Milan	IT			suspend	



**LEGENDA CGROLE:**

- **STUDENTE:** UTENTE SEMPLICE CHE SEGUE IL CORSO ED HA LA POSSIBILITA' DI MONITORARE IL PROPRIO ANDAMENTO
- **RESPONSABILE TEAM:** TEAM LEADER HA UN RUOLO DI MOTIVATORE ED E' UN RUOLO FONDAMENTALE IN CASO DI IMPLEMENTAZIONE DEI MECCANISMI DI GAMIFICATION. UN SOLO TEAM LEADER PER TEAM.
- **SUPERVISORE AZIENDA:** HA ACCESSO ALLA REPORTISTICA SULL' ANDAMENTO DEL CORSO, PER TUTTA LA POPOLAZIONE AZIENDALE, SIA IN MODO AGGREGATO CHE DI DETTAGLIO

**LE ORG SI POSSONO DEFINIRE IN DIVERSI MODI, PER ESEMPIO:**

- DEFINIRE I TEAM UTILIZZATI PER CYBER GURU AWARENESS AL FINE DI OTTENERE UNA RAPIDA CORRELAZIONE TRA LA FREQUENZA ALLA FORMAZIONE E IL TASSO DI CLICK SUL PHISHING
- AREA GEOGRAFICA
- FUNZIONE ORGANIZZATIVA
- RUOLO AZIENDALE
- FASCIA D'ETA'

LA DEFINIZIONE DI QUESTI CAMPI DA' LA POSSIBILITÀ DI MAPPARE IL RISCHIO DELLA TUA AZIENDA SEGMENTANDO LA POPOLAZIONE CON CRITERI DIVERSI

**I CAMPI :**

To MODIFY  
To DELETE  
To SUSPEND  
To ADD

INDICANO L'AZIONE DA EFFETTUARE SULL'UTENTE. SOLO UNO DEI CAMPI INDICATI PUO' ESSERE VALORIZZATO.

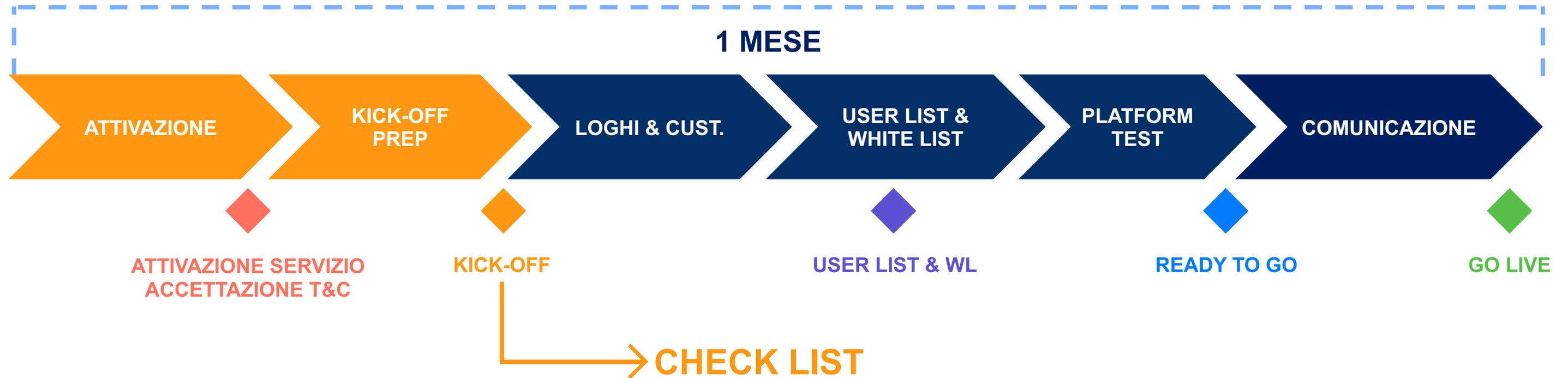
# Master Plan



**Il servizio è attivo dalla data di comunicazione di attivazione del servizio** (indipendentemente dal Go Live).

Al fine di mantenere un carico cognitivo adeguato e un apprendimento efficace, si consiglia un onboarding entro il mese dalla attivazione del servizio. Ritardi nel Go Live impongono una pianificazione dei rilasci che possono inficiare sull'efficacia del percorso formativo.

