SMARTFENSE

DATABOOK

Indice

SMARTFENSE è la piattaforma online premiata a livello internazionale per la Cyber Security Awareness per la consapevolezza e la promozione di abitudini sicure negli utenti.

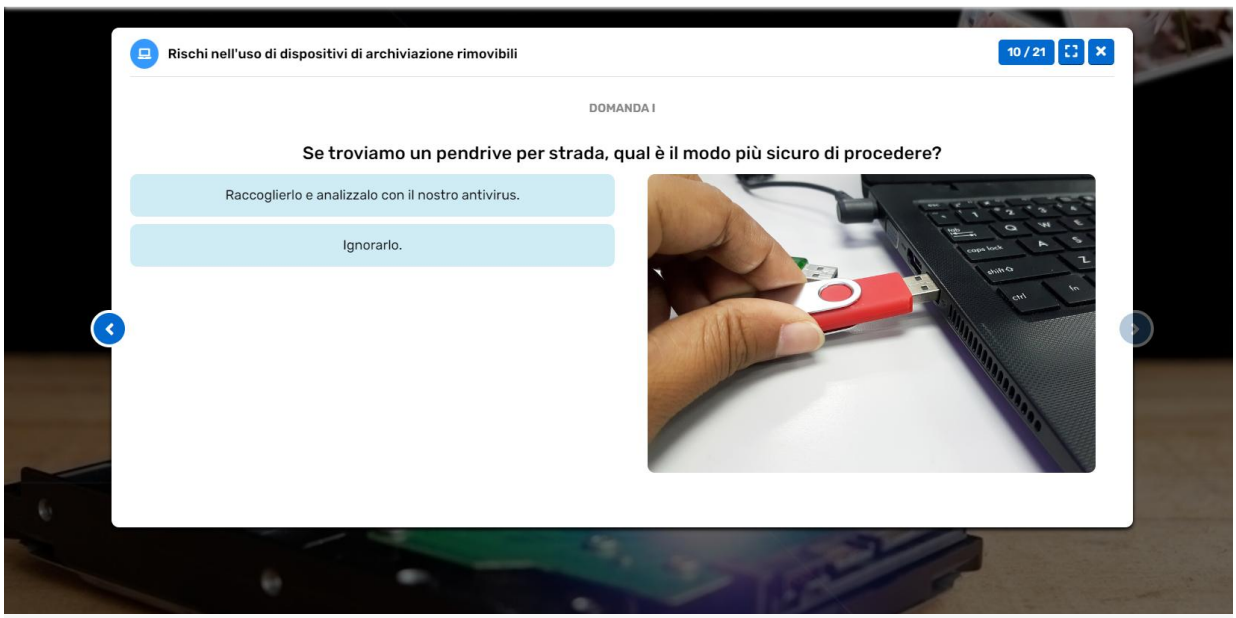
Applicando le ultime tendenze tecnologiche e le migliori pratiche pedagogiche nell'e-learning e nella gamification, i contenuti vengono presentati agli utenti in modo piacevole e interattivo al fine di ottenere un reale e duraturo cambiamento di comportamento.

1. Componenti

1.1. Strumenti di Awareness

1.1.1. Moduli interattivi

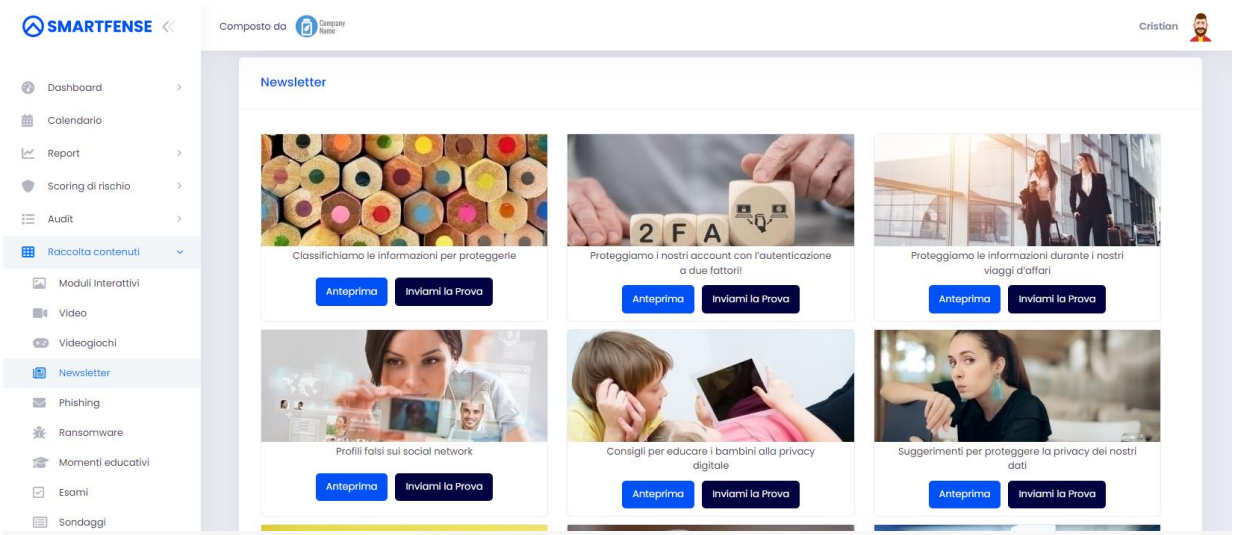
I Moduli Interattivi presentano diversi argomenti che combinano attività interattive, contenuti multimediali e GBL (Game-Based Learning). Ciò consente agli utenti di assimilare in modo fluido e piacevole i vari argomenti di sensibilizzazione.



Moduli Interattivi

1.1.2. Newsletter

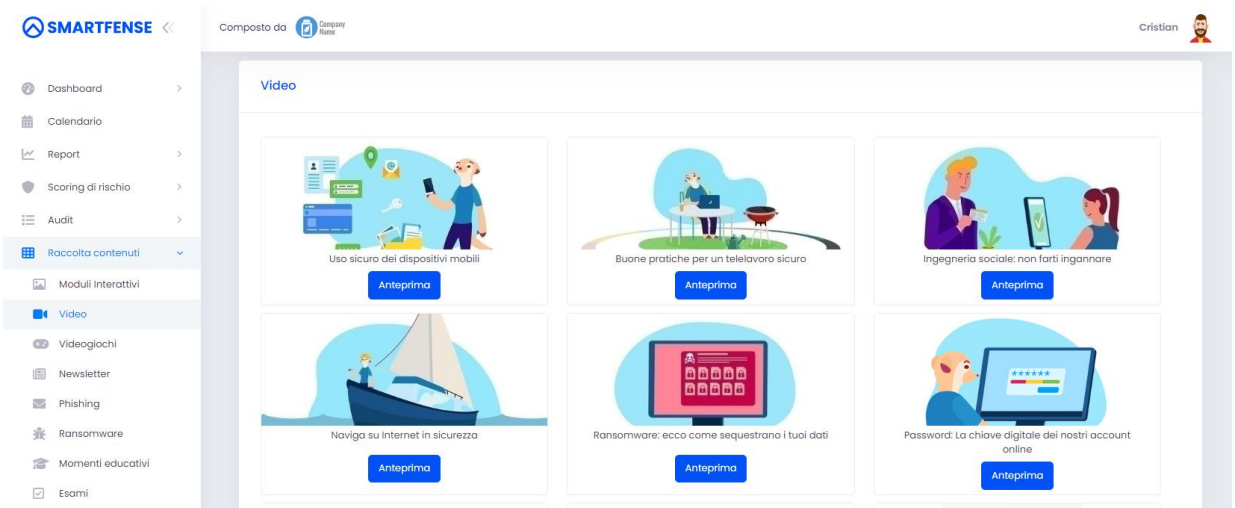
Le Newsletter hanno l'obiettivo di mantenere l'attenzione degli utenti su vari argomenti. Consentono di aggiungere domande alla fine di ciascuna Newsletter per convalidare la visualizzazione e la comprensione dei contenuti.



