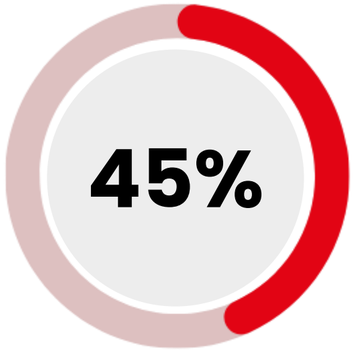
GLI ATTACCHI CYBER ATTRAVERSO LA SUPPLY CHAIN SONO IN COSTANTE AUMENTO. COME PROTEGGERSI?

Il problema: Controllare le Terze Parti

- La supply chain diventa sempre più complessa e sempre più aziende hanno reti informatiche interconnesse fra loro
- I nuovi regolamenti (NIS 2, DORA e altri richiedono il monitoraggio costante delle terze parti con cui ogni azienda si interfaccia
- **Gli attacchi informatici che utilizzano una terza parte come “Cavallo di Troia” sono in aumento esponenziale**



Secondo gli analisti di Gartner nel 2025 il 45% delle organizzazioni mondiali verranno in qualche forma danneggiate da attacchi informatici subiti da loro terze parti

Businesses fear rise of third-party attacks, as ransomware impact grows

Some 84% of organisations worldwide believe supply chain attacks can become a major threat within the next three years, with 48% in Asia-Pacific reporting at least one such attack in the past year and another 69% encountering at least one ransomware attack.

Written by **Eileen Yu,** Senior Contributing Editor on Dec. 7, 2021

SLING

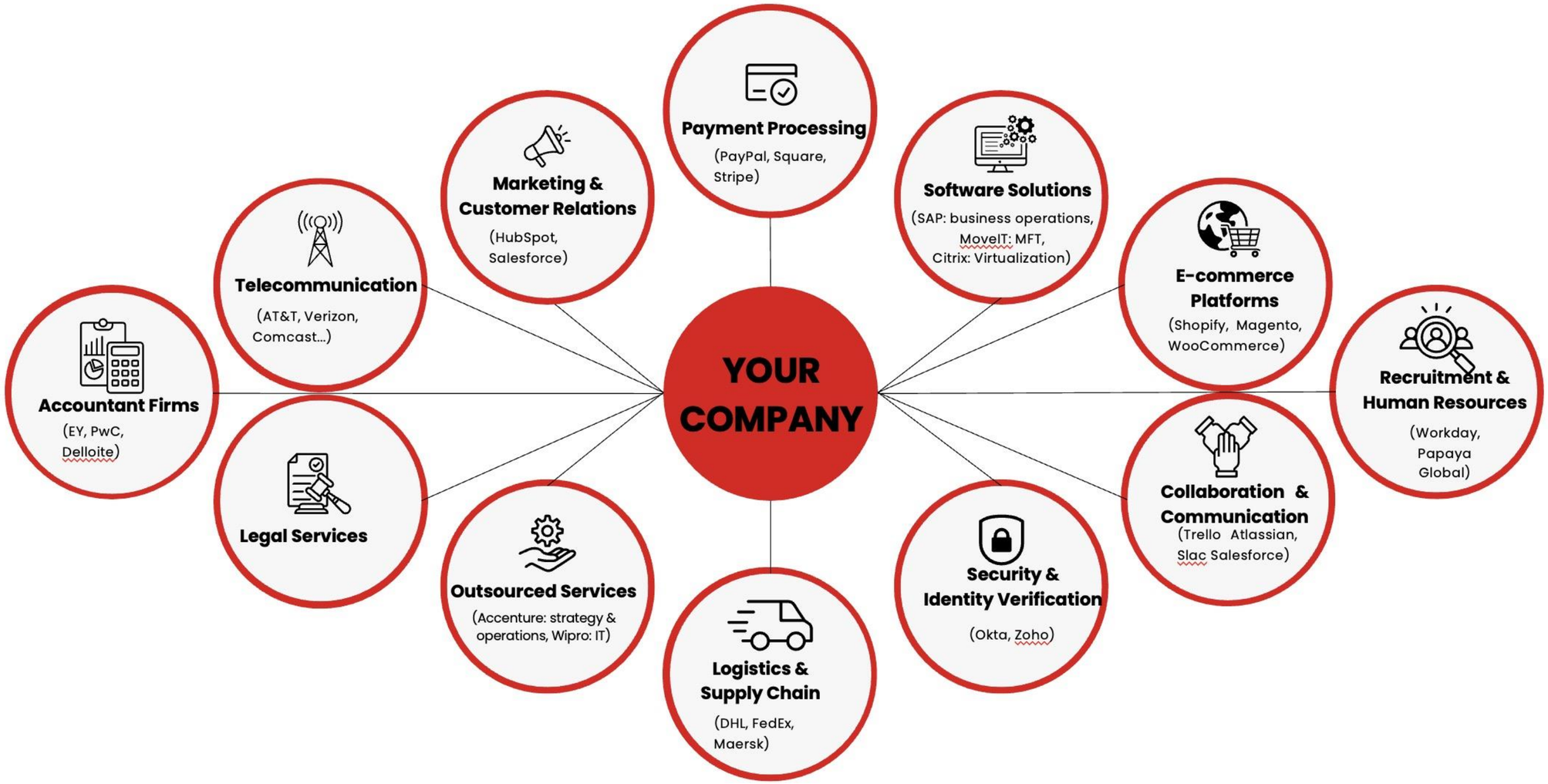
Alcuni esempi di attacchi attraverso terze parti