# OnBoarding: checklist



✓ **Referenti durante l'onboarding** e accesso al repository documentale e follow up

✓ **Nominativi** per accesso alla piattaforma come supervisor

✓ **Statistiche di dettaglio** con nominativi in chiaro

✓ **Sottodominio cliente** per creazione Tenant dedicato

✓ **Lingue richieste**

✓ **Gamification (fortemente consigliata)**

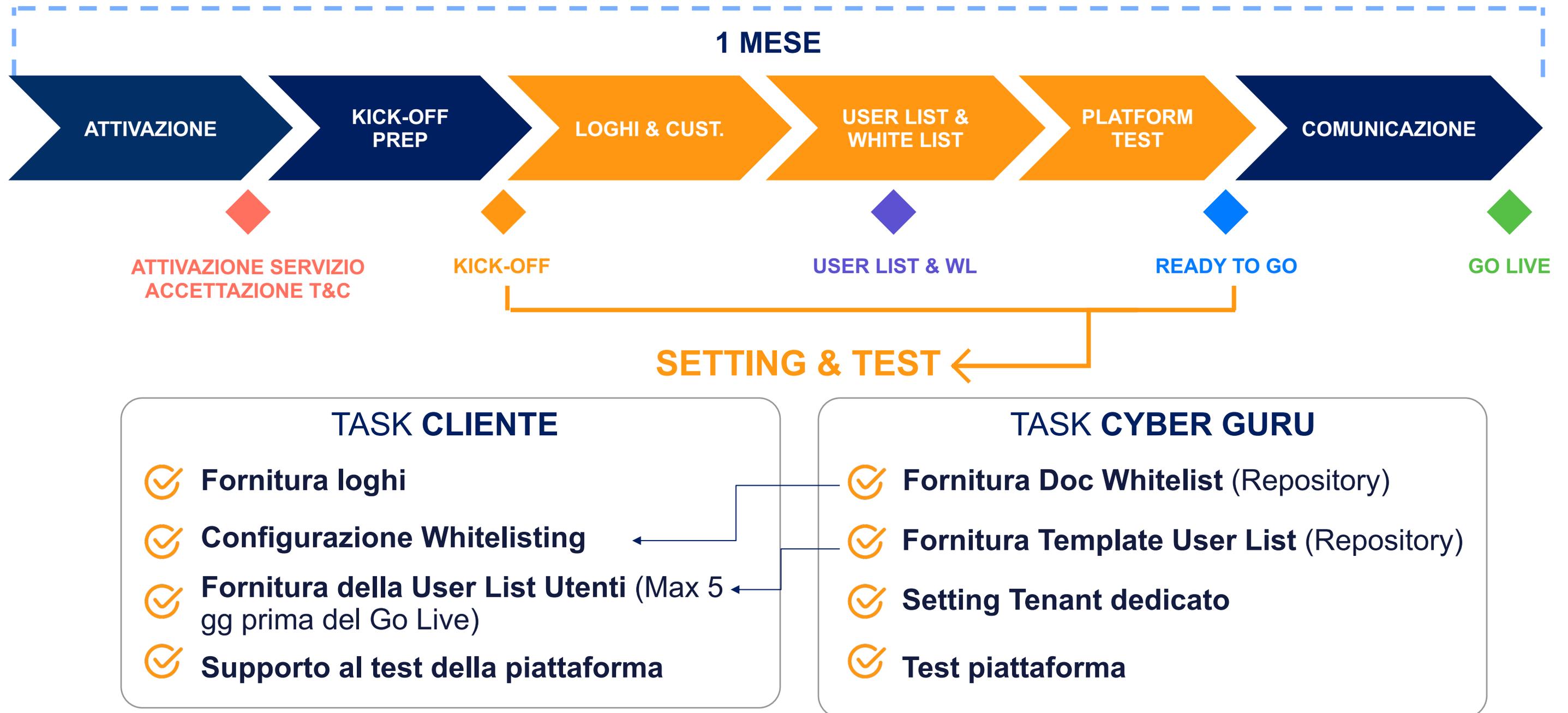
✓ Video a fruizione controllata con blocco barra di avanzamento

✓ Chiusura classifica (per livello/annualità o a chiusura di tutte le annualità)