Newsletter

1.1.3. Video

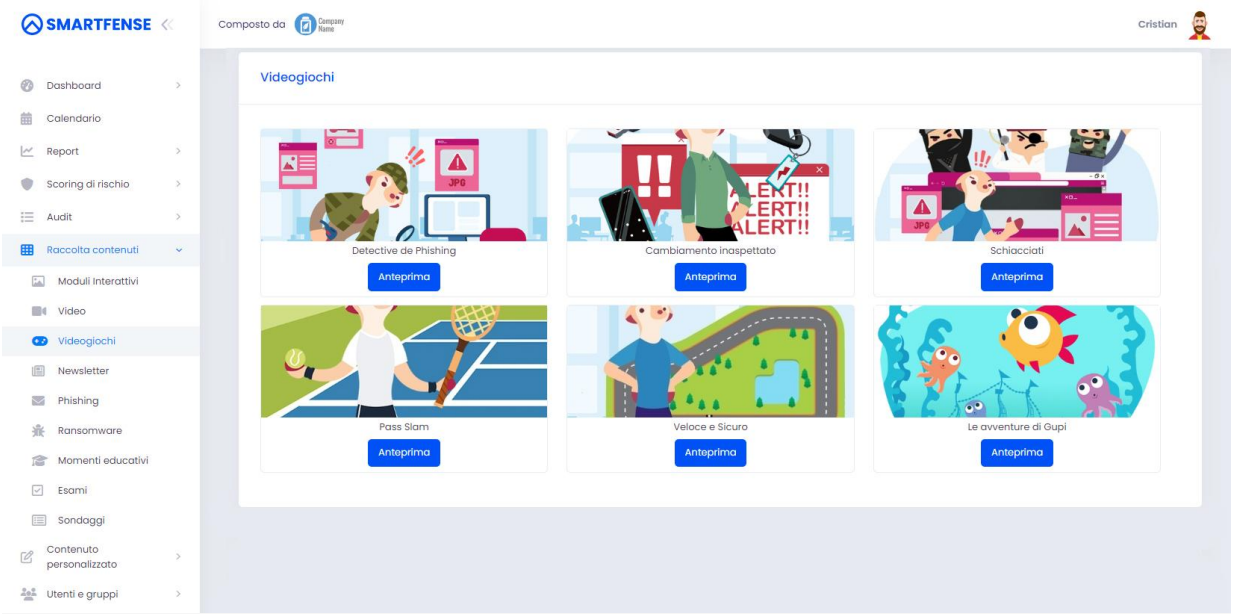
I video sono contenuti audiovisivi con lo scopo di sensibilizzare gli utenti e fornire un'alternativa più dinamica. Inoltre, consentono di aggiungere domande alla fine di ciascuno per verificare la visualizzazione e la comprensione dei contenuti.



Video

1.1.4. Videogiochi

I videogiochi di SMARTFENSE combinano sfide divertenti e feedback per promuovere comportamenti sicuri.



Videogiochi

1.1.5. Momenti Educativi

Un Momento Educativo si presenta come un breve contenuto ad alto impatto che viene mostrato in modo opzionale e automatico solo agli utenti che compiono un'azione considerata non sicura all'interno di una campagna di simulazione, aumentando così il livello di assimilazione del messaggio.

Momenti educativi

1.1.6. Fumetti

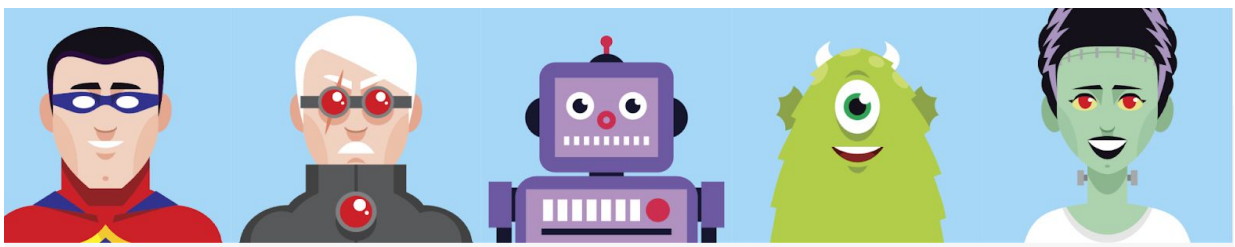
SMARTFENSE offre un fumetto educativo unico che promuove la consapevolezza delle minacce e delle misure di protezione nel mondo fisico e digitale. Combina narrazione visiva, formazione pratica e attività interattive per un'esperienza divertente e memorabile.

Fumetto: Cyber-Justice League

1.1.7. Gamification

Motivare gli utenti e catturare la loro attenzione migliora l'assimilazione dei contenuti e porta a cambiamenti di abitudini duraturi. Nella Dashboard, gli utenti possono visualizzare i loro Badge di Gamification, il progresso, la classifica e i punti esperienza.

Attraverso gli Avatar, l'utente può esprimere la propria identità in modo divertente, aggiungendo freschezza e diversità alla piattaforma.

