
Inside
INTELLIGENCE | SECURITY | INVESTIGATIONS
INSIDE:
la tua certezza
è qui dentro
Numero Aziendale
+41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch
LUGANO · LONDON · NEW YORK · MOSCOW · MILANO · ROMA · DUBAI · HONG KONG · CAPE TOWN · SAÕ PAULO

Inside

INTELLIGENCE | SECURITY | INVESTIGATIONS

CHI SIAMO

La prima Agenzia Investigativa specializzata in Business Security Intelligence

Numero Aziendale
+41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

Inside
INTELLIGENCE | SECURITY | INVESTIGATIONS

Siamo un'agenzia investigativa internazionale con Headquarter a Lugano, autorizzata con Licenza rilasciata dalla Polizia Cantonale – Repubblica e Cantone Ticino ai sensi della Legge sulle prestazioni private di sicurezza e investigazione (LPPS) del 09 novembre 2020 (RL 550.400) per lo svolgimento delle attività di investigazione e raccolta informazioni inerenti le persone.

INSIDE è un'agenzia di **Business Security Intelligence a Lugano**, nata nel 2014, dall'esperienza maturata nel tempo da un gruppo di professionisti attivi nel settore delle investigazioni.

La Business Security Intelligence è **un'attività strategica** che consente di analizzare, riconoscere, prevenire e neutralizzare possibili minacce nei confronti dei nostri clienti. In particolare, con il nostro metodo **Data Cross Investigation** incrociamo le informazioni commerciali con le informazioni derivanti dall'attività investigativa. In questo modo, riusciamo a fornire un risultato completo, preciso e puntuale ai nostri clienti. Supportiamo gli **Studi legali**, le **Aziende**, le **Assicurazioni** e le **Casse Malati** nella gestione dei rischi operativi, strategici, finanziari, informativi e di immagine fornendo una vasta gamma di servizi di investigazione, intelligence, due diligence, forensic, cyber security, sicurezza dei dati e delle informazioni.

A CHI SI RIVOLGONO I NOSTRI SERVIZI

Inside
INTELLIGENCE | SECURITY | INVESTIGATIONS

Numero Aziendale
+41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

I NOSTRI SERVIZI

Servizi

INSIDE offre un'ampia gamma di servizi dedicati a privati, aziende, assicurazioni, studi legali, sviluppati negli anni da un team di professionisti competenti e qualificati. INSIDE effettua indagini precise, con discrezione e nel rispetto delle normative vigenti in termini di privacy, garantendo sempre questi i 3 valori fondamentali:

CERTEZZA NEI COSTI

Quanto costa un investigatore privato? Trasparenza e nessuna sorpresa.

CERTEZZA NEI RISULTATI

Forniamo ai nostri clienti prove documentali valide in tribunale

CERTEZZA NEI TEMPI

Produciamo report concisi e trasparenti, in 3 giorni.

Inside INTELLIGENCE | SECURITY | INVESTIGATIONS

Numero Aziendale +41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

I NOSTRI SERVIZI

Investigazioni aziendali

Siamo specializzati nei **servizi informativi e d'intelligence a tutela del patrimonio aziendale**, utili ai fini della valutazione del rischio commerciale, di credito e reputazionale connesso a tutti gli stakeholders, per finalità di verifica dell'affidabilità, di recupero del credito, di due diligence e verifiche di conformità alla normativa sulla Compliance e Antiriciclaggio (Anti Money Laundering) con particolare approfondimento su vicende legali e giudiziarie che li abbiano coinvolti.

Similmente per la **valutazione reputazionale** di candidati manager e figure apicali in fase pre-assuntiva, le nostre indagini consentono di verificare il background curricolare e profilarne la compliance nella condotta professionale.

Inoltre in tutte le fasi successive all'instaurarsi di un **danno al patrimonio aziendale**, proveniente per esempio da **comportamenti scorretti e/o sleali** da parte di dipendenti e soci, attraverso i nostri servizi investigativi, siamo in grado di reperire elementi dalla valenza probatoria, utili a dimostrare l'illecito comportamentale e a **far valere i diritti dell'azienda in sede giudiziaria**.

La nostra consulenza permette di produrre prove concrete in tutti i casi in cui sia necessario accertare, far valere, o difendere un diritto in sede giudiziaria a tutela degli assets delle aziende.

Infedeltà aziendale

La normativa in materia di **infedeltà aziendale** mira a tutelare l'azienda contro ogni tipo di atteggiamento particolarmente sleale, messo in atto da **dipendenti o soci infedeli,** che potrebbe ledere o porre in posizione di svantaggio l'azienda stessa, come ad esempio il compimento, da parte di soci o dirigenti, di **atti di spionaggio e/o sabotaggio aziendale** o professionalmente scorretti.

Nel caso si sospetti infedeltà aziendale, INSIDE può avviare una serie di procedure d'indagine, tramite una rete di **investigatori privati** dislocati **in Svizzera** e nel resto del mondo, nei confronti del **socio infedele** o del **dipendente infedele** finalizzate documentare tutti i comportamenti scorretti e dannosi nei confronti dell'azienda e che violano il suddetto obbligo di fedeltà professionale.

L'**obbligo di fedeltà aziendale** rientra nella più ampia categoria del dovere di cooperazione da parte del dipendente che lo pone in una condizione di collaborazione e non di ostilità nei confronti dell'azienda.

VIOLAZIONE DEGLI OBBLIGHI DI FEDELTÀ E DEGLI ACCORDI DI RISERVATEZZA

L'obbligo di fedeltà ai lavoratori dipendenti, sancisce il divieto di "*trattare affari per conto proprio o di terzi in concorrenza con l'imprenditore" nonché di "divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa o farne uso in modo da poter recare ad essa pregiudizio*".

Nel primo caso si fa riferimento al divieto, sussistente sia durante che fuori l'orario di lavoro, di non svolgere attività che possano – in qualunque modo – entrare in conflitto con quelle del datore di lavoro. Il divieto riguarda in particolar modo quei lavoratori che, in ragione delle funzioni svolte, possono andare in contrasto con gli interessi aziendali, coinvolgendo una clientela comune al datore di lavoro.

Nel secondo caso si fa riferimento a tutte quelle informazioni riservate e strettamente connesse all'ambito aziendale che riguardano l'organizzazione aziendale, i flussi economici, gli ordini, la clientela, le relazioni con i fornitori, bilanci, dipendenti, e ogni altra vicenda "interna" all'azienda che se divulgata può risultare dannosa, anche in termini di competitività rispetto alle aziende concorrenti.

SVOLGIMENTO DI ATTIVITÀ LAVORATIVA DURANTE UN PERIODO DI DISOCCUPAZIONE

La condotta dell'impiegato che, nel periodo di fruizione del trattamento di disoccupazione, svolga attività lavorativa "in nero" presso altro datore di lavoro e percepisca quindi guadagni nascosto, è da considerarsi caso di infedeltà aziendale e, quindi, passibile di **licenziamento per giusta causa**. Il dipendente è infatti autore di un comportamento disciplinarmente rilevante talmente grave da non consentire, nemmeno in via temporanea, la prosecuzione del rapporto di lavoro.

USO DIFFORME DI BENI E STRUMENTI AZIENDALI

Nel caso si riscontrassero comportamenti scorrenti ai danni dell'azienda, **come licenziare un dipendente infedele?**

Il datore di lavoro, avvalendosi del nostro **servizio di investigazione per infedeltà di soci e dipendenti**, può l**icenziare per giusta causa un dipendente infedele** quando l'uso illecito, improprio o per finalità personali di beni o attrezzature informatiche di proprietà dell'azienda, costituisce un fattore di rischio per il datore di lavoro, non solo per il mantenimento dell'integrità delle apparecchiature adoperate ma soprattutto per la sicurezza dei dati di cui il lavoratore dispone.

A dimostrazione del **comportamento scorretto del dipendente**, il datore di lavoro deve necessariamente affidarsi ad un servizio di professionisti che accerterà l'illecito e procurerà prove inconfutabili e sempre valide in tribunale.

INSIDE svolge investigazioni su soci e dipendenti per accertare e documentare comportamenti lesivi come l'utilizzo di beni e strumenti aziendali per finalità diverse da quelle previste.

Indagini Pre Assunzione su un candidato

INSIDE è l'**agenzia di investigazione** con anni di esperienza nel settore investigativo in grado **controllare l'attendibilità del curriculum vitae** del candidato e verificare le informazioni e referenze inerenti le precedenti attività lavorative con focus su fascicoli giudiziari, civili e penali o problemi di natura finanziaria.

Ti forniremo il supporto per indagini preassunzione, al fine di **valutare l'onestà, l'affidabilità e le competenze** dichiarate **dal candidato selezionato**.

L'assunzione di una nuova figura professionale all'interno della propria struttura (si pensi ad un nuovo manager) è considerato un importante investimento per l'azienda. Una scelta troppo azzardata e senza le dovute precauzioni potrebbe però far cadere nelle mani sbagliate un ruolo

ritenuto strategico e, con il passare del tempo, rischierebbe di produrre forti ripercussioni da un punto di vista logistico, economico/finanziario, ma anche reputazionale per l'azienda stessa.

INSIDE mette a disposizione dei vertici aziendali deputati alla scelta della nuova figura, una procedura di **indagini preassuntive** nel totale rispetto di quanto previsto dalla Legge (statuto dei diritti dei lavoratori) con lo scopo di valutare l'idoneità del candidato. Effettuare indagini preassunzione si concretizza nella produzione di un dossier investigativo, accurato e su misura su persona fisica, finalizzato a definire l'indagato quale interlocutore per rapporti commerciali e/o incarichi professionali e/o societari. Sono presi in considerazione tutti gli indicatori di validità ed affidabilità di un soggetto nonché le informazioni raccolte in loco circa eventuali pregiudizi commerciali e/o personali.

La fiducia che il datore di lavoro deve poter riporre nel lavoratore è un presupposto fondamentale per creare un'azienda di successo. INSIDE è qualificata per adempiere ad ogni richiesta in merito ad indagini su dipendenti, futuri dipendenti o soci sempre nel pieno **rispetto delle normative vigenti sul lavoro e la privacy**.

Indagini sui dipendenti per assenteismo sul lavoro

Un **dipendente assenteista dal lavoro** può rappresentare un **grave problema** per un'azienda e può comportare disagi a datori di lavoro e colleghi.

La legge prevede la possibilità di recedere da un contratto "*prima della scadenza del termine, se il contratto è a tempo determinato, o senza preavviso, se il contratto è a tempo indeterminato, qualora si verifichi una causa che non consenta la prosecuzione, neppure a titolo provvisorio, del rapporto*".

Spesso, tuttavia, il datore di lavoro ha difficoltà a **licenziare un dipendente assenteista** e a far valere i propri diritti in assenza di **prove reali e documentate**.

INSIDE è l'**azienda investigativa** specializzata in **indagini sull'assenteismo dei dipendenti**, in grado di reperire e documentare elementi di prova utili a legittimare il licenziamento per assenteismo nei confronti del dipendente infedele e scorretto. Individuiamo le cause di assenza e/o i comportamenti opportunistici ed incompatibili con il rapporto di lavoro, al fine di dimostrare la sussistenza di fatti e ragioni valide che giustifichino l'assenza prolungata o meno del dipendente, nei casi di:

- Finta malattia
- Finto infortunio e svolgimento di una seconda attività
- Prolungamento dei tempi di guarigione
- Falsa attestazione di presenza

ASSENTEISMO PER FINTA MALATTIA DEL DIPENDENTE

La condotta del **lavoratore assenteista** che abbia agito fraudolentemente nei confronti del datore di lavoro simulando uno stato di **finta malattia** integra gli estremi di un inadempimento contrattuale tale da non consentire la prosecuzione, neppure transitoria, del rapporto di lavoro. **L'accertamento di assenteismo a lavoro** legittima il datore di lavoro a procedere con il **licenziamento del dipendente per giusta causa.**

Indagini per doppio lavoro

Un dipendente assente che finge malattia o sorpreso a svolgere doppio lavoro presso altro datore di lavoro, anche se familiare, è passibile di licenziamento per giusta causa.