✓ Data Go Live

✓ Pianificazione rilasci entro la data di scadenza licenze

# OnBoarding: checklist



# OnBoarding: GO LIVE



## TASK CLIENTE

- ✔ Comunicazione interna di **avvio** programma
- ✔ Caricamento **User List** in piattaforma

## TASK CYBER GURU

- ✔ Go Live

# Fruizione Training



GO LIVE

FINE SERVIZIO



## HELPDESK PER GLI UTENTI

[support@cyberguru.eu](mailto:support@cyberguru.eu)



## REPORTISTICA

La reportistica è standard come da piattaforma



## AGGIORNAMENTO USER LIST

Da consegnare con formato standard entro **5 giorni lavorativi** prima del Go Live



## FOLLOW UP

Follow up meeting



## GO LIVE

Le date di Go Live e relativi rilasci successivi devono essere pianificati almeno 5 giorni lavorativi prima della data



# Cyber Guru Phishing

Procedura di onboarding

**Come trasformare dipendenti e collaboratori  
nella prima linea di difesa dell'organizzazione**

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

# Overview CG Phishing

## Articolazione annualità

### 12 CAMPAGNE

Ogni campagna è composta da **10 template**; con le prime 3 campagne il motore di A.I. studia il comportamento del singolo destinatario per calibrare il livello degli invii successivi.

### 3-4 SETTIMANE

La **durata standard** della singola campagna è di 3-4 settimane

### INVIO CAMPAGNA

L'invio dei template è randomico per orario di invio, tipologia template inviato, utenti colpiti.

### DASHBOARD & ANALYTICS

La **Dashboard** disponibile in piattaforma evidenzia l'andamento delle campagne, la distribuzione degli weak/strong users per singola campagna, e numerose altre metriche.

### REMEDIATION

Sulla base di quanto emerge dalle statistiche, si può decidere di avviare campagne mirate su cluster di utenti o singoli utenti per rafforzare il livello di resistenza agli attacchi. Si consigliano un paio di **remediation** dopo **7/8 campagne**.

## Tipologia utenti:



#### Weak user:

Sono gli utenti che sono portati ad aprire le mail e cliccare sui link regolarmente