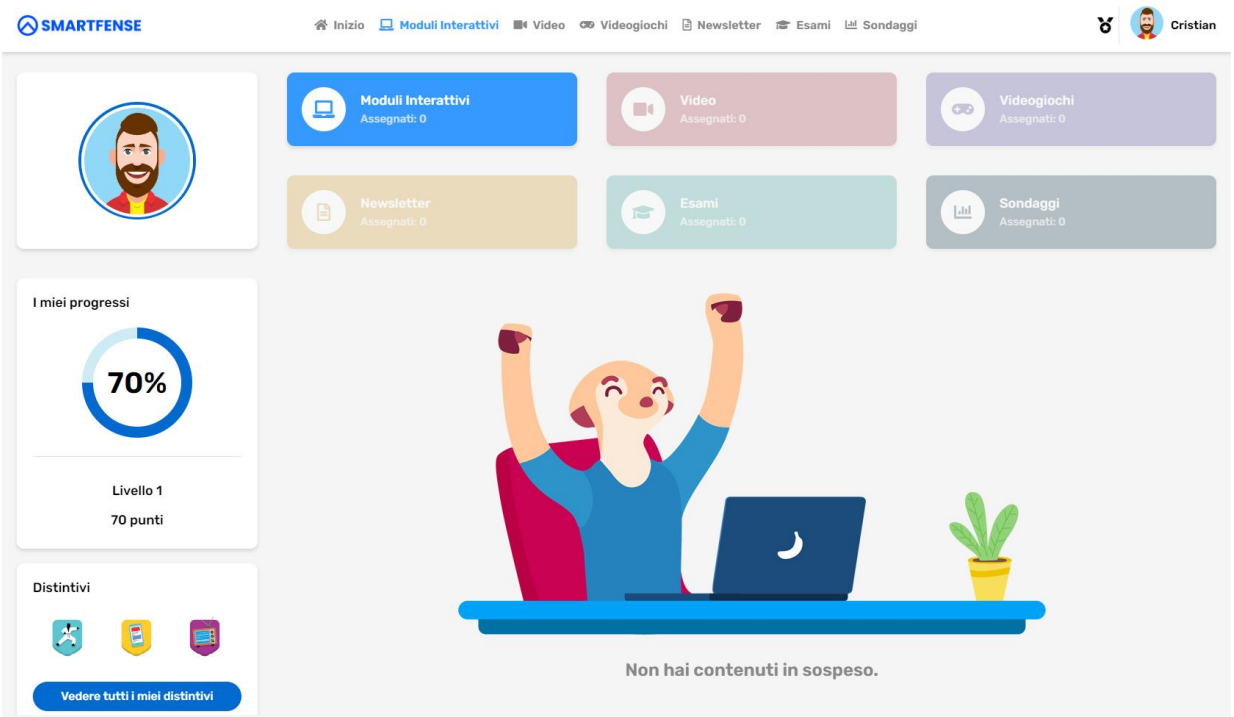


Avatar

Un Badge (distintivo) è una rappresentazione grafica di un merito ottenuto. Vengono assegnate automaticamente al completamento di azioni specifiche, come completare un Modulo Interattivo o rispondere correttamente a una Newsletter.

Badge

Man mano che l'utente finale compie azioni, vengono generati Punti Esperienza, permettendogli di salire di livello e vincere premi. Questo mostra il progresso e favorisce una sana competizione attraverso una classifica comparativa con gli altri utenti.

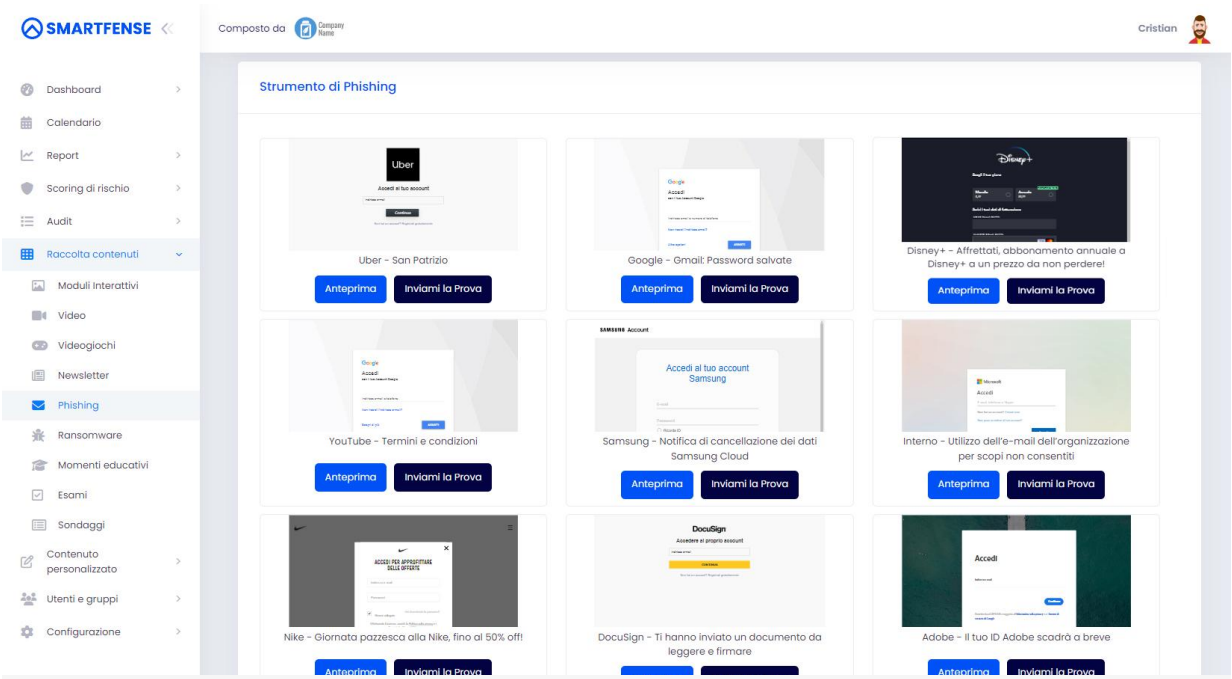


Gamification nella Dashboard dell'utente finale

1.2. Strumenti di Simulazione e Valutazione

1.2.1. Simulazione di attacchi di Phishing

SMARTFENSE consente di creare campagne di Phishing simulando email da aziende o enti riconosciuti in una presunta comunicazione ufficiale su internet. Queste campagne consentono di valutare quanti utenti cadono nel tranello di questi messaggi e mettono a rischio le informazioni confidenziali dell'azienda o del personale.



Simulazioni di Phishing

1.2.2. Simulazione di attacchi di Ransomware

SMARTFENSE consente di creare campagne di Ransomware che simulano l'invio di email da parte di organizzazioni affidabili o comunicazioni interne dell'azienda che invitano l'utente a scaricare un file sul proprio dispositivo. Attraverso queste campagne, l'amministratore può valutare quanti utenti mettono a rischio l'organizzazione installando un Ransomware.

1.2.3. Simulazione di attacchi con codice QR

Consente di creare campagne che simulano l'invio di email da aziende o enti riconosciuti, creando un'apparente comunicazione ufficiale che include un QR nel messaggio.

Simulazione di attacchi con codice QR

1.2.4. Simulazione di attacchi di Smishing

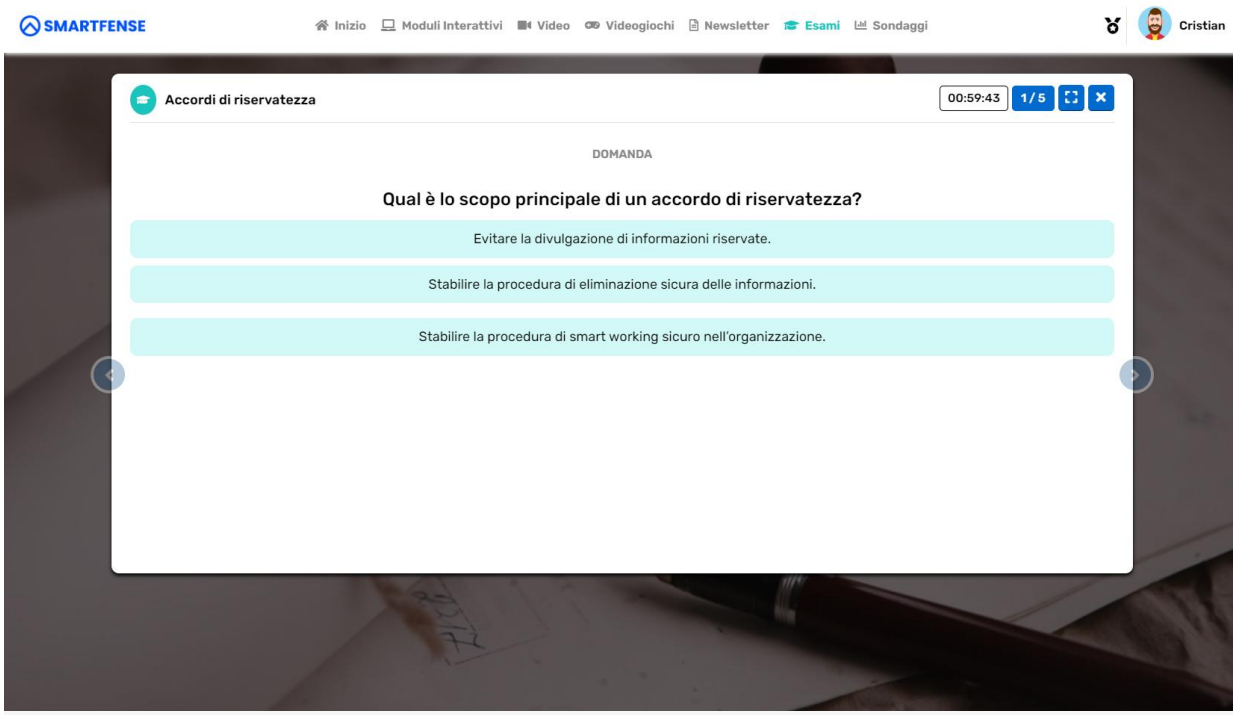
Le simulazioni di Smishing di SMARTFENSE sono messaggi SMS che ingannano l'utente per ottenere informazioni confidenziali tramite ingegneria sociale.