T-Mobile ha affrontato diverse falle di sicurezza, tra cui una vulnerabilità nelle API, esposizione di dati sensibili dei clienti e dei dipendenti e problemi causati da fornitori esterni.

MOVEit è stata colpita da un attacco ransomware sfruttando una vulnerabilità zero-day, coinvolgendo oltre 1.000 organizzazioni a livello globale.

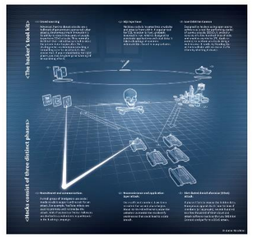
Okta ha subito una violazione tramite un fornitore terzo, con furto di dati personali sensibili di dipendenti.

Quali sono le terze parti da cui potrebbe arrivare l'attacco?



Chi è che ci attacca?

l’Hacker non è più il ragazzino con il cappuccio che «lavora» dal suo garage



Sono vere e proprie **organizzazioni criminali** che sanno tutto di noi incluso il nostro fatturato e quindi quanto presumibilmente possono estorcerci

In che modo potrebbero attaccarci?

Infettando i nostri sistemi

Compromettendo i nostri dati (Ransomware)

Compromettendo la nostra “Business Continuity

Quali danni potremmo subire?

Attacchi Ransomware

Gli attaccanti bloccano uno o più nostri server, o peggio ancora riescono ad impadronirsi dei nostri dati e li rendono non accessibili.
Per poter riprendere a lavorare siamo costretti a pagare un riscatto

Blocco dell'attività

La nostra rete non è disponibile, computer, macchinari e telefoni non funzionano più. Non possiamo produrre, né vendere, né fatturare. Siamo costretti a mandare a casa i dipendenti oppure averli davanti a noi che non possono fare altro che chiacchierare o giocare a carte

Violazione della privacy/ Furto della Proprietà Intellettuale

I nostri dati personali, quelli dei nostri dipendenti o peggio ancora dei nostri clienti vengono messi a disposizione pubblicamente sul web. Inoltre ci vengono sottratte le nostre proprietà intellettuali che potrebbero poi essere rivendute per esempio in Cina

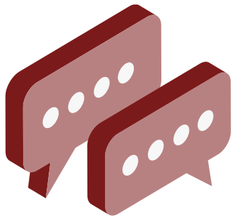
Danni reputazionali

La legge ci impone di comunicare pubblicamente gli attacchi subiti. Anche qualora si potesse evitare ci penseranno coloro che ci hanno attaccato. I clienti continueranno a fidarsi di noi sapendo che le loro informazioni personali sono state compromesse?