Se il datore di lavoro sospetta comportamenti scorretti in azienda, quali un **dipendente che simula malattia** o **svolge un secondo lavoro**, ha diritto a rivolgersi ad un investigatore privato per avviare **indagini sullo svolgimento di una seconda attività** o sull'assenteismo dello stesso.

Inoltre, è da considerarsi comportamento incompatibile con lo stato di malattia ogni atto volontario che pregiudica o rallenta la guarigione che pertanto legittima il datore di lavoro ad accertamento da parte di un'agenzia investigativa, che potrà fornire le prove necessarie a provare l'illecito in tribunale.

Indagini su furti in azienda

Le **indagini per furto da parte di dipendenti in azienda** trovano richiesta crescente e per tale ragione è bene tutelarsi ricorrendo a metodi investigativi per accertare l'accaduto e porre rimedio al fenomeno che danneggia l'impresa e la sua organizzazione, prima che questo possa evolversi ed arrecare un ingente danno economico. L'**appropriazione illecita di beni in azienda, tangibili e intangibili**, è uno dei problemi che maggiormente ricorre nelle aziende. INSIDE è specializzata in investigazioni su furti in azienda e sabotaggi ed opera **su tutto il territorio svizzero e mondiale, grazie ad investigatori privati** dislocati. In caso di sospetto di appropriazione indebita di merce o denaro da parte di un dipendente è opportuno affidarsi a investigatori privati professionisti che possano svolgere **indagini** sul furto in azienda **valide in sede giudiziaria**. Le indagini su furto in azienda vengono svolte con **strumenti tecnologicamente avanzati** e nel pieno **rispetto delle leggi**. INSIDE supporta le imprese nella **raccolta di elementi di prova** che identificano gli autori del furto in azienda, incoraggiando le stesse ad adottare misure e strumenti di prevenzione idonei a ridurre eventuali rischi che potrebbero compromettere l'immagine aziendale.

Il furto di beni aziendali legittima il licenziamento per giusta causa, a prescindere dal valore e dall'entità dei beni sottratti. Ciò che rileva è infatti il comportamento disonesto del lavoratore che, in quanto tale, si ripercuote sul rapporto di fiducia tra le parti integrando gli estremi di "*una condotta suscettibile di porre in dubbio la futura correttezza dell'adempimento, in quanto sintomatica di un certo atteggiarsi del dipendente rispetto agli obblighi assunti*". Il licenziamento per furto sul posto di lavoro è un diritto del datore di lavoro.

Antisabotaggio

Le **indagini sul sabotaggio industriale** (patrimoniale o materiale) sono volte ad individuare il trasgressore **colpevole di danneggiamento o distruzione di dispositivi aziendali** al fine di indebolire il concorrente e porre fine all'attività illecita.

INSIDE, con il massimo della professionalità e della competenza, offre un servizio di antisabotaggio industriale in grado di **tutelare l'azienda da azioni scorrette da parte dei concorrenti o dipendenti infedeli**, i quali potrebbero essere interessati a sottrarre furtivamente beni, informazioni riservate o mettere sotto controllo dispositivi aziendali. Operiamo in Svizzera e nel mondo grazie a sedi dislocate ed investigatori privati che seguono protocolli meticolosi a garanzia del successo di ogni caso di investigazione su sabotaggi industriali e altri illeciti in ambito aziendale.

Il dipendente che, anche con il supporto di individui esterni alla compagine aziendale, **danneggia beni strumentali** dell'azienda quali macchinari, uffici e sistemi informatici o istiga i colleghi ad atti di sabotaggio, pone in essere una condotta che, lesiva dell'economia nonché dell'immagine aziendale, comporta la completa perdita di affidabilità da parte di quest'ultima, giustificando l'adozione della sanzione disciplinare del **licenziamento per giusta causa**. Come tutelarsi da sabotaggio industriale? L'unico metodo a prevenzione di atti che danneggiano l'azienda dall'interno è rivolgersi ad un'agenzia investigativa qualificata per la raccolta dei dati utili in giudizio attraverso un **dossier ben curato**.

Indagini su concorrenza sleale e contraffazione

I casi di **concorrenza sleale e contraffazione di prodotti o marchi** sono fenomeni sempre più **diffusi** anche a causa della sregolata ascesa dei paesi orientali, in primis la Repubblica Popolare Cinese, che immettono prodotti sui nostri mercati ignorando tutte le normative internazionali.

È indispensabile avviare indagini su concorrenza sleale al verificarsi di condotte illecite, da parte di uno o più concorrenti, ai danni dell'impresa e con lo scopo di guadagnare un vantaggio sul mercato.

COSA PREVEDE LA LEGGE FEDERALE SVIZZERA (LCSL) CONTRO LA CONCORRENZA SLEALE

È bene chiarire che: "*è sleale e illecito qualsiasi comportamento o pratica d'affari ingannevole, o altrimenti lesivo delle norme della buona fede, che influisce sui rapporti tra concorrenti o tra fornitori e clienti*". La normativa ha l'obiettivo di garantire una concorrenza leale e inalterata nell'interesse di tutte le parti interessate e punisce i soggetti che:

- Utilizzano metodi sleali di pubblicità e di vendita e altri comportamenti illeciti, denigrando altri, le sue merci, le sue opere, le sue prestazioni, i suoi prezzi o le sue relazioni d'affari con affermazioni inesatte, fallaci o inutilmente lesive.
- Agiscono in modo sleale nei confronti di un cliente in Svizzera segnatamente chiunque, nella vendita a distanza, senza giustificazione oggettiva, per motivi legati alla sua nazionalità, al suo domicilio, al luogo della sua stabile organizzazione, alla sede del suo fornitore di servizi di pagamento o al luogo di emissione del suo mezzo di pagamento.
- Incitano a violare o a rescindere un contratto.
- Corrompono attivamente o passivamente un lavoratore, un associato, un mandatario a favore proprio o di terzi.
- Sfruttano, senza esserne autorizzati, i risultati affidatigli di un lavoro, come ad esempio: offerte, calcoli o piani.
- Agiscono in modo sleale, sfruttando o comunicando ad altri segreti di fabbrica o di affari che hanno spiato o di cui sono venuti a conoscenza in modo illecito.

- Agiscono in modo sleale coloro che non rispettano condizioni di lavoro imposte anche al concorrente da norme giuridiche o per contratto o conformi agli usi professionali o locali.
- Utilizzano condizioni commerciali abusive.

La normativa federale Svizzera (LCSI) prevede, inoltre, che il soggetto leso o minacciato da concorrenza sleale nella clientela, nel credito, nella reputazione professionale, negli affari o in genere negli interessi economici può domandare al giudice:

a. di proibire una lesione imminente;
b. di far cessare una lesione attuale;
c. di accertare l'illiceità di una lesione che continua a produrre effetti molesti.

Può in particolare chiedere che una rettificazione o la sentenza sia comunicata a terzi o pubblicata. Può inoltre, giusta il Codice delle obbligazioni, proporre azioni di risarcimento del danno, di riparazione morale e di consegna dell'utile conformemente alle disposizioni sulla gestione d'affari senza mandato.

Indagini su infedeltà dei Soci

Le indagini sull'infedeltà dei soci permettono di **sapere con esattezza se un socio intrattiene rapporti conflittuali con la società di appartenenza**, ad esempio rivelando a terzi informazioni strettamente riservate ovvero ponendo in essere comportamenti contrari ai doveri che lo stesso dovrebbe adempiere in ragione della qualità di socio. L'indagine vi permetterà di individuare il socio infedele, evitando pericolose **"fughe di notizie" verso l'esterno**, al fine di preservare e valorizzare il know-how aziendale.

Gli agenti incaricati acquisiscono la documentazione relativa ai soggetti da sottoporre ad indagine, così da poter delineare un profilo personale e professionale; la fase successiva consiste in una procedura di supervisione, che può essere sia attiva (pedinamento) che passiva (appostamento). Tali tecniche consentono agli investigatori di raccogliere materiale fotografico e video, così da poter accertare in maniera inconfutabile la condotta del socio in un determinato contesto di tempo e luogo. La procedura di supervisione consente di accertare in maniera inconfutabile un'eventuale condotta scorretta. Al termine delle indagini, gli investigatori redigono una **relazione tecnica**: si tratta di un documento all'interno del quale vengono descritti il lavoro svolto ed i risultati con esso ottenuti. La relazione può essere impiegata dal mandante delle indagini con **valore probatorio** (per ottemperare all'onere della prova) nell'ambito di un eventuale processo giudiziario.

Controspionaggio industriale

INSIDE è un'agenzia investigativa specializzata in indagini per spionaggio industriale e capace di fornire assistenza sul territorio Svizzero ed estero, grazie alle sedi dislocate nel mondo e l'esperienza di ciascun investigatore privato. La **prevenzione ed il rafforzamento della sicurezza aziendale rappresentano una priorità**, per tale ragione è bene selezionare solo personale affidabile.

Lo **spionaggio industriale è un reato punibile secondo il Codice penale**, pertanto le nostre strategie di controspionaggio sono focalizzate non solo alla prevenzione del fenomeno ma alla **scoperta di elementi probatori e prove inconfutabili in fase di giudizio**.

Sempre più spesso le aziende si trovano a dover affrontare il delicato problema dello spionaggio aziendale messo in atto da dipendenti o organizzazioni a ciò preposte, il cui scopo fondamentale consiste nello sfruttare l'altrui lavoro per ottenere illecitamente benefici e vantaggi, utilizzando strumentazioni tecnologiche, strategie e metodologie molto diverse tra loro: si pensi ad esempio, ai furti di dati, oggetti, progetti, pianificazioni, brevetti, software, elenchi nominativi, liste clienti, ricerche di mercato.

Sempre più di frequente, **gli episodi di spionaggio avvengono** ad opera esclusiva nonché **grazie alla collaborazione degli stessi dipendenti**. È importante, dunque, ricorrere a tecniche di controspionaggio al fine di contrastare efficientemente tali fenomeni.

Ricorrere al controspionaggio significa quindi proteggere la propria azienda. INSIDE è in grado di offrirvi soluzioni specifiche e personalizzate per ogni esigenza, attraverso controlli mirati delle vulnerabilità di dipendenti, collaboratori e soci utilizzando strumenti tecnologici all'avanguardia.

Verifica Clientela

Il servizio permette di controllare la clientela (persona fisica o giuridica) verificandone l'eventuale presenza in specifiche banche dati, di seguito indicate:

- **Liste Antiterrorismo:** contenenti elenchi stilati da legislatori e istituzioni di diversi Paesi;
- **Liste Antiriciclaggio**: contenenti nominativi di persone fisiche ed enti coinvolti nel territorio svizzero in delitti di questo tipo, in conformità anche alle disposizioni previste in materia dalle leggi internazionali;
- **Liste PEP Internazionali**: contenenti più di 400.000 nominativi di Persone Esposte Politicamente, di oltre 240 Paesi, individuati sulla base delle direttive del GAFI contro il riciclaggio (Gruppo d'Azione Finanziaria Internazionale) e della normativa mondiale in materia;
- **Liste Siti di Gioco Illegale**: contenenti l'indicazione dei siti redirect e delle società internazionali cui fanno capo i siti privi di autorizzazione AAMS (Amministrazione Autonoma Monopoli di Stato);
- **Blacklist & Watchlist:** contenenti i nominativi di soggetti ricercati da autorità investigative nazionali o internazionali, quali ad esempio DIA, FBI, Interpol, o governi, ovvero soggetti figuranti in liste di autorità giudiziarie o agenzie governative, o ancora soggetti raggiunti da provvedimenti emessi da autorità finanziarie come FINMA, o da autorità di vigilanza.