#### Strong user:

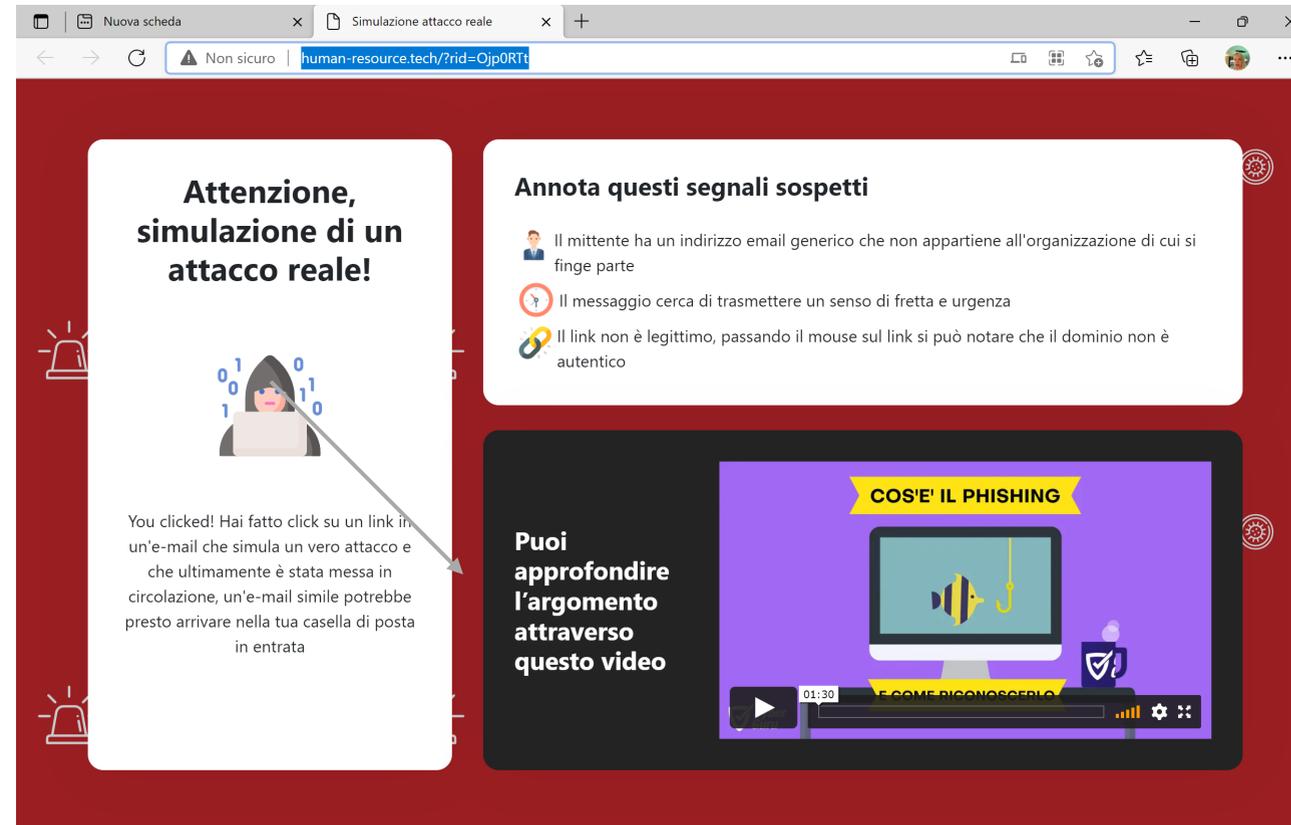
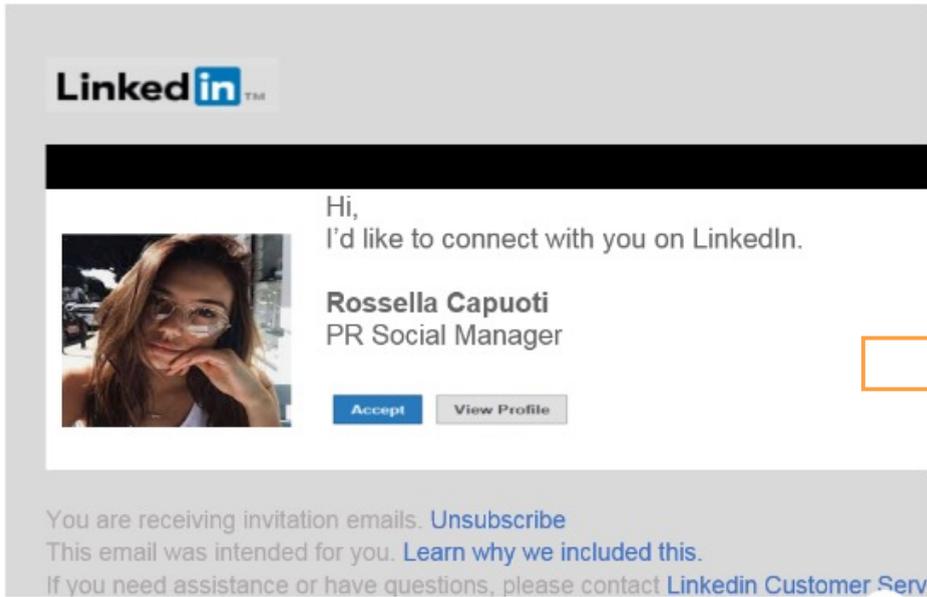
Sono gli utenti che possono aprire le mail ma non cliccano sui link



#### Defender:

Sono gli utenti che non solo non cadono nell'inganno ma segnalano il phishing attraverso la procedura prevista

# Overview CG Phishing



Nuova scheda x Simulazione attacco reale x +

Non sicuro | human-resource.tech/?rid=Ojpp0RTI

### Attenzione, simulazione di un attacco reale!

You clicked! Hai fatto click su un link in un'e-mail che simula un vero attacco e che ultimamente è stata messa in circolazione, un'e-mail simile potrebbe presto arrivare nella tua casella di posta in entrata

### Annota questi segnali sospetti

- Il mittente ha un indirizzo email generico che non appartiene all'organizzazione di cui si finge parte
- Il messaggio cerca di trasmettere un senso di fretta e urgenza
- Il link non è legittimo, passando il mouse sul link si può notare che il dominio non è autentico

### Puoi approfondire l'argomento attraverso questo video

**COS'E' IL PHISHING**

01:30

**Il click sul link** presente nella mail di phishing visualizza una pagina con contenuti informativi dei segnali che avrebbero dovuto essere notati e un video formativo.