1.2.5. Simulazione di attacchi USB Drop

Queste campagne consentono di valutare il comportamento degli utenti quando trovano nel luogo di lavoro una chiavetta USB che non appartiene loro. In particolare, è possibile scoprire se l'utente apre i file contenuti nella chiavetta USB e se attiva le Macro dei file aperti. Ci sono momenti educativi per gli utenti che cadono nel tranello.

1.2.6. Esami e Sondaggi

Gli Esami e i Sondaggi sono strumenti di valutazione e raccolta di opinioni, rispettivamente. Gli Esami misurano il livello di conoscenza e l'assimilazione degli utenti dei concetti esposti nelle campagne di training, mentre i Sondaggi raccolgono opinioni e prospettive su vari argomenti.



Esame

1.3. Componente delle Normative

Il componente delle Normative ti consente di stabilire una connessione tra i contenuti della piattaforma e le normative di interesse per la tua organizzazione (come ad esempio ISO 27001, PCI-DSS, GDPR, ecc.).

Attraverso questa connessione, vengono generati automaticamente report molto utili per la gestione del rispetto delle normative, ad esempio:

- Contenuti che contribuiscono al rispetto della normativa.
- Grado di finalità che ogni utente ha per ciascuna normativa.
- Azioni specifiche che ogni utente ha compiuto per raggiungere la finalità indicata.

2. Contenuti

Tutti i contenuti della piattaforma possono essere modificati, utilizzati come modelli per crearne altri o creati da zero. I contenuti predefiniti sono sviluppati da esperti di sicurezza informatica e costantemente aggiornati. Nessun contenuto include il logo di SMARTFENSE, rendendo la piattaforma completamente personalizzabile.

2.1. Predefiniti

La libreria di contenuti forniti da SMARTFENSE è progettata per favorire lo sviluppo di abitudini sicure e il cambiamento di comportamento delle persone.

I contenuti vengono aggiornati periodicamente, riflettendo i cambiamenti nella realtà della Cyber Security e i progressi nella conoscenza della disciplina. Sono disponibili localizzati nelle seguenti lingue: italiano, spagnolo (America Latina), spagnolo (Spagna), inglese, portoghese (Portogallo), portoghese (Brasile), catalano, basco e francese.

2.2. Personalizzati

SMARTFENSE permette la generazione di contenuti personalizzati specifici per ciascuno degli strumenti di sensibilizzazione, simulazione e valutazione, utilizzando come modello un contenuto predefinito o creando un nuovo contenuto da zero. A tale scopo, la piattaforma fornisce un editor di contenuti integrato appositamente progettato per lavorare in modo semplice e intuitivo.

I contenuti personalizzati, inoltre, possono includere variabili personalizzate con informazioni specifiche dell'organizzazione o degli utenti assegnati.

3. Utenti e Gruppi

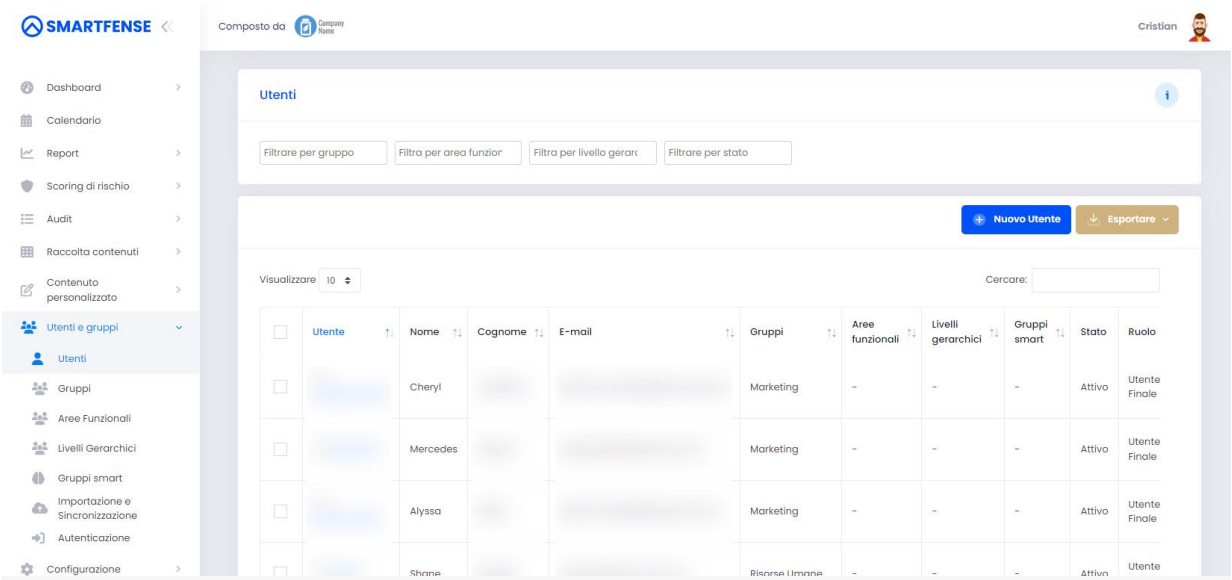
SMARTFENSE offre la possibilità di caricare gli utenti sincronizzando i dati con le ultime tecnologie disponibili sul mercato, come Microsoft Entra ID (Azure Active Directory) o Google, velocizzando l'integrazione con l'ambiente di ogni organizzazione.

Gli utenti possono essere assegnati a gruppi, aree funzionali, livelli gerarchici e gruppi intelligenti, che possono essere utilizzati come destinatari delle campagne.

3.1. Gruppi Intelligenti

Un gruppo intelligente è un tipo speciale di raggruppamento in cui gli utenti vengono aggiornati automaticamente in base a uno o più criteri definiti dall'amministratore della piattaforma.