Controllo della Supply Chain: Le sfide

Mancanza di informazioni in tempo reale: la maggior parte delle soluzioni per verificare il rischio proveniente dalle terze parti è basata su fonti statiche: Informazioni acquisite periodicamente o addirittura questionari informativi nei quali la terza parte spiega le sue misure di sicurezza

Non lavorando in tempo reale la maggior parte delle soluzioni trasmettono numerosi falsi positivi (Noise). Come si sa troppe informazioni da verificare equivalgono a nessuna informazione



Rilevato un problema è la terza parte che deve risolverlo; è quindi necessario stabilire un canale di comunicazione comodo per aiutarla a risolvere il problema per evitare che si ripercuota su di noi

Cosa è Sling

- Sistema SaaS (Software as a Service) a cui si accede attraverso qualsiasi browser inserendo nome utente e password

- Non è necessaria alcuna installazione presso il cliente

- Lavora in modo assolutamente passivo; è solo necessario inserire nella propria area i nomi dei domini delle aziende che si desiderano monitorare

- Gestito a monte da esperti di Cyber Intelligence, analisti e ricercatori

Cosa fa Sling

- Monitora in tempo reale il rischio che le terze parti subiscano un attacco (che potrebbe poi estendersi all'azienda utilizzatrice di Sling)

- Lavora in modo assolutamente passivo; il cliente non deve fare altro che inserire nella propria area riservata i nomi di dominio delle terze parti che desidera monitorare

- Fornisce in Output un punteggio da 0 a 100 [Sling Score] che rappresenta la percentuale di rischio che una terza parte subisca un attacco.

- Fornisce anche gli strumenti necessari, già pronti per aiutare la terza parte a risolvere i problemi

Come lavora Sling

1: Discovery
Sling ricerca e mappa gli asset digitali della terza parte come lo farebbe un potenziale attaccante

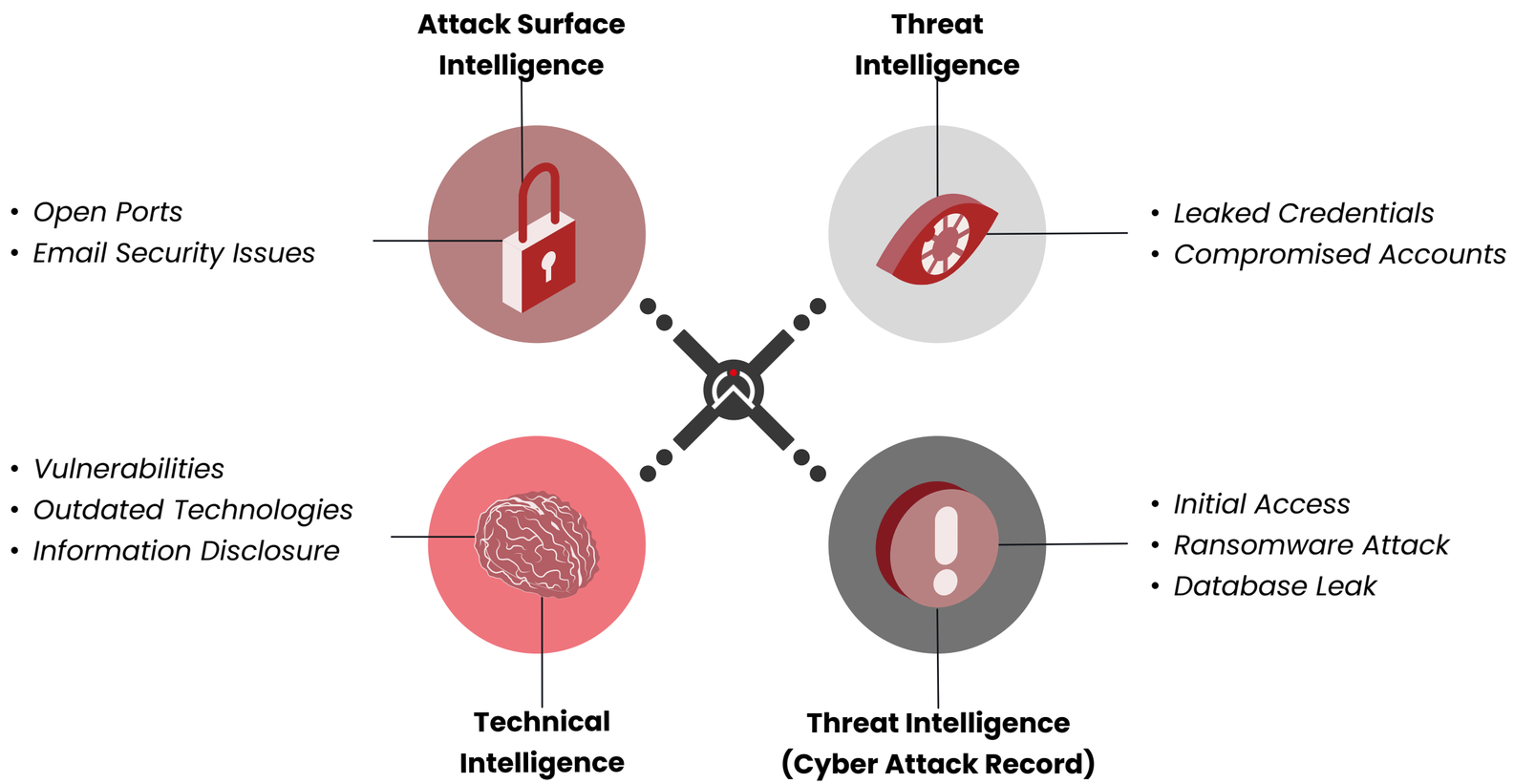
2: Collection & Analysis
Sling raccoglie sul Dark Net, su gruppi Telegram e molte altre fonti legate alla criminalità informatica dati relativi alla terza parte e altre informazioni che la potrebbero riguardare e li analizza