# Processo Onboarding

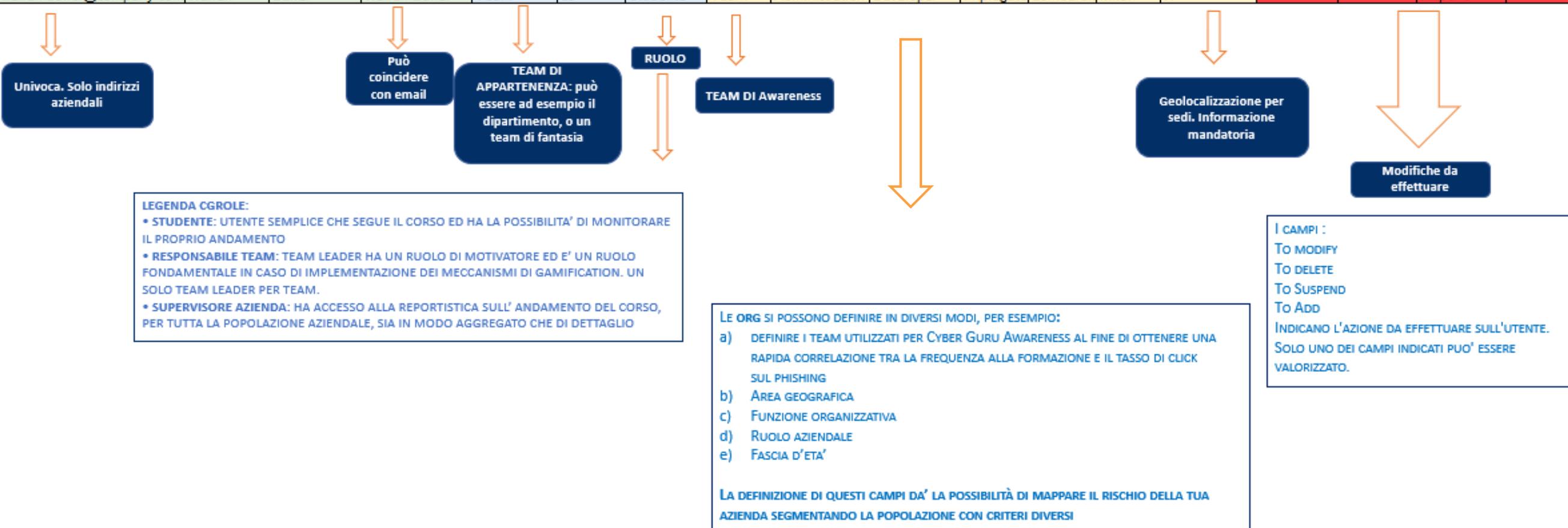
## Aspetti Operativi



OWNER

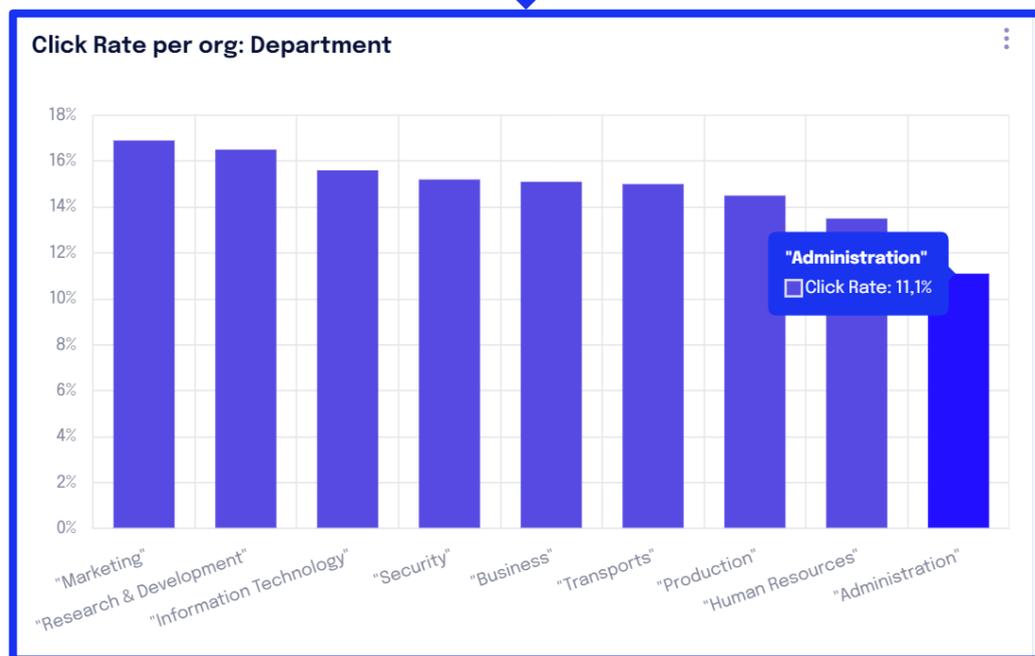
# Template User List

COMMON			AWARENESS/CHANNEL			PHISHING						POST GO LIVE (USER LIST UPDATE)					
Email	firstname	lastname	username	Team	lang	cgrole	Org_1	Org_2	Org_3	Org_4	Org_5	Org_6	Country*	To modify	To delete	To suspend	To add
john.smith@company.com	John	Smith	John.Smith	Red Team	it	Studente	Red Team	Marketing	CFO	Dirigente	Lazio	Rome	IT	modify			
mario.rossi@company.com	Mario	Rossi	Mario.Rossi	Blue Team	it	Studente	Blue Team	Sales	CEO	Dirigente	Lazio	Rome	IT				add
marco.lucini@company.com	Marco	Lucini	Marco.Lucini	Red Team	en	Supervisore Azienda	Red Team	Production	Inbound	Impiegato	England	London	UK				
bill.gates@company.com	Bill	Gates	Bill.Gates	Red Team	de	Team Leader	Red Team	Research & Development	Developer	Quadro	Illinois	Chicago	US	modify			
elon.musk@company.com	Elon	Musk	Elon.Musk	Yellow Team	fr	Studente	Yellow Team	Research & Development	Developer	Quadro	Catalogne	Barcelona	ES		delete		
warren.buffer@company.com	Warren	Buffer	Warren.Buffer	Yellow Team	es	Studente	Yellow Team	Administration	Junior Developer	Impiegato	Lombardia	Milan	IT			suspend	



# Mappatura rischi aziendali per Org

COMMON				AWARENESS/CHANNEL			PHISHING							POST GO LIVE (USER LIST UPDATE)			