L'uso di un gruppo intelligente, insieme ad altre caratteristiche di SMARTFENSE come le campagne di durata relativa, consente di avere campagne che assegnano automaticamente agli utenti che raggiungono un determinato livello di rischio. Inoltre, è possibile creare campagne di inserimento per nuovo personale che raggiungano automaticamente i nuovi utenti che sono creati sulla piattaforma.



Utenti e Gruppi

4. Integrazioni

La piattaforma SMARTFENSE offre diverse opzioni di integrazione con altri produttori:

4.1. Microsoft

È possibile sincronizzare gli utenti, i gruppi e le aree funzionali di SMARTFENSE con Microsoft Entra ID (Azure Active Directory) e eseguire l'autenticazione tramite Single Sign-On.

La piattaforma SMARTFENSE fornisce un pulsante di segnalazione di Phishing che può essere installato in Microsoft Outlook. Questo pulsante consente agli utenti di segnalare potenziali casi di Phishing in modo sicuro per un'analisi successiva da parte del team di risposta agli incidenti.

4.2. Google

Gli utenti possono accedere a SMARTFENSE utilizzando le credenziali di Auth0 tramite Single Sign-On.

4.3. Auth0

Gli utenti possono accedere a SMARTFENSE con le credenziali Auth0 tramite Single Sign-On.

4.4. Slack

SMARTFENSE consente la configurazione dell'invio delle notifiche tramite Slack.

4.5. SAP

SMARTFENSE si integra con SAP SuccessFactors attraverso registri di audit specifici per una comunicazione diretta tra le piattaforme.

4.6. Vanta

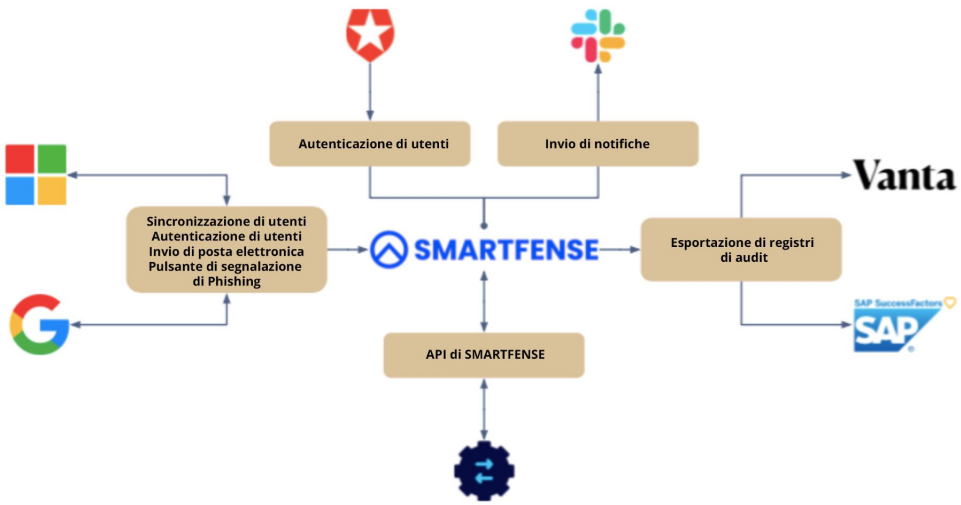
SMARTFENSE consente di inviare automaticamente a Vanta registri di audit associate alle azioni di sensibilizzazione effettuate.

4.7. Learning Management Systems (LMS)

SMARTFENSE consente l'integrazione con LMS come Moodle, Cornerstone o altri tramite un pacchetto SCORM. In questo modo, gli utenti possono accedere ai componenti della piattaforma in modo trasparente direttamente dall'LMS. Le statistiche vengono registrate sia su SMARTFENSE che sull'LMS.

4.8. API de SMARTFENSE

La piattaforma SMARTFENSE dispone di un'API che consente l'integrazione con altri sistemi.



Integrazioni

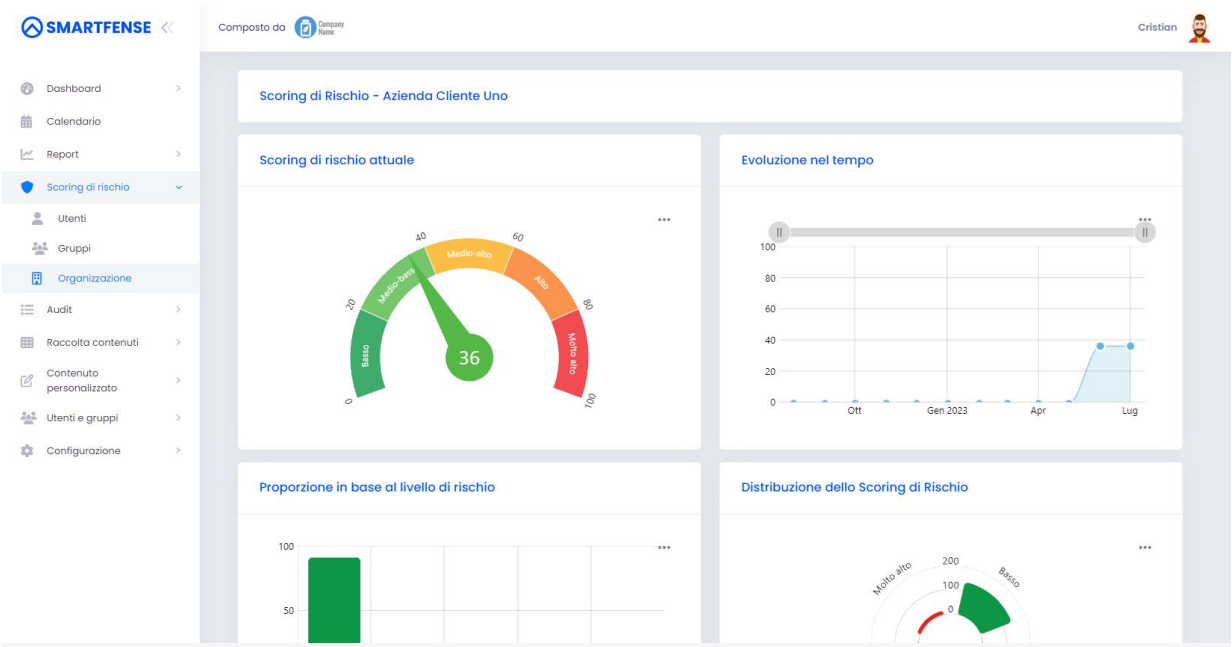
4.9. BeyGoo

I dati delle credenziali utente esposte ottenuti da BeyGoo sono ora incorporati in modo trasparente nei rapporti di Risk Scoring di SMARTFENSE.

5. Report e Audit

SMARTFENSE offre un completo insieme di report e registri di audit:

- Report interattivi per i manager sulle campagne lanciate, correlazione delle strumentazioni utilizzate, riassunto sull'uso di componenti specifici, ecc.
- Scoring di rischio degli utenti, dei gruppi e dell'organizzazione nel complesso. Per visualizzare i dati in modo efficace, viene utilizzata la tecnica della mappa termica.
- Tutte le attività svolte dagli utenti finali, dagli amministratori o dal sistema vengono riportati nei registri di audit come un diario di bordo.