I NOSTRI SERVIZI

Informazioni commerciali

Oltre ad offrire servizi di intelligence innovativi e dai contenuti tecnologici evoluti, INSIDE mette a disposizione INTELLIGENCEINSIDE.COM, il portale e-commerce pensato per le **esigenze degli studi legali** e sviluppato per l'acquisto online **di servizi info-investigativi per la Svizzera, l'Italia e per il resto del mondo**, tanto per la tutela e gestione del credito, quanto per le indagini reputazionali e di conformità.

I servizi info-investigativi acquistabili direttamente sul portale e-commerce, garantiscono ad ogni utente la **sicurezza di avere a portata di mano, soluzioni investigative rapide e innovative sia per il territorio svizzero che per le nazioni estere**.

Registro di Commercio Svizzera

Visure, documenti ufficiali e atti provenienti dalle camere di commercio in Svizzera. Per questo paese possono essere forniti, fascicoli completi sulla persona con cariche e partecipazioni, fascicoli completi sulla società con le informazioni della visura ordinaria, e visure camerali con le informazioni economiche e giuridiche relative a un'impresa.

FASCICOLO COMPLETO AZIENDA

Il servizio consente di ottenere tutte le informazioni allegate alla visura ordinaria (statuto, patti sociali vigenti, elenco pratiche depositate non ancora iscritte, società controllanti, partecipazioni in altre società). Viene fornito un quadro completo delle informazioni relative all'azienda in un unico documento:

- Informazioni da registro di commercio
- Evidenze di contatto
- Esponenti dirigenziali e aventi diritto di firma
- Indicazione del fatturato e numero dei dipendenti.

FASCICOLO COMPLETO PERSONA

Il servizio consente di ottenere tutte le informazioni connesse alle cariche e partecipazioni detenute dal soggetto nei pubblici registri.

Vengono fornite le informazioni relative al soggetto d'interesse in un unico documento:

- Mandati
- Informazioni desunte dal registro di commercio
- Informazioni di contatto

Informazioni Pre-Fido Svizzera

Le informazioni precontrattuali o pre-fido sono utili a definire la reale affidabilità commerciale dei clienti e partners in affari svizzeri in modo da prevenire e ridurre il rischio di insolvenza.

Le informazioni provengono innanzitutto da banche dati pubbliche, come nel caso di visure protesti e visure camerali, e sono successivamente integrate di notizie ufficiose circa la nomea sia della persona fisica che della persona giuridica, che vengono raccolte da più fonti. In questo modo è possibile avere un quadro completo della situazione e valutare la concessione del credito.

Con i nostri dossier pre-fido è possibile avere informazioni aggiornate su clienti oppure su fornitori, valutare la propria esposizione finanziaria, valutare il livello di affidabilità del prossimo partner commerciale, supervisionare l'operato del proprio ufficio commerciale e affinare le proprie strategie commerciali.

REPORT AZIENDE ONLINE

Il report fornisce in tempo reale le principali **informazioni pubbliche riguardanti le imprese con sede legale in Svizzera**. Nel dettaglio riporta:

- Informazioni legali e amministrative
- Composizione societaria (management, legami societari, informazioni relative all'attività svolta)
- Fatturato e indici finanziari
- Stato patrimoniale
- Sintesi dei principali dati dell'ultima annualità di bilancio disponibile
- Eventuali negatività a carico dell'azienda target e dei suoi esponenti
- Valore di affidamento consigliato
- Indice sintetico del livello di solvibilità.

VERIFICA DELLA SOLVIBILITÀ AZIENDA

Controllo della solvibilità **con indicatore del margine di rischio** e informazioni aggiuntive sull'azienda d'interesse:

- Verifica del grado di solvibilità con semaforo
- Consigli di azione
- Informazioni tratte dal registro di commercio
- Dati di pagamento aggiornati (servizio aggiuntivo).

TEMPISTICA DI PAGAMENTO

Verifica delle fatture passate al fine di valutare la tempestività di pagamento:

- Analisi pagamento delle ultime fatture
- Verifica della tempestività media dei pagamenti
- Calcolo di una percentuale di fatture note pagate con puntualità.

COMPANY CREDIT INFORMATION

Il report fornisce in tempo reale le principali informazioni pubbliche riguardanti le imprese con sede legale in Svizzera. Nel dettaglio riporta:

- Informazioni legali e amministrative.
- Composizione societaria (management, legami societari, informazioni relative all'attività svolta, organico).
- Eventuali negatività a carico dell'azienda target e dei suoi esponenti.
- Fatturato stimato.
- Sintesi dei principali dati dell'ultima annualità di bilancio disponibile.
- Indice sintetico del livello di solvibilità.
- Valore affidamento consigliato.

RINTRACCIO DATI DI BILANCIO (CANTON TICINO)

Il servizio consente di ottenere i dati di bilancio di società nel Canton Ticino. Le informazioni sono ottenute attraverso la raccolta per mezzo di contatti interpersonali, denominata **HUMan INTelligence, per il tramite di un'intervista investigativa diretta al target** e ai soggetti con i quali il medesimo intrattiene rapporti di collaborazione e più in generale tutti gli stakeholders (commercialista, consulente del lavoro, istituti di credito, ufficio contabilità, dipendenti, ecc...).

RINTRACCIO EFFETTIVA OPERATIVITÀ IMPRESA O SE TRATTASI SOLO DI C.D. "BUCA LETTERE" (CANTON TICINO)

Il servizio consente di verificare nel Canton Ticino l'operatività effettiva di un'impresa presso la sede dichiarata nel Registro di Commercio, ovvero la mera domiciliazione della posta all'indirizzo dichiarato.

VERIFICA DELLA SOLVIBILITÀ PERSONA

Controllo della solvibilità con indicatore del margine di rischio e informazioni sul soggetto d'interesse:

- Verifica del grado di solvibilità con semaforo
- Consigli di azione
- Data di nascita e indirizzi della persona fisica.

PERSONAL CREDIT INFORMATION

Per determinare l'affidabilità di una persona fisica quale interlocutore per rapporti commerciali e/o incarichi professionali e/o societari.

Nel dettaglio riporta:

- Verifica dati anagrafici ed indirizzo.

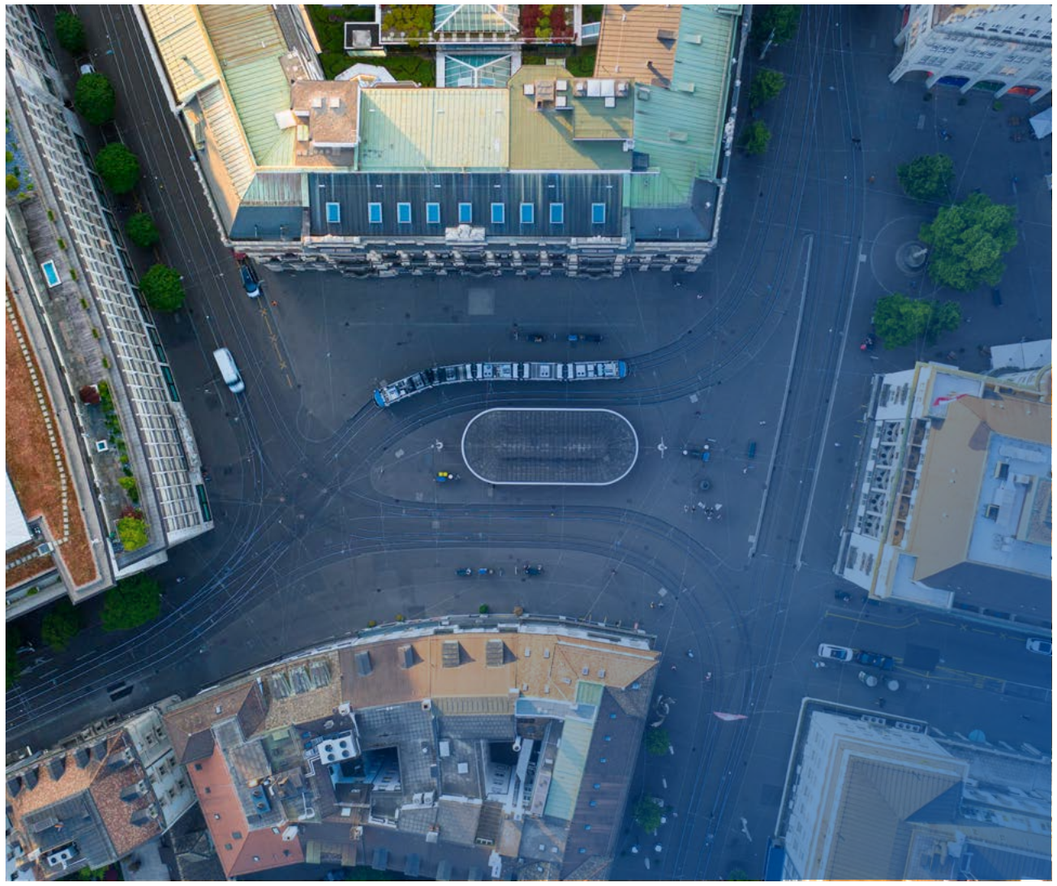
- Cariche ricorperte in società svizzere.
- Partecipazioni in società svizzere (Escluso SA).
- Controllo Ufficio.
- Esecuzione e Fallimenti (se fornito un giustificativo).
- Esperienze pagamenti.
- Pubblicazioni ufficiali.

ESTRATTO DELL'UFFICIO DI ESECUZIONE SU AZIENDA E PERSONA FISICA

Rassegna dei procedimenti esecutivi odierni e trascorsi:

- Estratto ufficiale di recupero del credito
- Procedimenti esecutivi in corso
- Eventuali recuperi risalenti agli ultimi due anni.

Ai sensi dell'art. 8a LEF, soltanto chi rende verosimile un interesse può consultare i verbali e registri degli uffici d'esecuzione e chiederne estratti. Per questo motivo, alla domanda d'informazione deve essere allegato un giustificativo, quale ad esempio una fattura che documenti l'esistenza di una trattativa di affari fra i soggetti e dalla quale si evince che il cliente è il creditore, un precetto, un decreto, o ancora un'ordinanza del giudice; trattasi dunque di un documento che attesti e comprovi l'interesse reale e legittimo del cliente ad effettuare le verifiche sul soggetto debitore. Naturalmente la pura curiosità non è considerata dalla legge come un interesse. Si può far valere un interesse legittimo nel caso della conclusione di un contratto; ad esempio, un locatore può verificare l'estratto del registro esecuzioni e fallimenti di un potenziale locatario.



Indagini Pre-Fido Italia

L'attività investigativa di INSIDE consente di **accedere a servizi di informazioni precontrattuali o pre-fido per l'Italia**. Questo genere di informazioni viene richiesto per valutare l'affidabilità commerciale di potenziali clienti, aziende e soci in affari al fine di verificare le possibilità di rischio di insolvenza.

Quando si ha a disposizione un dossier dettagliato con informazioni circa la **situazione economica e finanziaria del proprio contatto**, ottenute con una ricerca tra dati pubblici e le nostre investigazioni patrimoniali, è possibile prendere decisioni con maggiore consapevolezza e stabilire se vi è il r**ischio di andare incontro a operazioni commerciali infruttuose e potenzialmente pericolose**. Richiedere informazioni contrattuali o pre-fido è pratica comune di moltissime attività imprenditoriali, le quali ovviamente sono intenzionate a chiudere contratti con le maggiori garanzie possibili al fine di tutelare il proprio patrimonio.