Email	firstname	lastname	username	Team	lang	cgrole	Org_1	Org_2	Org_3	Org_4	Org_5	Org_6	COUNTRY*	To modify	To delete	To suspend	To add
<a href="mailto:John.Smith@company.com">John.Smith@company.com</a>	John	Smith	John.Smith	Red Team	it	Studente	Red Team	Marketing	CFO	Dirigente	Lazio	Rome	IT	modify			
<a href="mailto:Mario.rossi@company.com">Mario.rossi@company.com</a>	Mario	Rossi	Mario.Rossi	Blue Team	it	Studente	Blue Team	Sales	CEO	Dirigente	Lazio	Rome	IT				add
<a href="mailto:Marco.lucini@company.com">Marco.lucini@company.com</a>	Marco	Lucini	Marco.Lucini	Red Team	en	Supervisore Azienda	Red Team	Production	Inbound	Impiegato	England	London	UK				
<a href="mailto:Bill.Gates@company.com">Bill.Gates@company.com</a>	Bill	Gates	Bill.Gates	Red Team	de	Team Leader	Red Team	Research & Development	Developer	Quadro	Illinois	Chicago	US	modify			
<a href="mailto:Elon.Musk@company.com">Elon.Musk@company.com</a>	Elon	Musk	Elon.Musk	Yellow Team	fr	Studente	Yellow Team	Research & Development	Developer	Quadro	Catalogna	Barcelon	ES		delete		
<a href="mailto:Warren.buffer@company.com">Warren.buffer@company.com</a>	Warren	Buffer	Warren.Buffer	Yellow Team	es	Studente	Yellow Team	Administration	Junior Developer	Impiegato	Lombardi	Milan	IT			suspend	