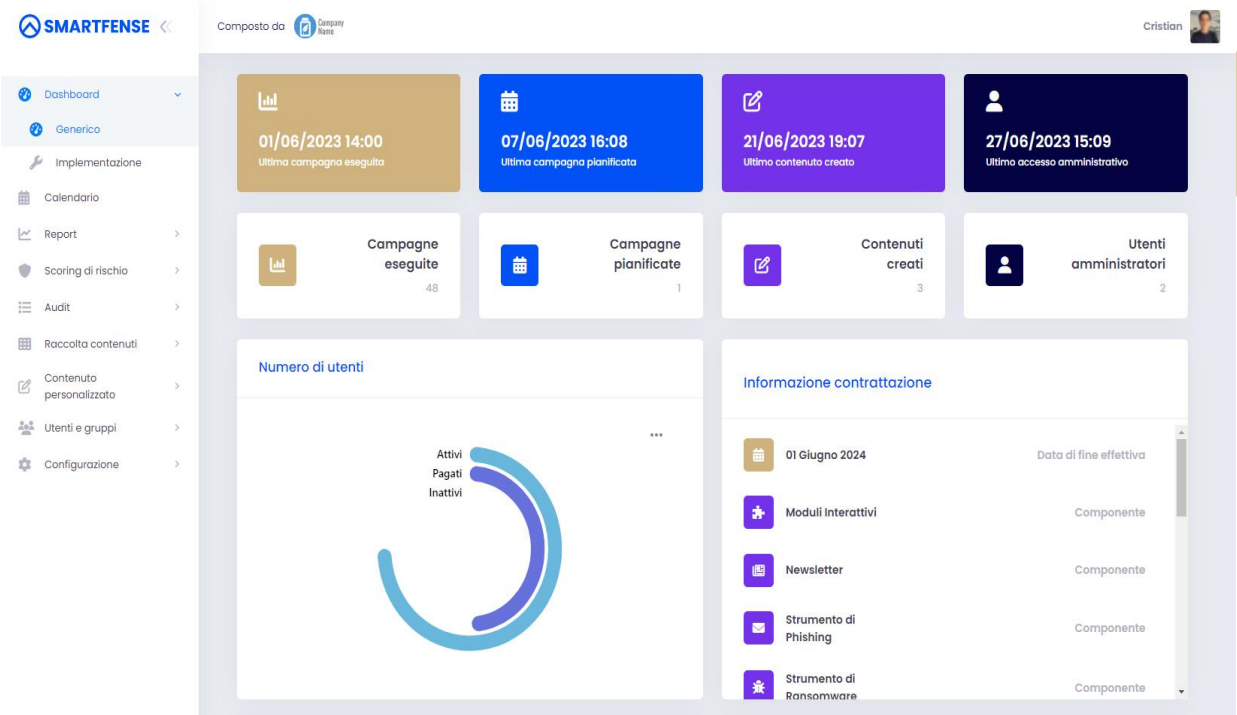
Report

6. Interfaccia utente

SMARTFENSE presenta due ambienti intuitivi nel suo design: una pensata per gli utenti con ruolo amministrativo e l'altra per gli utenti finali.

6.1. Ambiente per utenti con ruolo amministrativo

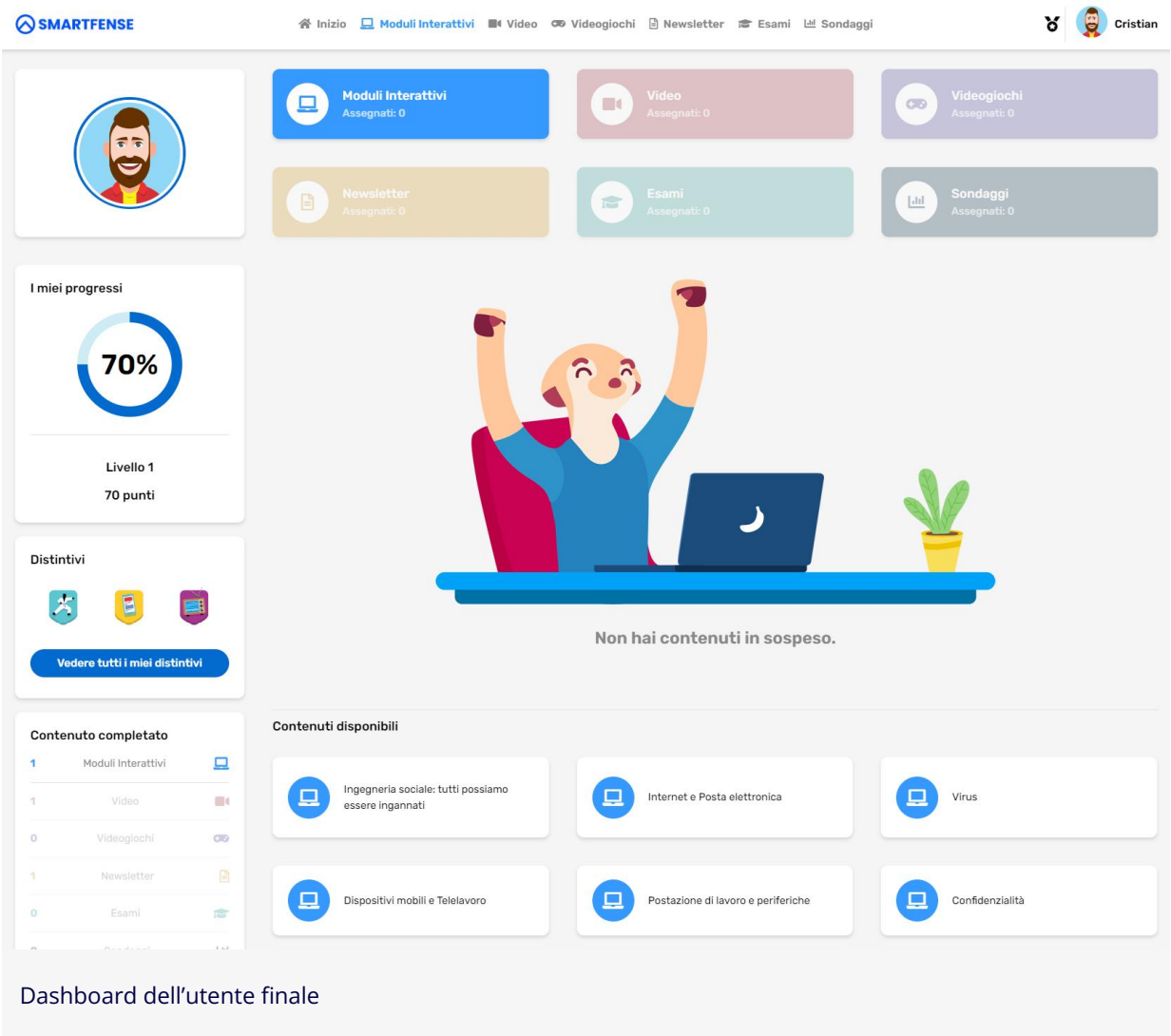
L'utente amministrativo ha accesso a diverse funzionalità e configurazioni della piattaforma SMARTFENSE. Le schermate disponibili e le azioni consentite sono definite in base al suo ruolo.



Dashboard dell'utente con ruolo amministrativo

6.2. Ambiente per utenti finali

L'utente finale ha a disposizione un'interfaccia chiara, moderna e completamente personalizzabile, dalla quale può accedere ai suoi contenuti in sospeso, disponibili e completati. Questa interfaccia include elementi di gamification come punti di progresso, distintivi e avatar.