Le prime informazioni che vengono raccolte da INSIDE provengono da banche dati pubbliche, come nel caso di visure camerali e visure protesti, le quali vengono successivamente affiancate da notizie ufficiose che riguardano la nomea della persona fisica o della persona giuridica, raccolte da più fonti vicine al soggetto investigato. In questo modo si può determinare la situazione economica, finanziaria e amministrativa dello stesso nella sua interezza e valutare in modo più realistico rischi e benefici della concessione del credito.

Attraverso le indagini commerciali pre-fido è possibile ottenere **dati aggiornati sui propri clienti oppure sui fornitori, valutando la presunta affidabilità del prossimo partner in affari**, analizzando le possibili varianti a livello finanziario, monitorando il lavoro svolto dal proprio ufficio commerciale e affinando le strategie commerciali della propria azienda.

Con INSIDE è possibile ottenere un report dettagliato sulla situazione patrimoniale complessiva di aziende italiane e persone residenti nel Paese, che viene redatto da consulenti investigativi della massima esperienza e non tramite gli algoritmi di un software, ed evitare rischi di insolvibilità.

DOSSIER COMPANY LIGHT

Il report consente di ottenere informazioni legali, economiche ed amministrative oltre a segnalare la presenza di elementi negativi (protesti e pregiudizievoli) sull'impresa oggetto della ricerca e tutti i suoi esponenti. Particolarmente **consigliato per la valutazione e concessione di fidi di piccola entità**.

Informazioni da registri pubblici:

- **Sintesi di Valutazione**: per valutare immediatamente la rischiosità dell'impresa
- **Dati Legali Identificativi**: reperiti dalla Camera di Commercio
- **Esponenti**: nominativi dei responsabili dell'impresa
- **Attività economica**: descrizione dell'attività economica e dell'oggetto sociale
- **Dipendenti dichiarati**: numero dei dipendenti rilevati dalla Camera di Commercio
- **Protesti e pregiudizievoli**: ricerca, su impresa ed esponenti, di protesti cambiari, interdizioni di firma, procedure concorsuali, pignoramenti ed ipoteche giudiziarie di natura immobiliare
- **Informazioni aggiuntive**: numero richieste effettuate a carico dell'impresa

DOSSIER COMPANY BASIC

Fornisce un elenco di dati reperiti da fonti ufficiali e sintetizzati da un modello di analisi statistica che, utilizzando sofisticati algoritmi, è in grado di **determinare il livello di rischiosità di un'impresa** e di consigliare un limite massimo di credito. Risulta di particolare utilità nella **valutazione e concessione di fidi** di media entità.

Il Report si compone delle seguenti sezioni:

- **Credit Limit:** evidenzia il limite massimo di credito consigliato dell'impresa in esame
- **Analisi di solvibilità**: viene espresso un rating ed un giudizio in merito alla solvibilità dell'impresa
- **Sintesi dei principali dati emersi**: estratto dei dati più importanti raccolti a carico dell'impresa
- **Dati Legali Identificativi**: reperiti dalla Camera di Commercio
- **Esponenti**: nominativi dei responsabili dell'impresa
- **Attività economica**: descrizione dell'attività economica e dell'oggetto sociale
- **Dipendenti dichiarati**: numero dei dipendenti rilevati dalla Camera di Commercio
- **Risk Press**: eventuali notizie stampa di carattere economico riguardanti l'impresa reperite da una rassegna stampa quotidiana su circa 150 testate nazionali
- **Proprietà immobiliari**: segnalazione (ed eventuale dettaglio) dei beni intestati all'impresa ed ai suoi principali esponenti responsabili
- **Protesti e pregiudizievoli**: ricerca, su impresa ed esponenti, di protesti cambiari, interdizioni di firma, procedure concorsuali, pignoramenti ed ipoteche giudiziarie di natura immobiliare
- **Informazioni aggiuntive**: numero richieste effettuate a carico dell'impresa
- **Dati di bilancio ed indici finanziari**: vengono riportate alcune delle principali voci estratte dall'ultimo bilancio depositato (solo per le Società di Capitali) ed alcuni dei più significativi indici finanziari

DOSSIER COMPANY FULL

Report completo che consente una valutazione approfondita sul rischio ed il livello di affidabilità di un'azienda, attraverso un'aggregazione di informazioni reperite da fonti ufficiali di natura pubblica estese anche ai legali rappresentanti ed esponenti; i principali dati economici sono sintetizzati in un modello di analisi statistica, ottenuto dall'elaborazione di sofisticati algoritmi in grado di **valutare il livello di rischiosità di un'impresa e di calcolare il limite massimo di credito consigliato**. Particolarmente utile nella valutazione e concessione di fidi di grande entità.

Il Report si compone delle seguenti sezioni:

- **Credit Limit**: evidenzia il limite massimo di credito consigliato dell'impresa in esame
- **Analisi di solvibilità**: viene espresso un rating ed un giudizio in merito alla solvibilità dell'impresa
- **Dati Legali Identificativi**: reperiti dalla Camera di Commercio
- **Sintesi dei principali dati emersi**: estratto dei dati più importanti raccolti a carico dell'impresa
- **Esponenti**: nominativi dei responsabili dell'impresa
- **Partecipazioni e Cariche Esponenti in altre imprese**: eventuali partecipazioni e cariche riscontrate a carico degli esponenti (primi tre) in altre imprese
- **Composizione Societaria**: elenco dei soci e la percentuale di capitale sociale detenuta da ciascuno di essi
- **Attività economica**: descrizione dell'attività economica e dell'oggetto sociale
- **Dipendenti dichiarati**: numero dei dipendenti rilevati dalla Camera di Commercio

- **Dati Camerali storici**: elenco di tutte le variazioni storiche societarie soggette a registrazione presso le Camere di Commercio
- **Risk Press**: eventuali notizie stampa di carattere economico riguardanti l'impresa reperite da una rassegna stampa quotidiana su circa 150 testate nazionali
- **Proprietà immobiliari**: segnalazione (ed eventuale dettaglio) dei beni intestati all'impresa ed ai suoi principali esponenti responsabili
- **Protesti e pregiudizievoli**: ricerca di protesti cambiari, interdizioni di firma, procedure concorsuali, pignoramenti ed ipoteche giudiziarie di natura immobiliare, attribuibili sia all'impresa, sia agli esponenti che dei soci di capitale, sia alle società in cui risultino cariche in capo agli esponenti
- **Informazioni aggiuntive**: numero richieste effettuate a carico dell'impresa
- **Dati di bilancio ed indizi finanziari**: viene riportato il bilancio riclassificato, estratto dall'ultimo depositato (solo per le Società di Capitali) ed alcuni dei più significativi indici finanziari

DOSSIER PERSONAL

Il report consente di ottenere **informazioni importanti sulle persone fisiche** (imprese individuali) per elaborare un quadro completo sull'affidabilità del soggetto.

- Ricerca dati ufficiali su Camere di commercio (anagrafica – partecipazioni in società – cariche ricoperte attuali e/o cessate – negatività)
- Recensioni stampa

REPORT IMPRENDITORE BASIC

Un prospetto informativo che offre un quadro sintetico per **valutare persone fisiche coinvolte in attività di impresa**. Permette anche di valutare gli eventi negativi legati a un soggetto e di verificarne gli indirizzi di residenza.

REPORT IMPRENDITORE FULL

Un ricco prospetto informativo che offre un quadro esaustivo per **valutare persone coinvolte in attività di impresa**. Oltre alle cariche e alle partecipazioni in altre società e alla presenza di eventi negativi, è possibile **visualizzare le unità immobiliari di un imprenditore**, con i relativi dettagli (terreno/fabbricato, dimensioni, ecc.).

PRE-AFFIDAMENTO STANDARD AZIENDA

Il report prevede la **verifica della situazione economica e patrimoniale dell'impresa**, ottenuta integrando i dati ufficiali dei pubblici registri con le risultanze ufficiose originate a mezzo di intervista investigativa effettuata attraverso la capillare rete di nostri corrispondenti. Il dossier consente la valutazione dello stato di salute economico-finanziario reale e dell'effettivo andamento commerciale dell'impresa, compresa la correttezza dei pagamenti.

Il Report si compone delle seguenti sezioni:

- **Credit Limit:** evidenzia il limite massimo di credito consigliato dell'impresa in esame
- **Analisi di solvibilità**: viene espresso un rating ed un giudizio in merito alla solvibilità dell'impresa
- **Sintesi dei principali dati emersi**: estratto dei dati più importanti raccolti a carico dell'impresa
- **Dati Legali Identificativi**: reperiti dalla Camera di Commercio
- **Esponenti**: nominativi dei responsabili dell'impresa

- **Attività economica**: descrizione dell'attività economica e dell'oggetto sociale
- **Dipendenti dichiarati**: numero dei dipendenti rilevati dalla Camera di Commercio
- **Risk Press**: eventuali notizie stampa di carattere economico riguardanti l'impresa reperite da una rassegna stampa quotidiana su circa 150 testate nazionali
- **Proprietà immobiliari**: segnalazione (ed eventuale dettaglio) dei beni intestati all'impresa ed ai suoi principali esponenti responsabili
- **Protesti e pregiudizievoli**: ricerca, su impresa ed esponenti, di protesti cambiari, interdizioni di firma, procedure concorsuali, pignoramenti ed ipoteche giudiziarie di natura immobiliare
- **Informazioni aggiuntive**: numero richieste effettuate a carico dell'impresa
- **Dati di bilancio ed indici finanziari**: vengono riportate alcune delle principali voci estratte dall'ultimo bilancio depositato (solo per le Società di Capitali) ed alcuni dei più significativi indici finanziari

PRE-AFFIDAMENTO ANALITICO AZIENDA

Il report prevede la verifica della situazione economica e patrimoniale dell'impresa, ottenuta integrando i dati ufficiali dei pubblici registri con le risultanze ufficiose originate a mezzo di intervista investigativa effettuata attraverso la capillare rete di nostri corrispondenti. Il dossier consente la **valutazione dello stato di salute economico-finanziario reale e dell'effettivo andamento commerciale dell'impresa**, compresa la correttezza dei pagamenti. Per le società di capitali vengono forniti inoltre i principali dati di bilancio. Il Report si compone delle seguenti sezioni:

Il Report si compone delle seguenti sezioni:

- **Credit Limit**: evidenzia il limite massimo di credito consigliato dell'impresa in esame
- **Analisi di solvibilità**: viene espresso un rating ed un giudizio in merito alla solvibilità dell'impresa
- **Dati Legali Identificativi**: reperiti dalla Camera di Commercio
- **Sintesi dei principali dati emersi**: estratto dei dati più importanti raccolti a carico dell'impresa
- **Esponenti**: nominativi dei responsabili dell'impresa
- **Partecipazioni e Cariche Esponenti in altre imprese**: eventuali partecipazioni e cariche riscontrate a carico degli esponenti (primi tre) in altre imprese
- **Composizione Societaria**: elenco dei soci e la percentuale di capitale sociale detenuta da ciascuno di essi
- **Attività economica**: descrizione dell'attività economica e dell'oggetto sociale
- **Dipendenti dichiarati**: numero dei dipendenti rilevati dalla Camera di Commercio
- **Dati Camerali storici**: elenco di tutte le variazioni storiche societarie soggette a registrazione presso le Camere di Commercio
- **Risk Press**: eventuali notizie stampa di carattere economico riguardanti l'impresa reperite da una rassegna stampa quotidiana su circa 150 testate nazionali
- **Proprietà immobiliari**: segnalazione (ed eventuale dettaglio) dei beni intestati all'impresa ed ai suoi principali esponenti responsabili
- **Protesti e pregiudizievoli**: ricerca di protesti cambiari, interdizioni di firma, procedure concorsuali, pignoramenti ed ipoteche giudiziarie di natura immobiliare, attribuibili sia all'impresa, sia agli esponenti che dei soci di capitale, sia alle società in cui risultino cariche in capo agli esponenti
- **Informazioni aggiuntive**: numero richieste effettuate a carico dell'impresa
- **Dati di bilancio ed indizi finanziari**: viene riportato il bilancio riclassificato, estratto dall'ultimo depositato (solo per le Società di Capitali) ed alcuni dei più significativi indici finanziari

Indagini Pre-Fido Estero

INSIDE può fornire servizi di investigazioni per l'ottenimento di **informazioni precontrattuali o pre-fido per nazioni estere**, al fine di verificare con maggiore precisione la situazione patrimoniale complessiva di un'azienda con sede estera in caso di trattative in corso, e valutare gli eventuali rischi di insolvenza. Il servizio viene offerto per stati dell'Europa e nazioni extraeuropee, combinando dati pubblici con le notizie ufficiose provenienti da corrispondenti locali.