3: Assessment
Utilizzando un algoritmo A.I. proprietario addestrato utilizzando migliaia di casi di attacchi Sling calcola lo Sling Score che riflette in modo preciso il rischio che quella terza parte subisca un attacco

4: Actionable Output
È possibile esportare i dati rilevati e fornire alla terza parte la risoluzione dei problemi a partire dai più gravi al fine di migliorare subito la sicurezza

Intelligence Types

Sling collects cyber risks from multiple Darknet & surface web sources:



Quali problemi rileva Sling

Attack Surface intelligence	
	Porte Aperte
	Problemi di sicurezza delle email
Technical Intelligence	
	Vulnerabilità (in genere dovute a software da aggiornare)
	Tecnologie obsolete
	Information Disclosure (un attaccante è in grado di impadronirsi di dati del sistema aziendale)
Threat Intelligence	
	Rilevamento delle credenziali violate
	Account Compromessi
	Initial Access (un gruppo criminale ha trovato la strada per entrare nei sistemi aziendali e ha messo in vendita le informazioni sul Dark Net)
	Verifica attacchi Ransomware (in corso sull'azienda o su aziende simili e anche passati)
	Violazione di Database

Output di Sling: 1 – Sling Score

Dopo aver effettuato tutte le analisi e eliminato le informazioni non utili (Noise) Sling calcola lo Sling Score un punteggio fra 0 e 100 che riflette l'effettiva probabilità che un'organizzazione subisca un attacco.