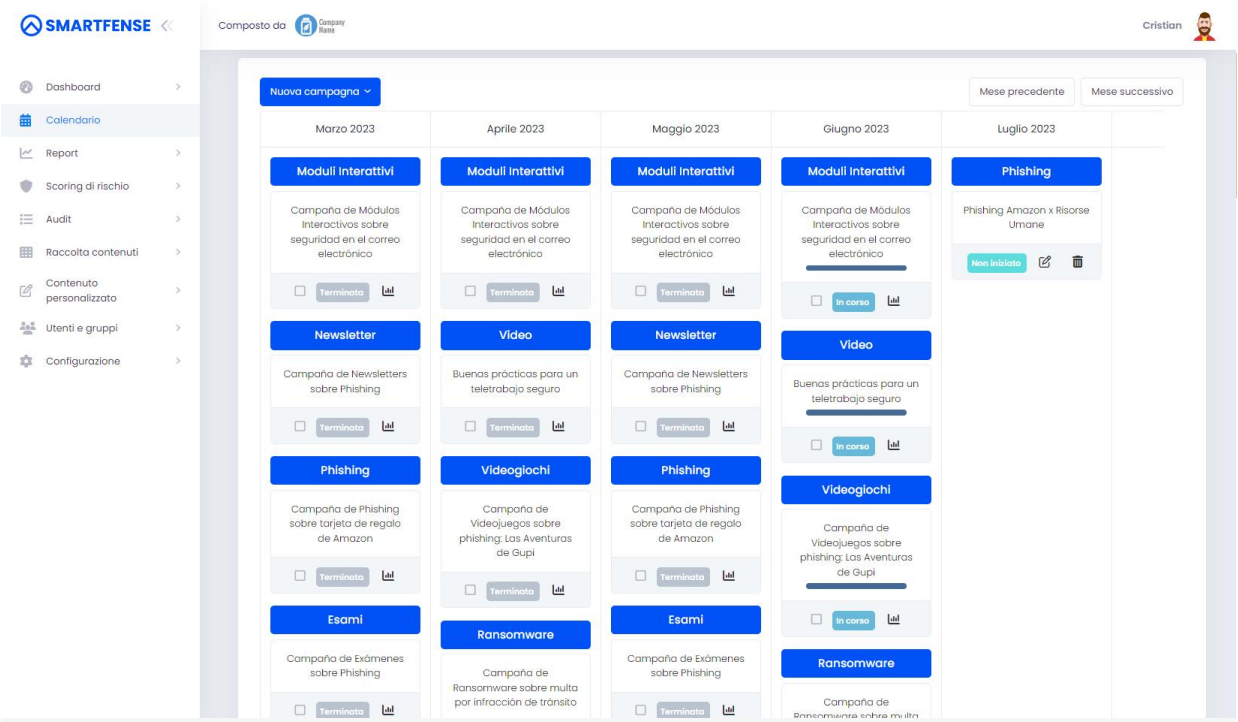


Dashboard dell'utente finale

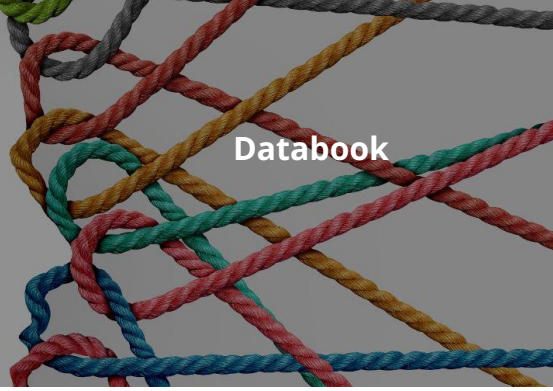
7. Calendario delle campagne

SMARTFENSE facilita la pianificazione delle campagne di awareness consentendo la selezione di contenuti predefiniti o personalizzati da assegnare a gruppi di utenti, aree funzionali, livelli gerarchici, gruppi intelligenti o singoli utenti. Il calendario fornisce una visione mensile di tutte le campagne programmate.

Inoltre, è possibile configurare un server di posta elettronica proprio per tutte le email inviate dalla piattaforma.



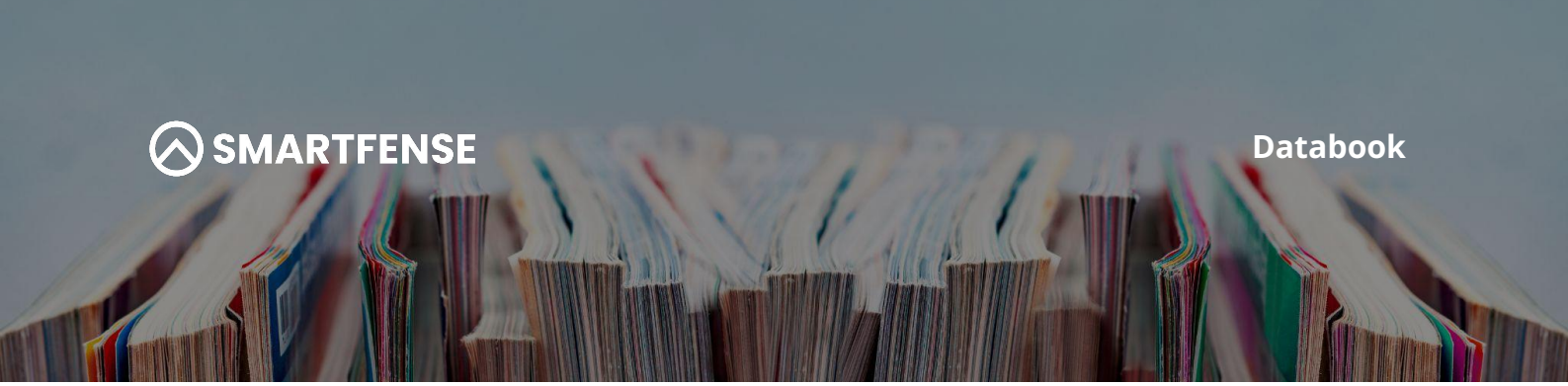
Calendario delle campagne



8. Multitenant

Il portale di gestione offre la possibilità di amministrare centralmente diverse entità, note come "organizzazioni gestite". Esistono diversi casi d'uso in cui questa funzionalità viene utilizzata per facilitare le attività amministrative e risparmiare tempo. Ad esempio, un'azienda con sedi in diversi territori o un gruppo aziendale.

Il portale offre una navigazione semplice tra le organizzazioni gestite, mantenendo i dati di ciascuna organizzazione separati. Potrete accedere direttamente alle loro informazioni, monitorare i loro progressi, lanciare campagne e creare i contenuti più appropriati per loro, tutto da un unico luogo.



9. Multicatalogo

I cataloghi sono un concetto per raggruppare i contenuti di sensibilizzazione e formazione per lavorare con essi in modo intuitivo e ordinato.