REPORT AZIENDE ESTERO ONLINE

Il **report aziende online per le nazioni estere** fornisce in tempo reale le principali **informazioni commerciali pubbliche riguardanti le imprese con sede legale all'estero**, e permette di conservare la discrezione che si vuole mantenere al fine di non rovinare il rapporto di fiducia che si vuole instaurare con il nuovo partner commerciale. L'evasione del servizio è immediata e viene effettuata via mail.

Il report aziende estero riporta nel dettaglio le seguenti informazioni:

- Informazioni legali e amministrative
- Composizione societaria (management, legami societari, informazioni relative all'attività svolta)
- Fatturato azienda e indici finanziari (se disponibile)
- Stato patrimoniale (se disponibile)
- Sintesi dei principali dati dell'ultima annualità di bilancio disponibile (se disponibile)
- Eventuali negatività a carico dell'azienda target e dei suoi esponenti

DOSSIER COMPANY PRE-FIDO ESTERO

Per determinare l'affidabilità commerciale di una azienda estera e minimizzare il rischio nelle transazioni commerciali internazionali.

Il dossier consente di **verificare l'affidabilità economica, la solvibilità e il grado di coinvolgimento di imprese e società** aventi sede legale all'estero, quali potenziali clienti, ovvero di monitorare i clienti storici o anche conoscere la solidità finanziaria di un fornitore.

La ricerca viene effettuata attraverso la consultazione dei dati ufficiali*, l'analisi delle risultanze provenienti dalle fonti aperte (Open Source Intelligence o OSINT), la verifica dei database internazionali e le notizie provenienti da corrispondenti locali.

Nello specifico sono riportati:

1. Dati di sintesi
2. Anagrafica con dettaglio proveniente da dati legali e amministrativi ufficiali*
3. Sedi attive e cessate
4. Soci
5. Esponenti
6. Partecipazioni
7. Beni immobili di proprietà
8. Informazioni e analisi da fonti aperte (OSINT) sulla società, i soci e gli esponenti attuali con focus sulle notizie di tenore negativo.
9. Evidenze da Database internazionali sulla società, i soci e gli esponenti
10. Stato dell'attività e dati finanziari
11. Eventi pregiudizievoli ufficiali
12. Dati ufficiosi riguardanti l'organico e l'ambito di operatività
13. Dati ufficiosi riguardanti le esperienze di pagamento
14. Fornitori e loro referenze
15. Notizie di stampa
16. Analisi e comparazione settoriale
17. Bilancio e analisi di bilancio
18. Referenze bancarie
19. Score creditizio e rating di affidabilità
20. Notizie e informazioni ufficiose provenienti da corrispondenti locali.

*DATI UFFICIALI

Il dossier conterrà dati ufficiali di natura legale e amministrativa provenienti dal EBR (European Business Register) per i Paesi e nelle combinazioni di seguito indicate:

AREA 1: Andorra – Austria – Belgio – Francia – Germania – Gibilterra – Gran Bretagna – Irlanda – Olanda -Portogallo – Principato di Monaco – Spagna (comprese Isole Canarie e Baleari).

AREA 2: Albania – Algeria – Arabia Saudita – Bielorussia – Bosnia & Erzegovina – Bulgaria – Canada – Cipro – Croazia – Danimarca – Egitto – Emirati Arabi – Estonia – Finlandia – Grecia – Islanda – Lettonia – Libano – Libia – Liechtenstein – Lituania – Lussemburgo – Macedonia del Nord – Malta – Marocco – Moldavia – Montenegro – Norvegia – Polonia – Repubblica Ceca – Romania – Russia – Serbia – Slovacchia – Slovenia – Stati Uniti – Svezia – Tunisia – Turchia – Ucraina – Ungheria.

AREA 3: Cina – Giappone e i rimanenti Paesi non descritti nelle aree precedenti.

Indagini Recupero Crediti

Le indagini per recupero crediti rappresentano un'**attività preliminare indispensabile** ed imprescindibile e sono volte, oltre all'individuazione di dati confidenziali, anche alla **verifica di beni intestati aggredibili**. Talvolta i debitori risultano nullatenenti, anche intenzionalmente, vanificando ogni tentativo di recupero delle somme dovute o di aggredire qualunque bene non direttamente intestato; si evince pertanto l'importanza delle investigazioni per il recupero crediti.

L'indagine per recupero crediti **è volta a ricevere il pagamento**, totale o parziale, **dell'importo dovuto** da parte del debitore per i beni e servizi usufruiti. La procedura di recupero crediti potrà avvenire in **via stragiudiziale**, ovvero con accordo tra le parti e per mezzo di un mediatore, **o in via giudiziale** e con una sentenza emessa dal giudice. Ambo le soluzioni sono valide, sebbene i tempi di recupero crediti possano variare significativamente nel secondo caso; qualora il debitore non collaborasse, si potrà procedere con la risoluzione del caso attraverso un processo civile per il recupero dei crediti.

Il servizio è consigliato all'insorgere di un contenzioso e permette di valutare l'effettiva situazione finanziaria e patrimoniale del debitore.

RINTRACCIO DOMICILIO EFFETTIVO (CANTON TICINO E ALTRI CANTONI)

Il servizio fornisce informazioni circa la residenza ufficiale e l'effettivo domicilio di una persona fisica.

RINTRACCIO ATTIVITÀ LAVORATIVA (CANTON TICINO)

Nel caso di soggetti lavoratori nel Canton Ticino, titolari di:

- permesso G (frontaliere)
- permesso B (domiciliato)
- permesso C (residente)

il servizio consente di **individuare il datore di lavoro alle cui dipendenze il soggetto lavora regolarmente**, il tipo di contratto e, ove disponibile, l'emolumento percepito al fine di effettuare un pignoramento del salario per recupero del credito. Le informazioni sono ottenute attraverso la raccolta di informazioni per mezzo di contatti interpersonali, denominata **HUMan INTelligence**, per il tramite di un'intervista investigativa diretta al target e ai soggetti con i quali il medesimo intrattiene rapporti di collaborazione e più in generale tutti gli stakeholders (commercialista, consulente del lavoro, istituti di credito, ufficio contabilità, dipendenti, ecc…).

Ai sensi dell'art. 8a LEF, soltanto chi rende verosimile un interesse può consultare i verbali e registri degli uffici d'esecuzione e chiederne estratti. Per questo motivo, alla domanda d'informazione deve essere allegato un giustificativo, quale ad esempio una fattura che documenti l'esistenza di una trattativa di affari fra i soggetti e dalla quale si evince che il cliente è il creditore, un precetto, un decreto, o ancora un'ordinanza del giudice; trattasi dunque di un documento che attesti e comprovi l'interesse reale e legittimo del cliente ad effettuare le verifiche sul soggetto debitore. Naturalmente la pura curiosità non è considerata dalla legge come un interesse. Si può far valere un interesse legittimo nel caso della conclusione di un contratto; ad esempio, un locatore può verificare l'estratto del registro esecuzioni e fallimenti di un potenziale locatario.

STIMA REDDITUALITÀ LAVORATIVA E QUANTIFICAZIONE PATRIMONIO (CANTON TICINO)

Il servizio consente di reperire informazioni utili a determinare la **stima su base annua sia dei redditi lavorativi percepiti** sia di quelli derivanti dalla **sostanze patrimoniali** detenute dal soggetto d'interesse nel Canton Ticino. Le informazioni sono ottenute attraverso la raccolta di informazioni per mezzo di contatti interpersonali, denominata **HUMan INTelligence,** per il tramite di un'intervista investigativa diretta al target e ai soggetti con i quali il medesimo intrattiene rapporti di collaborazione e più in generale tutti gli stakeholders (commercialista, consulente del lavoro, istituti di credito, ufficio contabilità, dipendenti, ecc…).

RINTRACCIO VEICOLI DA NOMINATIVO (CANTON TICINO)

Il servizio consente di individuare i veicoli intestati ad un nominativo nel Canton Ticino. Le informazioni sono ottenute attraverso la **raccolta di informazioni per mezzo di contatti interpersonali,** denominata **HUMan INTelligence**.

RINTRACCIO VEICOLI DA TARGA (CANTON TICINO)

Il servizio consente di individuare nel Canton Ticino il proprietario del auto/motoveicolo a partire dalla targa svizzera, **anche nel caso di targhe soggette al blocco della comunicazione** dei dati personali dagli elenchi pubblici.

Le informazioni sono ottenute attraverso la r**accolta di informazioni per mezzo di contatti interpersonali,** denominata **HUMan INTelligence**.

RINTRACCIO PROPRIETÀ IMMOBILIARI DA NOMINATIVO (CANTON TICINO)

Il servizio è volto ad individuare le proprietà immobiliari di un soggetto nel Canton Ticino. Le informazioni sono ottenute attraverso la r**accolta di informazioni per mezzo di contatti interpersonali,** denominata **HUMan INTelligence**.

VISURA IPOTECARIA (CANTON TICINO)

Il servizio di visura ipotecaria in Svizzera fornisce l'elenco dei gravami presenti sulle proprietà immobiliari di un soggetto.

RINTRACCIO NATANTI DA NOMINATIVO – SVIZZERA (CANTON TICINO + TUTTI I CANTONI)

Il servizio consente di individuare i natanti intestati ad un nominativo.

Le informazioni sono ottenute attraverso la **raccolta di informazioni per mezzo di contatti interpersonali,** denominata **HUMan INTelligence**.

RINTRACCIO UBO (ULTIMATE BENEFICIAL OWNER)

Report consigliato per l'adempimento delle **procedure antiriciclaggio** da parte dei professionisti che consente l'identificazione nel Canton Ticino della persona fisica per conto della quale è realizzata un'operazione o un'attività, ovvero, nel caso di entità giuridica, la persona o le persone fisiche che, in ultima istanza, possiedono o controllano tale entità, ovvero ne risultano beneficiari. Le informazioni sono ottenute attraverso la raccolta di informazioni per mezzo di contatti interpersonali, denominata **HUMan INTelligence**, per il tramite di un'intervista investigativa diretta al target e ai soggetti con i quali il medesimo intrattiene rapporti di collaborazione e più in generale tutti gli stakeholders (commercialista, consulente del lavoro, istituti di credito, ufficio contabilità, dipendenti, ecc...).

