SMARTFENSE

# Linee guida per la presentazione dei servizi di awareness

# Indice

# Obiettivo generale

Lo scopo di questo documento è quello di **aiutare il partner a presentare i servizi di sensibilizzazione in modo indipendente** ai propri clienti e prospect.

Le presentazioni più efficaci sono quelle che si adattano alle esigenze specifiche dei clienti potenziali. Per questo motivo, è essenziale **ascoltare attentamente le loro sfide** e poi **adattare la proposta** in base alle informazioni raccolte. Questo approccio, noto come **vendita consultiva**, prevede l'offerta di **servizi a valore aggiunto del partner**, **supportati da SMARTFENSE come strumento**, piuttosto che una semplice presentazione del prodotto. Si consiglia inoltre che il partner offra un servizio **completamente gestito**..

## 1. Analisi della situazione, dei problemi e delle esigenze

In questa sezione, ci concentreremo su una serie di domande chiave che ti aiuteranno a identificare le esigenze e i problemi del potenziale cliente, per poter offrire una soluzione adeguata. È cruciale prendersi il tempo necessario per ascoltare con attenzione, annotando le risposte e le parole chiave che il cliente menziona.

- **Hanno mai intrapreso azioni di sensibilizzazione sulla sicurezza delle informazioni?**
- **Queste attività sono svolte su base continuativa?**
- **Stanno ancora realizzando queste iniziative?**
- **Qual è stato il riscontro ottenuto?**

Queste domande ti aiuteranno a capire il livello di preparazione del prospect in termini di consapevolezza sulla sicurezza.

**Dati da Raccogliere: Maturità dell'organizzazione: Valuta quanto l'azienda sia avanzata nella consapevolezza sulla sicurezza delle informazioni.**

—

- **È la prima volta che valutano una soluzione per il programma di awareness?**

Questa domanda è utile per capire se il cliente ha già esperienza con strumenti di sensibilizzazione o se sta valutando diverse opzioni. Adattare la presentazione in base a queste informazioni può fare la differenza.

## Dati da Raccogliere: Nome dello strumento attualmente in uso.

—

- **Qual è la portata del programma di awareness?**
- **Quanti utenti volete raggiungere?**

Comprendere la portata del programma di sensibilizzazione è cruciale per determinare la probabilità che un potenziale cliente diventi effettivo. Ecco alcune considerazioni chiave:

- **Organizzazioni con pochi utenti (meno di 100)**: Queste tendono a non percepire appieno il valore di SMARTFENSE e potrebbero optare per soluzioni più economiche e generiche, anche se meno efficaci. Questa scelta è spesso dovuta a un basso livello di investimento nella sicurezza informatica. Tuttavia, le piccole organizzazioni soggette a normative di conformità o con un elevato livello di maturità della sicurezza sono in grado di riconoscere e apprezzare il valore di SMARTFENSE.
    - I nostri partner possono offrire istanze multi-cliente per servire i clienti più piccoli, facilitando così l'adozione della nostra soluzione anche per le organizzazioni con esigenze minori.
- **Organizzazioni di medie dimensioni:** Queste aziende tendono a comprendere meglio il valore del nostro servizio senza essere eccessivamente esigenti nei confronti del fornitore e del partner. La maggior parte dei clienti di SMARTFENSE rientra in questo settore, e noi abbiamo vasta esperienza e numerose storie di successo da condividere.
- **Organizzazioni molto grandi:** Queste tendono a valutare più opzioni e ad avere esigenze più elevate. La chiave per soddisfare le loro necessità è dimostrare l'efficacia della piattaforma e l'esperienza del partner con clienti di grandi dimensioni. Se l'azienda opera in più territori o fa parte di una holding, è fondamentale evidenziare la capacità di gestire efficacemente queste complessità con il sistema Multitenant di SMARTFENSE.

## Dati da Raccogliere: Numero di utenti da raggiungere.

—

- **Chi guida le azioni di awareness sulla sicurezza delle informazioni nella vostra organizzazione?**

È utile sapere se stiamo parlando con chi prende le decisioni o se è necessario coinvolgere altri membri.

- Spesso è il **CISO** a mostrare interesse per i servizi di sensibilizzazione e a prendere le decisioni. Con il CISO, evitare dettagli tecnici e concentrarsi sulla

**valorizzazione del tempo e delle risorse del suo team**. Assicurare che il partner si occupi degli aspetti tattici e operativi, coinvolgendo il CISO solo per questioni strategiche.