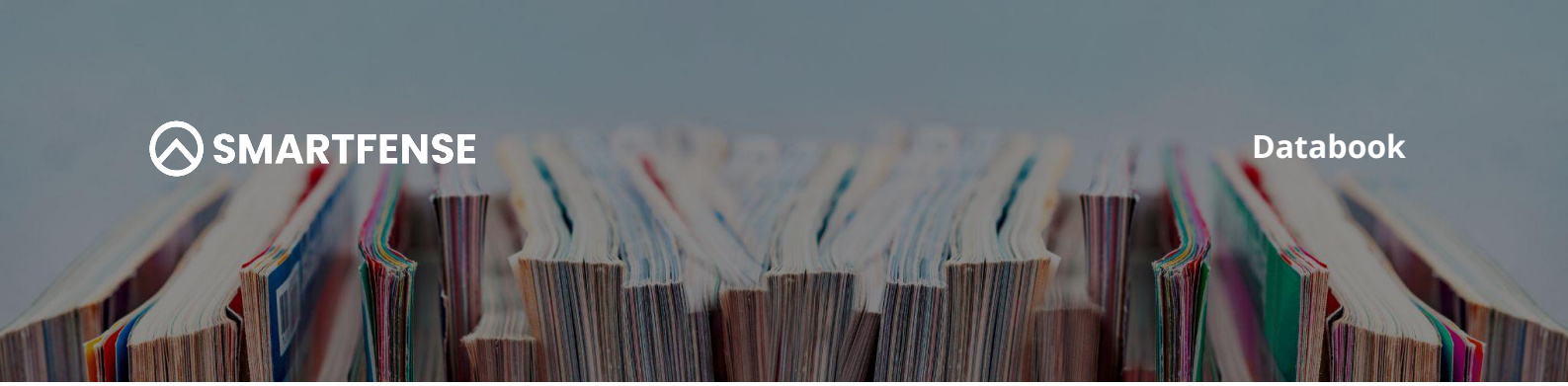
SMARTFENSE consente di lavorare con più cataloghi di contenuti. Di default, la piattaforma contiene il seguente catalogo:

- Cyber sicurezza per gli utenti finali.

D'altra parte, la piattaforma consente di acquistare i seguenti cataloghi:

- Cyber sicurezza per utenti esperti.
- Cyber sicurezza industriale.

I ruoli degli utenti amministrativi possono essere applicati diversamente per ogni catalogo. Ciò consente una gestione flessibile. Ad esempio, possiamo avere un utente amministrativo incaricato di creare contenuti e inviare campagne sulla cyber sicurezza industriale. I report, i registri di audit e altre informazioni provenienti dalla piattaforma mostreranno le informazioni all'utente che ha i permessi su quel catalogo (in questo caso, i contenuti e le campagne sulla cyber sicurezza industriale).



9. Multicatalogo

I cataloghi sono un concetto per raggruppare i contenuti di sensibilizzazione e formazione per lavorare con essi in modo intuitivo e ordinato.

SMARTFENSE consente di lavorare con più cataloghi di contenuti. Di default, la piattaforma contiene il seguente catalogo:

- Cyber sicurezza per gli utenti finali.

D'altra parte, la piattaforma consente di acquistare i seguenti cataloghi:

- Cyber sicurezza per utenti esperti.
- Cyber sicurezza industriale.

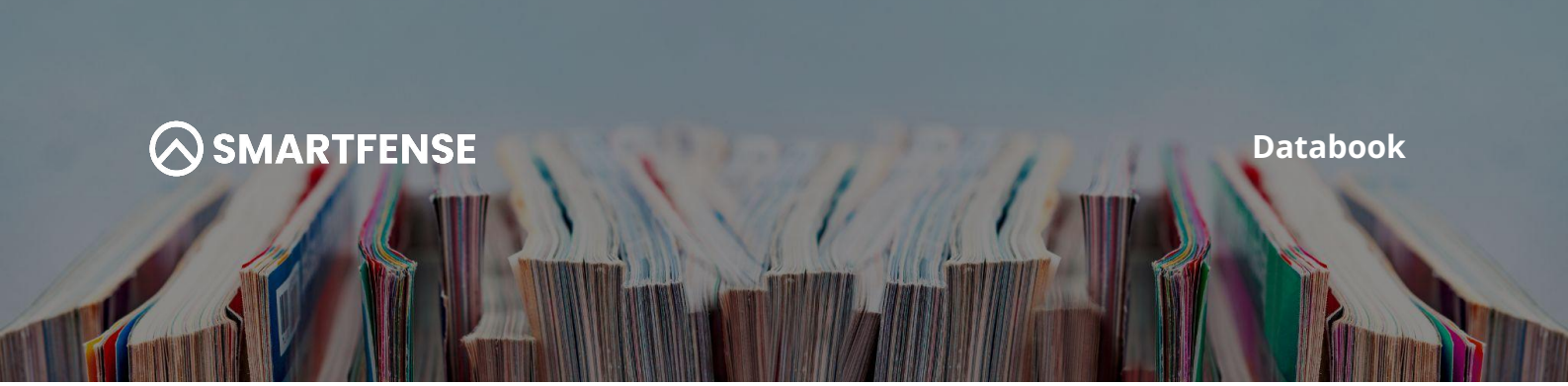
9.1. Catalogo di Cyber sicurezza industriale.

L'obiettivo principale di questo catalogo è quello di fornire informazioni specifiche sulle minacce alla sicurezza informatica e sulle migliori pratiche negli ambienti industriali.

Si rivolge alle organizzazioni del settore manifatturiero e delle infrastrutture critiche, nonché a quelle che utilizzano sistemi di controllo industriale (ICS) e tecnologie associate. D'altra parte, è adatto anche agli enti responsabili della regolamentazione e della supervisione dei settori industriali critici.

Gli utenti target per questo tipo di contenuti sono:

- Personale che gestisce sistemi di controllo industriale.
- Professionisti dell'IT e della sicurezza.
- Dirigenti e decisori.



9.2. Catalogo dei contenuti avanzati

L'obiettivo principale di questo catalogo è fornire informazioni avanzate e aggiornate sulle minacce informatiche in generale, nonché sulle tattiche e le tecniche all'avanguardia utilizzate dai criminali informatici.

Si rivolge alle aziende di diversi settori che desiderano una comprensione approfondita delle minacce informatiche odierne. Si rivolge anche alle organizzazioni con un approccio proattivo alla sicurezza informatica e con l'esigenza di rimanere al passo con le ultime tendenze. Può essere interessante anche per i fornitori di servizi di sicurezza informatica e le società di consulenza specializzate.

Gli utenti target di questo tipo di contenuti sono:

- Gli utenti finali che hanno soddisfatto i requisiti dei cataloghi di sensibilizzazione di base e che ora cercano di tenersi aggiornati sulle ultime tattiche e tecniche dei criminali informatici.
- Personale di nuova generazione che è cresciuto con l'uso della tecnologia e ha assorbito in modo trasparente i comportamenti di base della sicurezza informatica.
- Professionisti in aree tecnologiche o con grandi responsabilità all'interno dell'organizzazione.

I ruoli degli utenti amministrativi possono essere applicati per ogni catalogo. Ciò consente una gestione flessibile. Ad esempio, possiamo avere un utente amministrativo incaricato di creare contenuti e inviare campagne sulla sicurezza informatica industriale. I report, gli audit trail e altre informazioni provenienti dalla piattaforma mostreranno le informazioni all'utente che ha i permessi su quel catalogo (in questo caso, i contenuti e le campagne sulla sicurezza informatica industriale).