Indagini Finanziarie

INSIDE offre servizi di indagini finanziarie utili per la risoluzione di controversie legate alle mancate risoluzioni di debiti tra privati e aziende. Nell'ambito delle **informazioni per il recupero del credito**, la ricerca di conti correnti bancari e postali in capo al soggetto debitore risulta determinante preliminarmente al pignoramento presso terzi. **Conoscendo preventivamente la patrimonialità** della controparte è infatti possibile **intraprendere** quelle che sono le **azioni giudiziali consentite** per il recupero del credito con maggiore consapevolezza e minore rischio di infruttuosità della procedura.

I professionisti di INSIDE possono fornire per Svizzera, Italia e altre 32 nazioni estere (europee, asiatiche e americane) dossier investigativi per la ricerca di informazioni finanziarie in tutto il mondo. Le attività di indagine vengono estese anche alle banche on-line, e originate attraverso attività di HUMan INTelligence, ovvero raccogliendo delle informazioni tramite interviste investigative tenute presso gli istituti di credito, al fine di geolocalizzare le eventuali relazioni bancarie e postali della persona fisica o giuridica richiesta, con possibilità di conoscere la giacenza media.

INFORMAZIONI FINANZIARIE – SVIZZERA

Il nostro dossier investigativo per la ricerca delle **informazioni finanziarie in Svizzera** è in grado di rilevare i **conti correnti bancari** della persona fisica o giuridica richiesta **in tutto il territorio** elvetico con indicazione, ove possibile, della capienza stimata.

L'**indagine bancaria** per il **rintraccio dei conti correnti svizzeri** viene svolta rispettando principalmente tre fasi:

1. acquisizione dei dati e delle **informazioni finanziarie inerenti al titolare dei conti correnti** attivati presso un istituto di Credito svizzero,
2. attività di **rintraccio dei conti bancari** che può essere svolta su base locale, regionale o nazionale e che include un numero più o meno ampio di istituti di credito fisici e online.
3. stesura del **dossier investigativo** nel quale vengono illustrati i risultati ottenuti dalle indagini bancarie svolte.

Nel dossier vengono riportati i seguenti dati:

- conti correnti bancari
- conti correnti online
- capienza media stimata

Il dossier investigativo per la ricerca di **informazioni finanziarie Svizzera** ha valore informativo a supporto del **processo giudiziario per il recupero del credito**, oppure, può integrare i riscontri emersi da una più ampia azione di due diligence a carico di una società con dati oggettivi ottenuti per mezzo di procedure professionali e certificate.

INDAGINI FINANZIARIE "SILVER" – ITALIA

Il **dossier investigativo per la ricerca delle Informazioni Finanziarie Silver,** è in grado di **geolocalizzare** gli eventuali **conti bancari e postali della persona fisica o giuridica richiesta** e di fornire in modo preventivo le informazioni relative alla patrimonialità del debitore, per intraprendere, con maggiore consapevolezza e con un minore rischio di infruttuosità della procedura, le azioni giudiziali consentite per il **recupero del credito**.

La **ricerca delle informazioni finanziarie** viene svolta attraverso attività di **Human Intelligence**, ovvero raccolta di informazioni, assunte a mezzo intervista investigativa presso gli istituti di Credito ed è estesa alle **banche** (escluse on-line) e a **Poste Italiane**.

Nel dossier investigativo Silver vengono riportate, se rilevate, le seguenti informazioni:

- conti correnti bancari
- conti correnti postali
- libretti di risparmio
- carte prepagate con IBAN

L'indagine finanziaria Silver non include informazioni relative alla **capienza stimata dei conti correnti**, le quali possono essere ottenute attraverso il dossier investigativo Gold e Platinum.

INDAGINI FINANZIARIE "GOLD" - ITALIA

Le **indagini Finanziarie Gold** sono in grado di fornire Informazioni relative ad un rapporto intrattenuto da una persona fisica o giuridica, con istituti di credito, quali **banche fisiche** e **Poste Italiane**, in tutto il territorio nazionale.

La **ricerca delle informazioni finanziarie** viene svolta attraverso attività di **Human Intelligence**, ovvero raccolta di informazioni, assunte a mezzo intervista investigativa presso gli istituti di Credito.

Nel **dossier investigativo GOLD** vengono riportate, se rilevate, le seguenti informazioni:

- conti correnti bancari
- conti correnti postali
- libretti di risparmio
- carte prepagate con IBAN
- **giacenza media stimata**

INDAGINI FINANZIARIE "PLATINUM" - ITALIA

L'**indagine finanziaria Platinum** è in grado di fornire in modo completo e con il massimo grado di approfondimento, le eventuali relazione bancarie della persona fisica o giuridica con **estensione alle banche online e a Poste Italiane**.

Le **informazioni finanziarie** contenute nel dossier, vengono raccolte attraverso attività di Human Intelligence, assunte a mezzo intervista investigativa presso i vari istituti di Credito, in tutto il territorio nazionale.

Nel **dossier investigativo PLATINUM** vengono riportate, se rilevate, le seguenti informazioni:

- conti correnti bancari **con estensione banche on-line**
- conti correnti postali
- libretti di risparmio
- carte prepagate con IBAN
- giacenza media stimata

INDAGINI FINANZIARIE "DIAMOND" - ITALIA

L'indagine **economico finanziaria** è volta all'individuazione di eventuali conti correnti bancari e conti postali della persona fisica o impresa.

Numero Aziendale +41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

La ricerca dei conti correnti viene svolta su tutto il territorio nazionale, con estensione alle Banche e a Poste Italiane e viene generata attraverso **attività di HUMan INTelligence**, ovvero raccolta di informazioni, assunte a mezzo intervista investigativa presso gli Istituti di Credito

Nel **dossier investigativo DIAMOND** vengono riportate, se rilevate, le seguenti informazioni:

- conti correnti bancari con estensione banche on-line
- conti correnti postali
- libretti di risparmio
- carte prepagate con IBAN
- giacenza media stimata
- **acquisto e vendita di azioni e/o titoli pubblici**

INDAGINI FINANZIARIE "DE CUIUS" - ITALIA

Il dossier investigativo per la ricerca di **informazioni finanziarie de cuius** è volto all'individuazione di eventuali **conti correnti bancari e conti postali della persona defunta** con indicazione della giacenza media stimata.

Questo tipo di **indagine bancaria persona** è specificatamente indicata nel caso di successione mortis causa per rintracciare l'eventuale massa patrimoniale ereditaria detenuta dal soggetto deceduto.

Nel dossier investigativo DE CUIUS vengono riportate, se rilevate, le seguenti informazioni:

- conti correnti bancari con estensione banche on-line
- conti correnti postali
- **rapporti di conto corrente estinti**
- libretti di risparmio
- carte prepagate con IBAN
- giacenza media stimata
- **locazioni immobiliari**
- **comodato e donazioni**
- **preliminari di acquisto registrati**
- **compravendita immobili e terreni**
- **aggiudicazione appalti**
- **acquisto e vendita di azioni e/o titoli pubblici**
- **fideiussioni**
- **mutui bancari (esclusi finanziamenti)**

La **ricerca dei conti correnti del defunto** viene svolta su tutto il territorio nazionale, con estensione alle **Banche e a Poste Italiane** e viene generata attraverso attività di **HUMan INTelligence**, ovvero raccolta di informazioni, assunte a mezzo intervista investigativa presso gli Istituti di Credito.

INDAGINI FINANZIARIE - ESTERO

INSIDE offre servizi di **indagini finanziarie per le nazioni estere**, che consentono di risolvere tutte le controversie relative alla non risoluzione di un debito tra aziende oppure tra privati. Grazie all'attività dei nostri consulenti investigativi e dei nostri collaboratori internazionali è possibile apprendere di più sulla situazione patrimoniale di un soggetto estero con il quale si hanno delle difficoltà a risolvere un debito, al fine di valutare se intraprendere o meno le dovute azioni per il recupero del credito.

Numero Aziendale +41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

I NOSTRI SERVIZI

Indagini reputazionali

Indagini Reputazionali

Con INSIDE è possibile richiedere **indagini reputazionali all'interno del territorio elvetico**, al fine di raccogliere informazioni su persone o società, per mettere in evidenza eventuali rischi economici o reputazionali derivanti da una collaborazione con partner commerciali, clienti o competitor. Il team di consulenti investigativi della nostra agenzia può **indagare gli organigrammi societari di aziende con sede legale in Svizzera** e individuare controversie e conflitti di interesse, oppure può scoprire più **informazioni su una persona fisica**, sia per dipendenti già assunti che nuove assunzioni.

La **gestione dei rischi d'impresa** è una pratica fondamentale all'interno di una società che desidera perseguire obiettivi di crescita ed in virtù di questo è necessario comprendere a priori il livello di rischio che l'impresa è disposta ad assumere per raggiungere ciascun traguardo, con il supporto di uno studio adeguato delle strategie.

Governance, gestione dei rischi e conformità (GRC) sono pilastri imprescindibili della gestione aziendale e da questi ne conseguono le decisioni della board manageriale. Tali attività sono strettamente legate e puntano a identificare **rischi d'impresa**, aree di **miglioramento delle performance aziendale e della produttività** nonché al conseguimento degli obiettivi ed al mantenimento della crescita.

INSIDE è un'agenzia investigativa riconosciuta a livello internazionale e con sedi dislocate in diverse parti del mondo in grado di studiare ed integrare un **programma di Governance, Risk Management & Compliance** ai processi aziendali ottenendo risultati concreti nel tempo.

Il dossier che prepareremo conterrà tutte le informazioni rilevanti, proveniente da fonti esterne, **relative a soggetti giuridici**.

Ad essere oggetto di valutazione è il grado di esposizione al rischio delle persone giuridiche o enti, e quindi dei relativi esponenti; si studia l'operato degli stessi (**rischio operativo**) ed il trascorso dal punto di vista reputazionale (**rischio reputazionale**), le condizioni economiche, il **rischio di compliance** (vicende legali-giudiziarie).

Numero Aziendale
+41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

L'intelligence per l'analisi del rischio reputazionale e di compliance

Al giorno d'oggi il concetto di "rischio reputazionale" acquisisce sempre maggior importanza per le aziende in crescita. Le nuove opportunità e i nuovi mercati, l'aumento del numero di controparti strategiche e commerciali con le quali collaborare accrescono anche i rischi associati a tale espansione, all'affidabilità e onorabilità dei potenziali partner e all'adeguatezza e conformità delle loro organizzazioni.

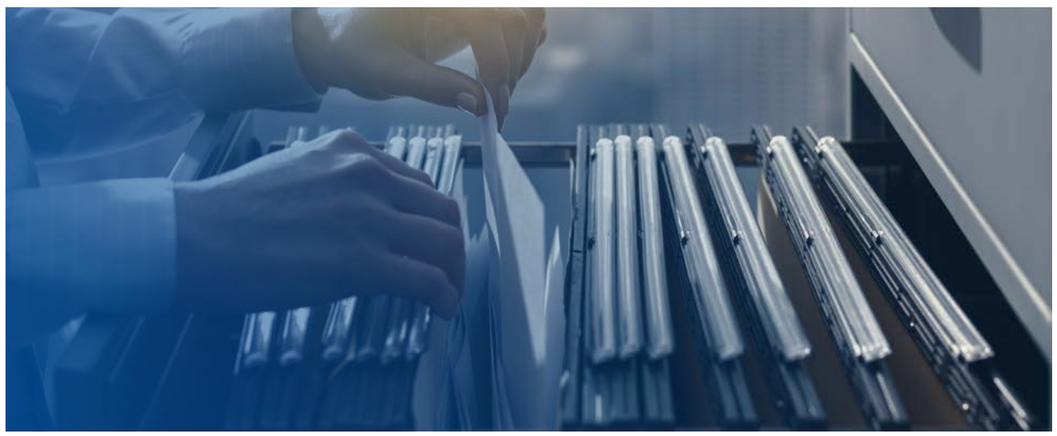
L'esigenza di relazionarsi con persone e imprese la cui "reputazione" ed il profilo di compliance siano ineccepibili è divenuta una priorità per la tutela dell'immagine e del patrimonio aziendale.