Rischio Elevato (0 - 50)

Rischio Medio (51 - 75)

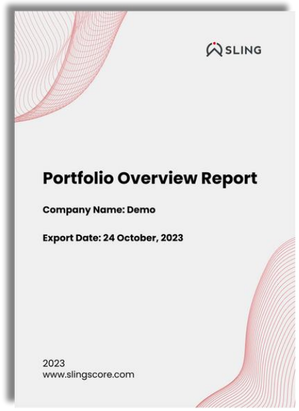
Rischio Basso (76 - 100)

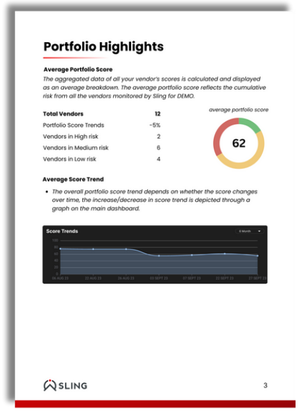
Lo Sling Score viene calcolato in TEMPO REALE 24/7 e si aggiorna automaticamente in base ai problemi risolti o a nuovi rischi che emergono

Output di Sling: 2 – Report

- Report scaricabili automaticamente dal sistema in formato PDF
- Spiegano cosa è Sling e i rischi rilevati
- Spiegano dettagliatamente come risolvere i problemi più importanti
- Comodi da condividere con le terze parti affinché possano mettersi a posto e non rischiare più di compromettere la sicurezza del cliente di Sling (e altri)

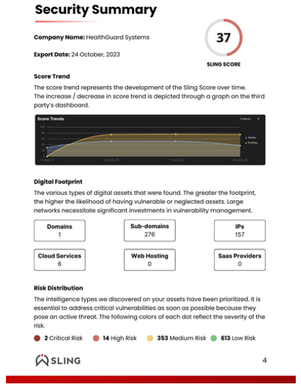
Sling Portfolio Report





Report generale su tutto il portafoglio delle Terze Parti per una visione globale del rischio

Sling Cyber Risk Report



Report su una singola terza parte da condividere con la terza parte stessa

Perché scegliere proprio Sling?

- Grazie al gruppo Kela (uno dei due leader mondiali nei progetti di Cyber Threat Intelligence) cui Sling appartiene accesso diretto ed in **tempo reale alle fonti del Dark Net** (Communities, forum Gruppi Telegram e altro). Le soluzioni concorrenti in genere acquistano dati da altre aziende e non hanno quindi l'informazione in tempo reale

- Monitora anche i gruppi di Hacker che agiscono a livello statale attaccando infrastrutture critiche e loro Terze Parti

- Algoritmo unico e proprietario addestrato utilizzando l'analisi di migliaia di attacchi ransomware e non solo

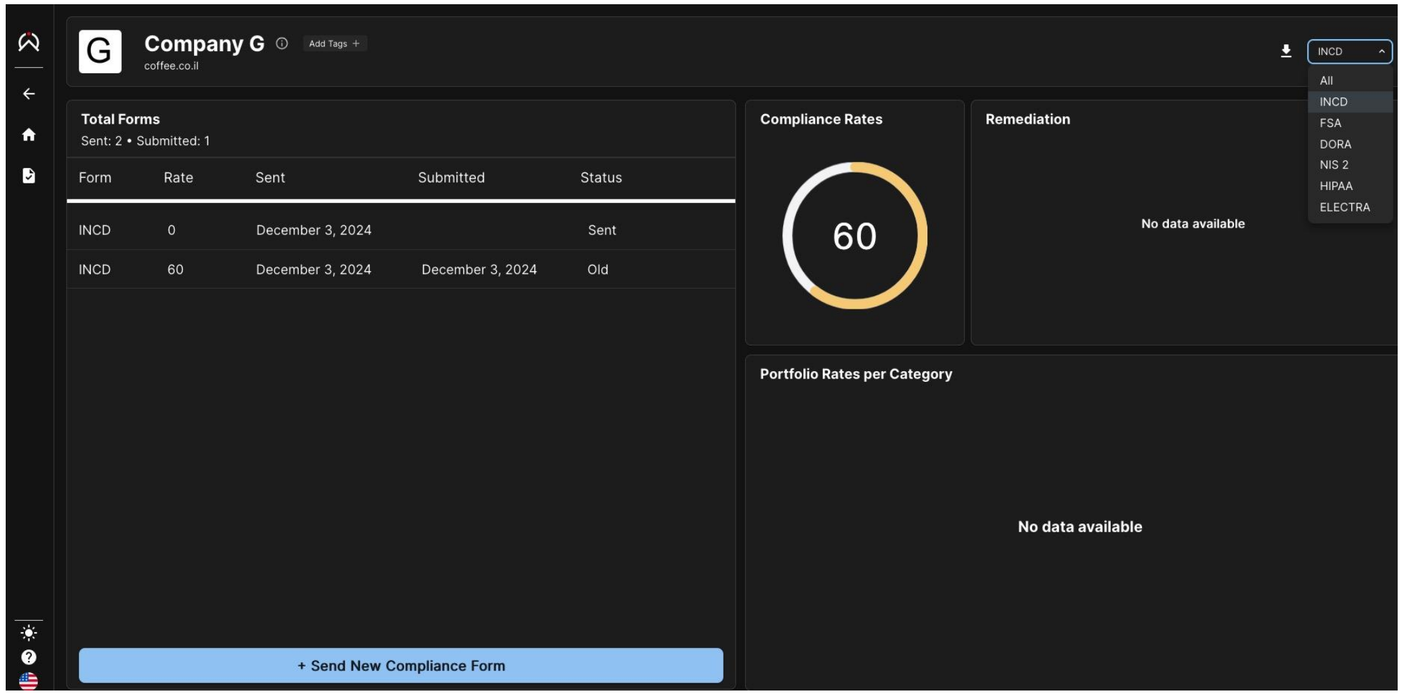
- Semplicità di utilizzo: è necessario solo il nome del dominio della terza parte che si desidera monitorare e Sling entro 24 ore fornisce l'analisi completa