- In alcuni casi, un **Analista** sotto il CISO è incaricato di gestire il programma. In questi casi, parleremo del supporto del partner come servizio gestito, oppure offriremo la possibilità di lavorare insieme a loro (in modo che non si sentano minacciati). Dobbiamo concentrarci sugli aspetti della **produttività**, in modo che vedano che gli aspetti operativi saranno di competenza del produttore e del partner, mentre gli aspetti tattici saranno svolti insieme a loro. Avranno un contenuto più professionale, mentre la comunicazione e la reputazione dell'area miglioreranno.
- Quando la responsabilità ricade sull'**area IT** per l'assenza di un reparto di cyber security dedicato, proporre un **servizio gestito come soluzione**. Evidenziare che il partner e il produttore gestiranno la maggior parte del lavoro, permettendo al team IT di intervenire solo su aspetti minori.

Inoltre è utile sapere chi gestisce il budget.

- Può darsi che il budget sia gestito dalle persone con cui stiamo parlando, ma può anche darsi che sia gestito dalle **Risorse Umane**. In questo caso, dovremmo concentrarci sul fatto che la soluzione utilizzata può essere **integrata senza problemi con la maggior parte delle piattaforme di e-learning** esistenti.

**Dati da Raccogliere: Decisore.**

—

- **In quale arco di tempo pensate di implementare uno strumento di sensibilizzazione? A breve, medio o lungo termine?**

Serve a creare un senso di urgenza e a prevenire la procrastinazione. Può essere utilizzato per esercitare pressione, evidenziando il rischio di rimanere in violazione della due diligence per un periodo prolungato.

**Dati da Raccogliere: data della possibile vendita.**

—

- **Hanno già stanziato un budget o lo stanno ancora valutando?**

Se hanno già stanziato un budget, dobbiamo enfatizzare che questo investimento offre un ROI migliore rispetto ad altri investimenti in sicurezza informatica, in quanto è relativamente più economico e allo stesso tempo più facile da dimostrare e spiegare.

Se non hanno ancora stanziato un budget, spetterà al partner decidere se registrare l'opportunità ora o aspettare per farlo in un secondo momento. Se non è un progetto a breve termine, **le opportunità non dovrebbero essere registrate immediatamente**, poiché il tempo inizia a scorrere per la scadenza dell'opportunità.

**Dati da Raccogliere: disponibilità di budget.**

—

Una volta raccolte tutte queste informazioni, possiamo iniziare a rispondere e spiegare al potenziale cliente, **concentrandoci sulle loro esigenze specifiche**.

Ricorda che l'importante non è lo strumento in sé, ma il **SERVIZIO A VALORE AGGIUNTO** che il partner può fornire.

# 2. Presentazione

Sulla base delle informazioni raccolte, **la presentazione deve essere adattata alle esigenze del cliente**.

Il partner dovrebbe offrire **servizi** gestiti e/o a valore aggiunto per accompagnare da vicino il prospect. La presentazione **non** deve concentrarsi sulla dimostrazione delle capacità del prodotto, ma sul **valore fornito dal partner**.

Nel caso della presentazione della piattaforma, l'attenzione deve essere focalizzata sull'interfaccia dell'utente finale, **evitando di mostrare l'interfaccia amministrativa**, **in modo che il potenziale cliente non possa immaginarne l'utilizzo**, poiché dovrebbe essere il partner a svolgere questo compito.

Ci saranno situazioni in cui il potenziale cliente vorrà sapere se la piattaforma soddisfa determinati requisiti tecnici. Il partner, conoscendo le capacità, può dire se e come le soddisfa e vedere se è necessario dimostrarlo. A parte questi casi eccezionali, la vista amministrativa non dovrebbe essere mostrata. Questi sono i passi proposti, adattati sulla base di quanto rilevato in precedenza

## 2.1. Punti di forza e validazione

In questa prima fase, sulla base delle risposte ottenute, dobbiamo argomentare **perché l'interessato dovrebbe assumere i servizi del partner sulla piattaforma SMARTFENSE**. Cogliere l'occasione per convalidare le informazioni ottenute e consolidare una stretta relazione.