La conoscenza di tutte le controparti con cui si collabora, dei soggetti che le controllano, direttamente o indirettamente, e di tutte quelle parti ad essi correlate e l'identificazione di tutti gli elementi di anomalia o di potenziale rischio (red flags) cui si è esposti è indispensabile per fronteggiare i rischi operativi, strategici e di compliance dell'azienda.

Disporre di tutte le informazioni utili ad assumere le decisioni più importanti ed implementare un processo strutturato di qualifica e monitoraggio dei fornitori che tenga conto dei rischi reputazionali ed economici, è la finalità delle BACKGROUND & DUE DILIGENCE INVESTIGATIONS.

OBIETTIVI

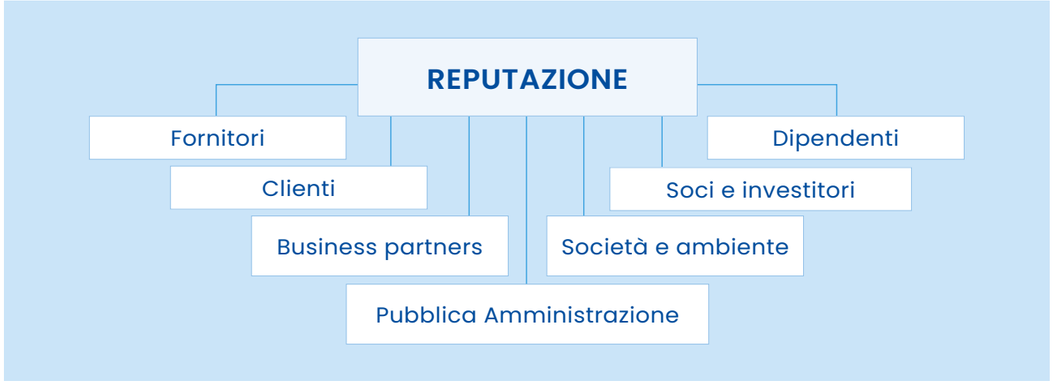
- Identificare i rischi di conformità
- Valutare i rischi reputazionali e di immagine
- Prevenire impatti operativi ed economici
- Stabilire partnership fondate su fiducia, rispetto e sostegno
- Pianificare strategie di remedation e mitigazione del rischio



Numero Aziendale
+41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

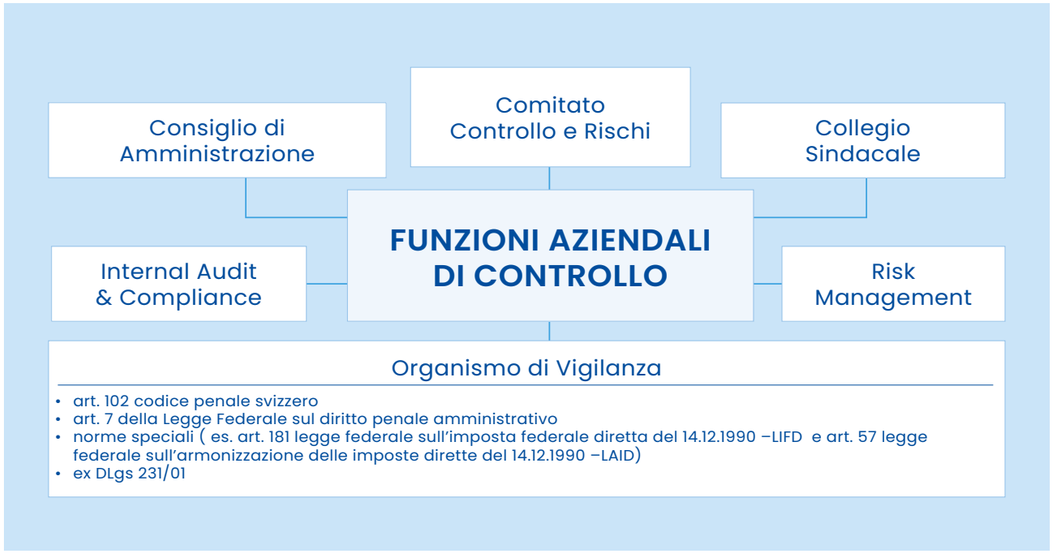
L'analisi delle controparti per la tutela della reputazione e del valore aziendale

Valutare adeguatamente le proprie controparti (interne ed esterne) e rilevare tempestivamente eventuali minacce ed elementi di rischio è sempre più un requisito essenziale per la tutela delle imprese e delle organizzazioni al fine di non compromettere la fiducia di clienti, finanziatori ed investitori a causa di accadimenti negativi a loro carico.



Funzioni tenute ai controlli

La piena consapevolezza e una concreta attenzione alla gestione dei rischi di reputazione e conformità rappresentano una priorità per gli organi di governo e le funzioni/strutture interessate alle tematiche di controllo.



Numero Aziendale
+41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

Obiettivi

Le funzioni aziendali interessate ad un'adeguata gestione del "rischio controparti" sono molteplici. In un contesto dinamico, caratterizzato da elevate interazioni con soggetti differenti, sono molti i processi aziendali che richiedono un'accurata gestione del rischio derivante da controparti, con profili di rischio differenti in relazione al settore di operatività, alle caratteristiche e al funzionamento dell'organizzazione.

ACQUISTI / APPROVVIGIONAMENTI

Qualifica e classificazione di fornitori e appaltatori (inclusi soci, amministratori, manager, consulenti, ecc.).

FINANZA

- Monitoraggio dei flussi finanziari.
- Verifica della clientela ai fini antiriciclaggio.

OUTSOURCING

Qualifica e valutazione delle controparti (outsourcer) in ambito ICT, legal, payroll, ecc.

FRANCHISING

Qualifica e valutazione delle controparti da parte di agenti della rete di vendita, gestori di punti vendita, ecc.

VENDITE

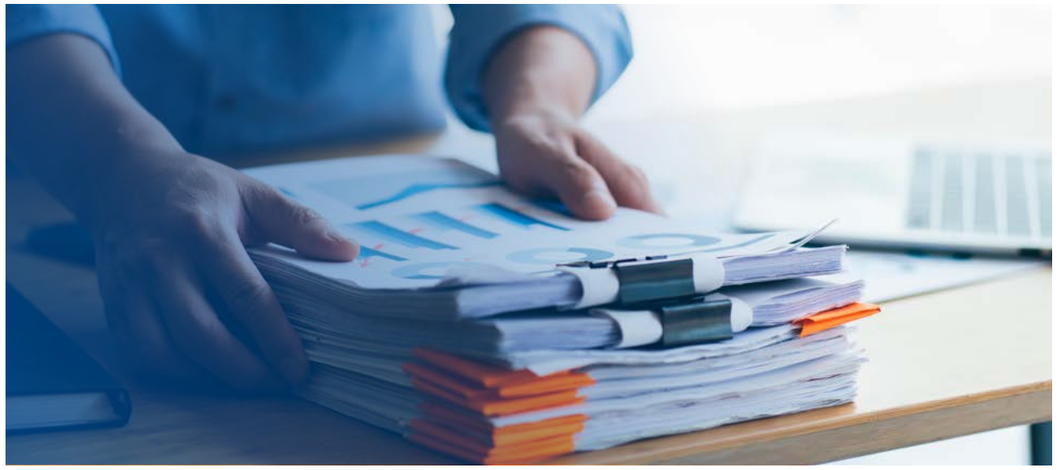
- Qualifica e classificazione di promotori, clienti, agenti, distributori, business partners, ecc.
- Monitoraggio periodico dell'affidabilità di controparti strategiche.

RISORSE UMANE

Selezione ed assunzione di personale e collaboratori.

PARTNERSHIP

Qualifica e valutazione delle controparti da parte di partners in joint ventures, associati in partecipazione, ecc.



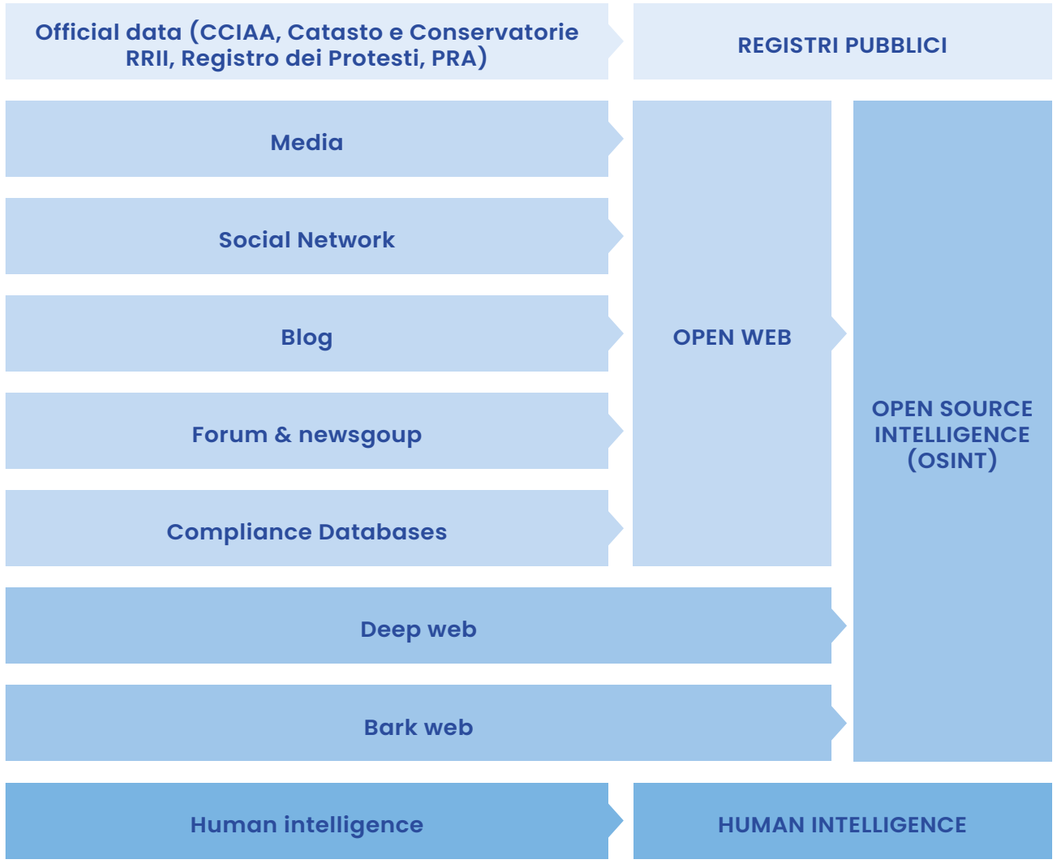
Numero Aziendale
+41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

Processi

RICEZIONE	• Raccolta delle esigenze del cliente • Identificazione delle necessità informative • Definizione degli obiettivi d'indagine • Definizione del Piano operativo e del perimetro d'analisi
PREPARAZIONE	• Raccolta di eventuale documentazione integrativa fornita dal Cliente. • Raccolta dati ufficiali di base: Visure camerali, Visure catastali, Protesti, Fallimenti e procedure concorsuali, Pregiudizievoli da conservatoria, Bilanci, Cointeressenze, Ritagli stampa presenti su repository ufficiali
ELABORAZIONE	• Liste Antiriciclaggio: PEP, PEP-L, SOE, Global Sanctions Lists, Black List/Watch List, AML, CFT, Global regulatory and law enforcement lists, ecc. • Identificazione Beneficial Owners • Analisi OSINT strutturata nel surface/open web (Social Network, Blog, News, Forum, ecc), deep web e dark web e ricerca di adverse media e bad news. • Profilazione della società target, soci, esponenti significativi • Verifica eventuali Albi e referenze (es: White List, rating di legalità, ecc.) • Identificazione e descrizione di criticità etico-reputazionali associate • Identificazione e descrizione di eventuali difformità, anomalie, lacune rispetto ai dati ufficiali e/o alla documentazione fornita dal Cliente • analisi predittiva del comportamento finanziario dell'azienda finalizzata a stabilire il grado di similarità dei bilanci rispetto a quelle di aziende criminali ovvero fallite • Analisi del rischio ESG (Environmental, Social, Governance) • Attività di HUMAN INTELLIGENCE (HUMINT): Raccolta di informazioni in loco da fonti investigative riservate e confidenziali
REDAZIONE	• Inserimento delle evidenze raccolte in un formato sintetico, riassuntivo ed intellegibile.