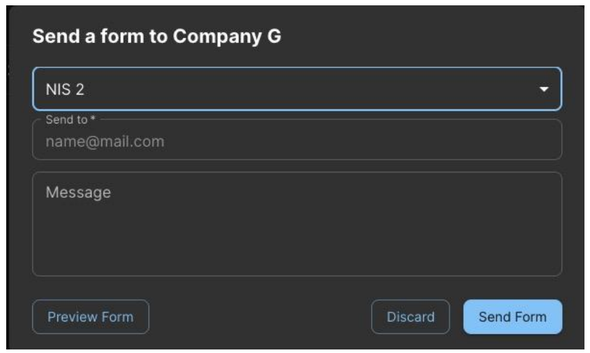
- Senza agenti – non intrusivo – non richiede alcuna autorizzazione dalle terze parti

- Fornisce in modo dettagliato le informazioni necessarie per porre rimedio ai problemi attraverso i report e una Chat GPT appositamente addestrata

- Dispone del modulo Compliance per gestire tutta la procedura dei questionari di conformità

Il modulo «Compliance»





NIS2

1. For all organizational entities (e.g., vendor's vendors, subcontractors, fourth parties, Nth parties) is there a contractual relationship that extends obligations to each entity?

- Yes
- No
- Other

2. Does the organization's assessment of third parties include identifying and evaluating all risks in relation to the contractual arrangement, including those presented by the geographic location of a subcontractor or dependency on a single provider for multiple activities?

- Yes
- No
- Other

3. Does the organization's senior management demonstrate leadership and commitment concerning the information security program by ensuring the policy objectives and requirements align with the strategic direction of the entire organization, and are integrated into the organization's processes?

- Yes
- No
- Other

SLING

E per proteggere la tua azienda?

- Inserisci nel sistema anche il **TUO dominio** come fai con quello delle terze parti
- Sling effettuerà l'analisi, ti fornirà il tuo score e l'elenco di tutti i problemi di cyber sicurezza della tua organizzazione
- Utilizzando i suggerimenti step by step del nuovo avanzatissimo sistema Chat GPT incluso nella piattaforma, e addestrato in modo specifico per risolvere i problemi di sicurezza informatica potrai rimediare a tutto quanto rilevato
- Dopo aver risolto i problemi potrai dimostrare a qualunque partner o grande cliente che la tua azienda è sicura
- Usufruisci di una Cyber Intelligence da Multinazionale ad un costo da PMI

SLING

NOVASYSTEM

GRAZIE