**Dati ottenuti: maturità organizzativa per l'awareness.**

- Le organizzazioni che probabilmente avranno bisogno di servizi SMARTFENSE e di awareness sono quelle che hanno già intrapreso un'iniziativa e conoscono l'enorme sforzo che comporta farlo senza uno strumento e un partner che fornisca servizi.
    - **Punto di forza:** attingere all'esperienza e alle storie di successo del partner per dimostrare che si può ottenere di più con meno sforzo, in modo che il potenziale cliente utilizzi il tempo per concentrarsi sulla strategia.
- D'altro canto, se si tratta di un'organizzazione che non sta facendo nulla, bisogna concentrarsi sulla **due diligence/compliance**. Non facendo nulla, in caso di attacco, potrebbe essere messo in discussione se ha fatto ciò che doveva essere fatto per prevenire l'incidente. Poiché la maggior parte degli attacchi ha come obiettivo il fattore umano, non fare nulla è una decisione molto rischiosa.
    - **Punto di forza:** dire loro che se non fanno nulla si espongono a un enorme rischio di due diligence perché è il fattore più attaccato (il fattore umano).

### Dati ottenuti: Nome dello strumento attualmente in uso.

- Il presentatore deve conoscere le Battle Card per poterne spiegare le differenze.
    - **Punto di forza:** differenziare SMARTFENSE in base alla specifica Battle Card, disponibile sul Partner Portal, nella sezione documenti commerciali.
    - **Punto di forza:** differenziare il servizio a valore aggiunto che può essere offerto grazie alla flessibilità della soluzione.
    - **Punto di forza:** vicinanza del partner e del prospect al produttore.

### Dati ottenuti: Numero di utenti da raggiungere.

- Organizzazioni con pochi utenti (meno di 100).
    - **Punto di forza:** Se non si dispone di personale specializzato a sufficienza, è meglio stipulare un contratto per un servizio gestito, poiché le piattaforme di awareness di oggi richiedono competenze più elevate per essere gestite.
- Organizzazioni di medie dimensioni.
    - **Punto di forza:** Anche se le organizzazioni di queste dimensioni dispongono di personale che può avere un ruolo di sicurezza informatica incentrato sul programma di awareness, tale persona deve concentrarsi sull'apporto di valore all'organizzazione. Per questo motivo, si consiglia

vivamente di affidarsi a un partner esperto che non solo gestisca la piattaforma, ma possa anche fornire raccomandazioni tattiche sul programma.

- Organizzazioni molto grandi.
    - **Punto di forza:** Usa l'esperienza e le storie di successo del partner per dimostrare che è possibile ottenere di più con meno sforzo, consentendo al cliente di concentrarsi sulla strategia. L'utilizzo della funzionalità Multitenant può facilitare una gestione centralizzata e decentralizzata allo stesso tempo. L'intero programma può essere gestito dalla piattaforma, e le azioni di simulazione possono essere collegate al cambiamento comportamentale degli utenti.

## 2.2. Presentazione

In questa seconda fase, il partner può concentrarsi su **tre principali servizi a valore aggiunto** per migliorare l'efficacia del programma di cyber security awareness:

- Accompagnamento nella preparazione del programma di awareness, programmazione ed esecuzione delle campagne definite.
- Personalizzazione dei contenuti adattati alla cultura aziendale.
- Consegna di Report sull'evoluzione dei comportamenti.

### Accompagnamento nella preparazione del programma di awareness, programmazione ed esecuzione delle campagne definite

Dobbiamo innanzitutto concentrarci sul programma di awareness in base all'indagine realizzata, cercando di coprire i punti di interesse e i punti dolenti menzionati dai prospect.

In questo caso, il partner deve essere esperto nel preparare il piano iniziale (baseline) e nell'adattarlo in base all'evoluzione del comportamento degli utenti, come risulta dai report ottenuti. La **baseline** rappresenta il punto di partenza per la progettazione di un programma adatto all'organizzazione del cliente, poiché fornisce una valutazione iniziale delle competenze e delle vulnerabilità esistenti. Successivamente, il partner deve essere in grado di modificare il programma in risposta ai cambiamenti osservati nel comportamento.

Leggere questo articolo Designing an Awareness Program per comprenderne l'importanza. Di seguito viene proposto un esempio di programma.

### Quali sono i vantaggi di questo lavoro?

- Raggiungere la consapevolezza e il rinforzo attraverso diversi contenuti (moduli interattivi, video, videogiochi, fumetti, newsletter, momenti educativi) che consentano all'utente di acquisire abitudini sicure.
- Condurre valutazioni e misurazioni costanti (simulazioni di phishing, simulazioni di ransomware, simulazioni di smishing, USB Drop, quiz e sondaggi) per dimostrare l'evoluzione nel tempo.