# Master Plan



**Il servizio è attivo dalla data di comunicazione di attivazione del servizio** (indipendentemente dal Go Live).

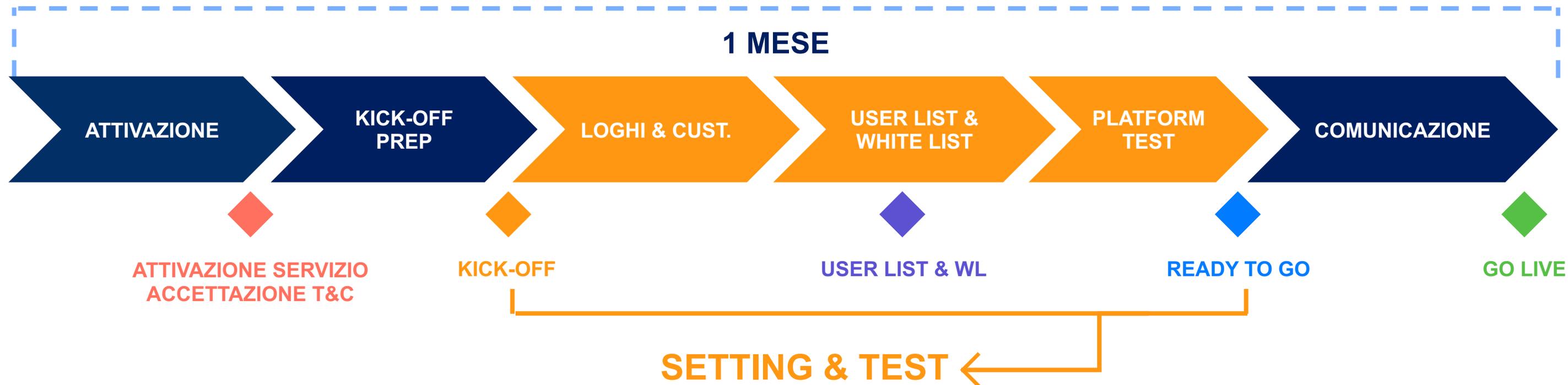
Al fine di mantenere un carico cognitivo adeguato e un apprendimento efficace, si consiglia un onboarding entro il mese dalla attivazione del servizio.

# OnBoarding: checklist



- ✓ **Referenti durante l'onboarding** e accesso al repository documentale e follow up
- ✓ **Nominativi** per accesso alla piattaforma come supervisor
- ✓ **Statistiche di dettaglio** con nominativi in chiaro
- ✓ **Dominio Email** per creazione Tenant dedicato
- ✓ **Lingue e country richiesti**
- ✓ **Data Go Live**
- ✓ **Pianificazione rilasci** entro la data di scadenza licenze

# OnBoarding: setting e test



## TASK CLIENTE

- ✓ Fornitura logo
- ✓ Configurazione Whitelisting
- ✓ Preparazione e consolidamento della User List Utenti (Max 5 gg prima del Go Live)
- ✓ Supporto al test della piattaforma

## TASK CYBER GURU

- ✓ Fornitura Doc Whitelist (Repository)
- ✓ Fornitura Template User List (Repository)
- ✓ Setting Tenant dedicato
- ✓ Test piattaforma

# OnBoarding: GO LIVE



## TASK CLIENTE

- ✓ Approvazione campagne di Baseline
- ✓ Caricamento **User List** in piattaforma

## TASK CYBER GURU

- ✓ Go Live

# Erogazione campagne phishing





**Cyber  
Guru**

# PhishPro



## 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 REMEDICATION

Effettuare delle **azioni di Remediation Adattiva**: 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