## Personalizzazione dei contenuti adattati alla cultura aziendale

In secondo luogo, è essenziale che il partner adatti ogni contenuto alla cultura dell'organizzazione del prospect per ottenere un maggiore coinvolgimento. Questo approccio personalizzato aumenta l'efficacia del programma di awareness. Con SMARTFENSE, non solo è possibile **regolare e creare contenuti**, ma anche **configurare** tutti i feedback e le notifiche ricevute dagli utenti, utilizzando la tipografia e i colori dell'organizzazione del cliente.

I contenuti su SMARTFENSE sono facili da creare, sia utilizzando i modelli predefiniti disponibili nei nostri cataloghi, sia partendo da zero. Nell'articolo sulla personalizzazione dei contenuti, è disponibile una guida pratica per farlo in modo semplice ed efficace.

### Quali sono i vantaggi di questo lavoro?

Il partner deve mostrare nell'**istanza di demo**(vedi articolo: Come condividere l'accesso a diversi contenuti) esempi di contenuti che tengano conto dei seguenti vantaggi di ciascun tipo di contenuto:

- 100% white label. Poiché può essere adattato al manuale aziendale del cliente, i messaggi vengono inviati con l'immagine del brand del client
- Contenuto adattato e localizzato alla cultura organizzativa.

Una volta progettato il programma di awareness con i contenuti definiti, sia dal catalogo predefinito di SMARTFENSE sia creati appositamente per il cliente, il partner può programmare le campagne con i contenuti nel calendario della piattaforma. Per saperne di più sulla programmazione delle campagne.

## Consegna di Report sull'evoluzione dei comportamenti

In terzo luogo, il partner deve specificare che fornirà vari report al potenziale cliente. Questi report possono essere ottenuti tramite **Report**, **Scoring di rischio**, **Audit** e **API**. Sarebbe ottimale che il partner presentasse report personalizzati invece di utilizzare solo quelli forniti dalla piattaforma, anche se può mostrare anche quelli forniti direttamente dalla piattaforma.

- In **Report** e **Scoring di Rischio** è possibile vedere i grafici con i risultati del comportamento degli utenti e la loro evoluzione nel tempo.
- In **Audit** fornisce tutte le informazioni sul funzionamento della piattaforma. Ad esempio, in campagne e utenti, vengono presentati dati e statistiche per:
    - Campagne (numero di eventi realizzati, eventi futuri ed eventi cancellati, a seconda del tipo di contenuto).
    - Utenti (a quale campagna hanno partecipato, dettagli su ciascuno di essi, dettagli generali). Ad esempio, è possibile filtrare per un particolare contenuto e vedere quali utenti hanno eseguito campagne di simulazione di phishing e il loro risultato.
    - Amministrazione (dettagli su tutto ciò che hanno fatto gli utenti amministratori).
- È possibile collegare le **API di SMARTFENSE** a strumenti di Business Intelligence (BI) come Power BI, Looker Data Studio o Tableau per creare dashboard interattivi, facendo così una grande differenza.

L'articolo sui report personalizzati illustra in dettaglio i dati e i grafici che è possibile trovare sulla nostra piattaforma e che possono essere utilizzati per creare i propri report.

Infine, va ricordato che il partner si occuperà non solo del **supporto di primo livello**, ma anche dell'**implementazione**, che comprende:

- Registrazione di utenti e gruppi.
- Configurazioni di whitelist.
- Setup della piattaforma.

### Quali sono i vantaggi di questo lavoro?

- Fornire rapporti personalizzati al cliente.
- Adattare le azioni proprie o esterne del programma di awareness.

- Fornire risposte alla domanda su quale sia il livello di rischio per ogni utente dell'organizzazione, per ogni gruppo e per l'organizzazione stessa.

# 3. Differenziatori

Nel caso in cui il potenziale cliente stia valutando diverse soluzioni, il partner non dovrebbe basarsi solo sulla Battlecard specifica del concorrente. È importante essere consapevoli dei fattori di **differenziazione** della piattaforma e citarli in linea con le esigenze e le problematiche elencate dal potenziale cliente nella fase iniziale.


www.smartfense.com

info@smartfense.com