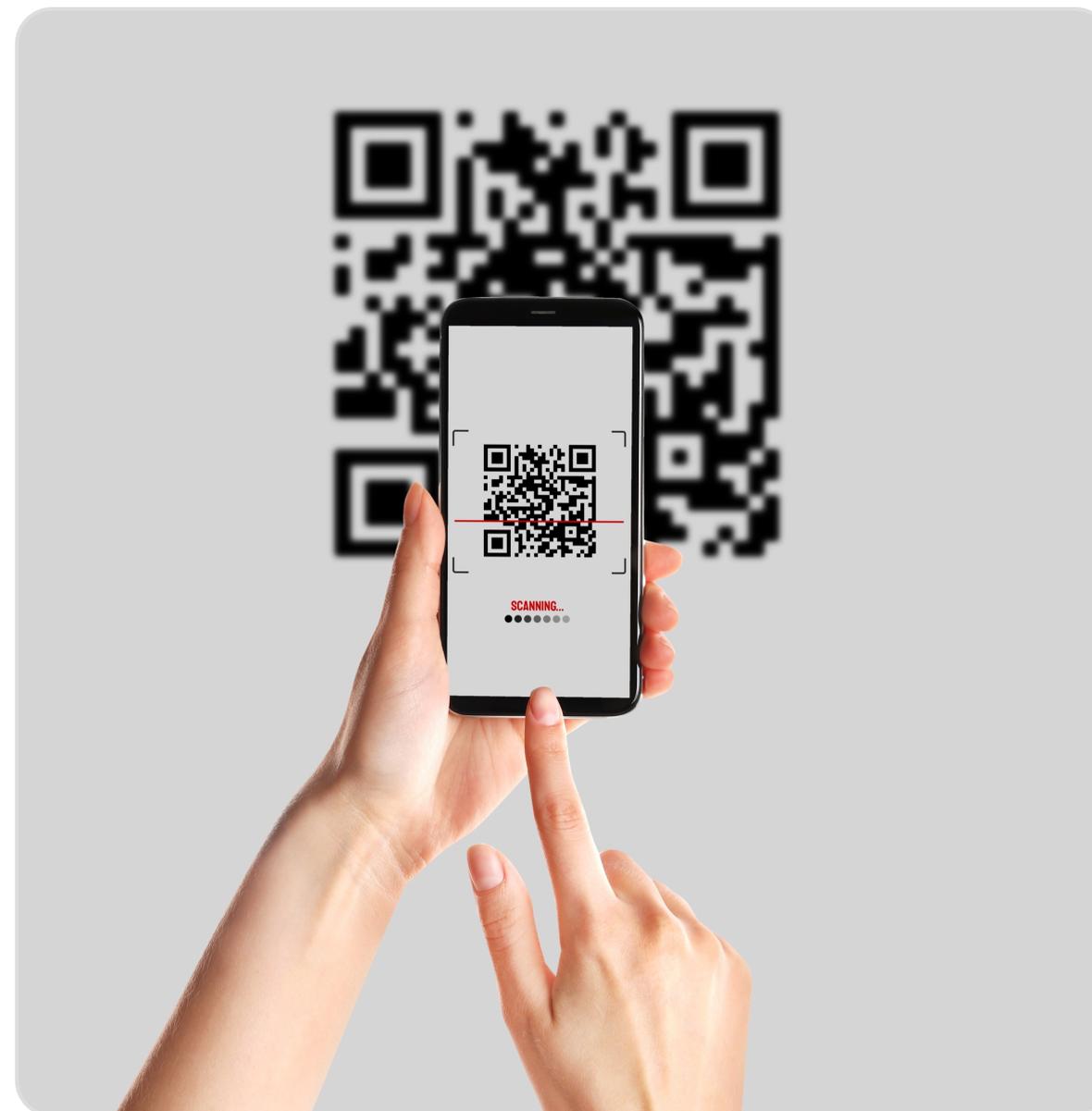


## Obiettivo:

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

## Caratteristiche:

- I supervisori 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 adattiva: 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.



# OnBoarding Phishpro



## Stesso onboarding di Phishing

Le funzionalità di PhishPro si presentano come 3 nuove «Remediation»

<p><b>Attacchi QR Code</b> <span>Inizia...</span></p>  <p>Configura i parametri della campagna e ricevi via email il QR code di attacco.</p>	<p><b>Attacchi USB</b> <span>Inizia...</span></p>  <p>Configura i parametri della campagna e ricevi via email l'attachment per i tuoi attacchi USB</p>
<p><b>Remediation Adattiva</b> <span>Inizia...</span></p>  <p>Assegna via email contenuti formativi dedicati e aggiuntivi agli studenti "a rischio" in base ai loro risultati sulle campagne di phishing</p>	

# 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
- Rendicontazione periodica del bundle ore allocate

LEGENDA

**XS** Users  $\leq$  250

**S** 251 < Users  $\leq$  1000

**M** 1001 < Users  $\leq$  3000

**L** 3001 < Users  $\leq$  10000

**XL** Users > 10000



SECURITY AWARENESS TRAINING THAT WORKS!

**Grazie**

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