Numero Aziendale +41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

Fonti



Numero Aziendale +41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

Ricerche e analisi

DOSSIER COMPANY REPUTATION (DUE DILIGENCE INVESTIGATIVA)

La Due Diligence investigativa su **persone giuridiche** viene effettuata attraverso l'interrogazione di compliance data-bases e media search associando specifiche adverse keywords. Il livello di analisi include un controllo completo di banche dati utili ad identificare le seguenti informazioni:

GIURIDICHE: dati aziendali, compagine societaria e eventuali partecipazioni od interessenze aziendali, tramite l'uso di Business Databases.

DI COMPLIANCE: identificazione di sanzioni, embargo, watch-lists e banche dati relative a persone esposte mediante l'utilizzo di Compliance Databases e banche dati pubbliche e private.

REPUTAZIONALI: presenza di potenziali "red Flag" su media e news, identificati grazie a ricerche multimediali con l'utilizzo di "adverse key words", attraverso la disamina elettronica di riviste, siti web, pubblicazioni di settore, testate giornalistiche e media locali e internazionali, motori di ricerca. La raccolta delle informazioni di natura reputazionale avverrà tramite metodologia Osint (Open Source Intelligence) con il fine di identificare potenziali criticità nel profilo della controparte rinvenienti da media internazionali e locali o da un profilo "rischioso" del soggetto investigato.

FINANCIAL BEHAVIOUR DATA INTELLIGENCE: analisi predittiva del comportamento finanziario dell'azienda finalizzata a stabilire il grado di similarità dei bilanci rispetto a quelle di aziende criminali ovvero fallite (sono presi in considerazione gli ultimi dieci anni di bilanci depositati). Viene inoltre analizzata, ricostruita e classificata la rete partecipativa di società e persone alla ricerca di potenziali filiere di rischio e possibili casi di interlocking, prestanome, cartelli. L'intelligenza Artificiale consente di individuare e classificare le anomalie contabili predittive di frodi, riciclaggio, falsa fatturazione, bancarotta fraudolenta, altri reati.

INFORMAZIONI SU RISCHIO PAESE con particolare riferimento a tematiche di Bribery&Corruption relativamente allo stato dove opera la società oggetto di analisi.

ESAME DI FONTI LOCALI UTILI AD IDENTIFICARE:

- News di interesse.
- Sentenze/pendenze giudiziarie avverse in tribunali locali come condanne per corruzione, riciclaggio, insider trading (tramite l'utilizzo di Litigation Databases).
- Eventuale identificazione di potenziali interrelazioni con società e/o soggetti a rischio.
- Potenziali fatti censurabili a carico del target.

APPROFONDIMENTI SU DATI ECONOMICO-FINANZIARI della controparte (struttura societarie e stato patrimoniale, identificazione degli share-holders compresa la loro nazionalità e identificazione dell'ultimate beneficial owner, verifica della consistenza economico-finanziaria, i.e. bilanci se disponibili, capitale sociale versato) e analisi specifiche ad hoc in caso di potenziali "red-flag" identificati ai punti precedenti, al fine di raccogliere tutte le informazioni utili a supportare le valutazioni e ad escludere "falsi positivi".

Numero Aziendale +41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch
Inside INTELLIGENCE | SECURITY | INVESTIGATIONS

DOSSIER COMPANY REPUTATION SVIZZERA

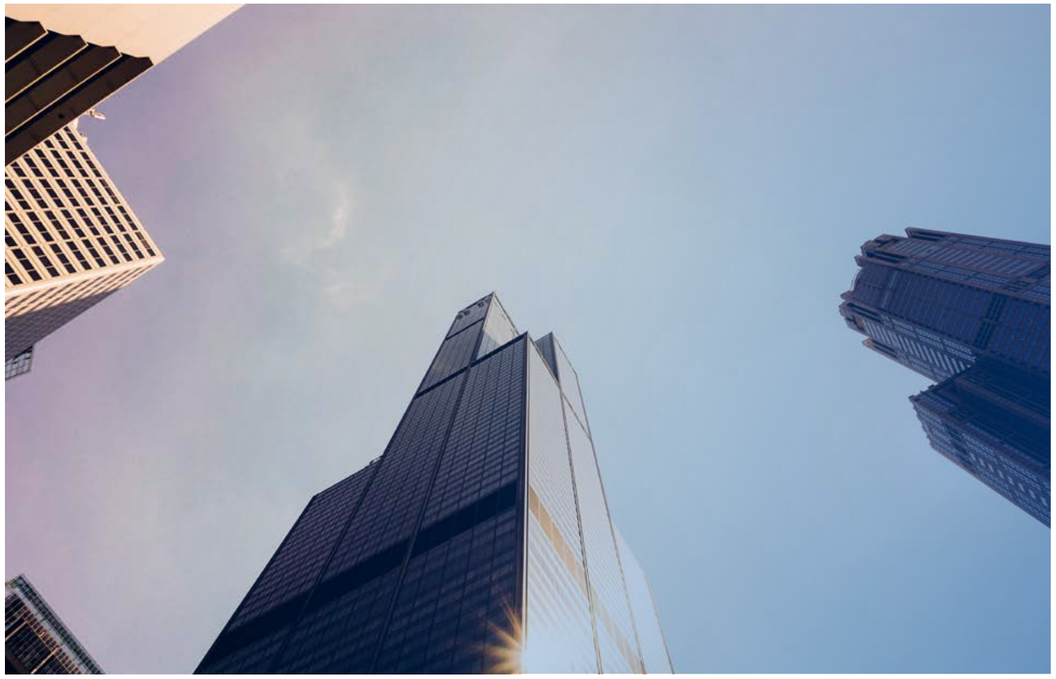
		DOSSIER COMPANY REPUTATION BASE	DOSSIER COMPANY REPUTATION INTERMEDIO	DOSSIER COMPANY REPUTATION APPROFONDITO
1° LIVELLO	**Informazioni da registri pubblici:** • Anagrafica completa • Attività prevalenti • Dipendenti • Sedi secondarie (uffici/unità locali attive) • Eventuale gruppo di appartenenza • Soci/Esponenti (amministratori, procuratori, institori, responsabili tecnici, collegio sindacale ecc.) • Cariche (attive o cessate) degli esponenti in altre aziende • Dati di Bilancio • Eventi negativi • Trasferimenti/cessioni – incorporazioni – fusioni ecc. • Notizie storiche **Informazioni da fonti aperte su:** • Società Target • Eventuale gruppo di appartenenza • Soci/Esponenti (ove disponibili) **Evidenze da DATABASE Internazionali sul conto di:** • Società Target • Eventuale gruppo di appartenenza • Soci/Esponenti (ove disponibili)	✓		
2° LIVELLO	**Informazioni da registri pubblici:** • Financial Beneficial Owner (ove disponibile) • Soci / Esponenti cessati entro i 2 anni antecedenti la data del Report (ove disponibili) **Informazioni da fonti aperte su:** • Financial Beneficial Owner (ove disponibile) • Soci / Esponenti cessati entro i 2 anni antecedenti la data del Report (ove disponibili) **Evidenze da DATABASE internazionali sul conto di:** • Financial Beneficial Owner (ove disponibile) • Soci / Esponenti cessati entro i 2 anni antecedenti la data del Report (ove disponibili) **Verifiche (sulla denominazione/Partita IVA del target) presso l'Ufficio del Catasto**		✓	
3° LIV.	**Attività di HUMINT (HUMan INTelligence)**			✓

Inside INTELLIGENCE | SECURITY | INVESTIGATIONS
Numero Aziendale +41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

DOSSIER PERSONAL REPUTATION SVIZZERA

I report consente la **valutazione reputazionale di potenziali partner commerciali**, candidati manager e figure apicali in fase pre-assuntiva. Si forniranno i seguenti dati:

- Verifica dati anagrafici ed indirizzo
- Cariche in società svizzere
- Partecipazioni in società svizzere (escluse SA)
- Controllo Ufficio Esecuzione e Fallimenti (se in possesso di un giustificativo)
- Esperienze pagamenti
- Pubblicazioni ufficiali
- Informazioni reperite attraverso metodologia OSINT (Open Source Intelligence), con relativa indicazione circa la presenza di eventi negativi, di natura legale e giudiziaria, che abbiano coinvolto il soggetto di interesse.



Numero Aziendale +41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

Inside INTELLIGENCE | SECURITY | INVESTIGATIONS

DOSSIER COMPANY REPUTATION ITALIA

I nostri report sono gli strumenti più adatti per la valutazione del rischio "commerciale e reputazionale" dei partner, tanto nelle operazioni societarie ordinarie (nel caso di clienti o fornitori) quanto nelle straordinarie (fusioni e incorporazioni d'azienda).

		DOSSIER COMPANY REPUTATION BASE	DOSSIER COMPANY REPUTATION INTERMEDIO	DOSSIER COMPANY REPUTATION APPROFONDITO
1° LIVELLO	**Informazioni da registri pubblici:** • Anagrafica completa • Attività prevalenti • Dipendenti • Sedi secondarie (uffici/unità locali attive) • Eventuale gruppo di appartenenza • Soci/Esponenti (amministratori, procuratori, institori, responsabili tecnici, collegio sindacale ecc.) • Cariche (attive o cessate) degli esponenti in altre aziende • Dati di Bilancio • Negatività (pregiudizievoli di conservatoria, protesti, fallimenti ecc.) • Trasferimenti/cessioni di rami d'azienda – incorporazioni – fusioni ecc. • Notizie storiche	✓	✓	✓
	Informazioni da fonti aperte su: • Società Target • Eventuale gruppo di appartenenza • Soci/Esponenti • Verifica iscrizione in White Lists prefettizie (solo per società attive in comparti previsti dal codice antimafia)	✓	✓	✓
	Evidenze da DATABASE Internazionali sul conto di: • Società Target • Eventuale gruppo di appartenenza • Soci/Esponenti (ove disponibili)	✓	✓	✓
	Focus ECG	✓	✓	✓
2° LIVELLO	**Informazioni da registri pubblici:** • Financial Beneficial Owner • Soci / Esponenti cessati entro i 2 anni antecedenti la data del Report		✓	✓
	Informazioni da fonti aperte su: • Financial Beneficial Owner (ove disponibile) • Soci / Esponenti cessati entro i 2 anni antecedenti la data del Report		✓	✓
	Evidenze da DATABASE internazionali sul conto di: • Financial Beneficial Owner (ove disponibile) • Soci / Esponenti cessati entro i 2 anni antecedenti la data del Report		✓	✓
	Verifiche (sulla denominazione/Partita IVA del target) presso Agenzia del Territorio e Conservatorie dei Registri immobiliari (verifica terreni e fabbricati - ispezioni ipotecarie)		✓	✓
3° LIV.	**Attività di HUMINT (HUMan INTelligence)**			✓

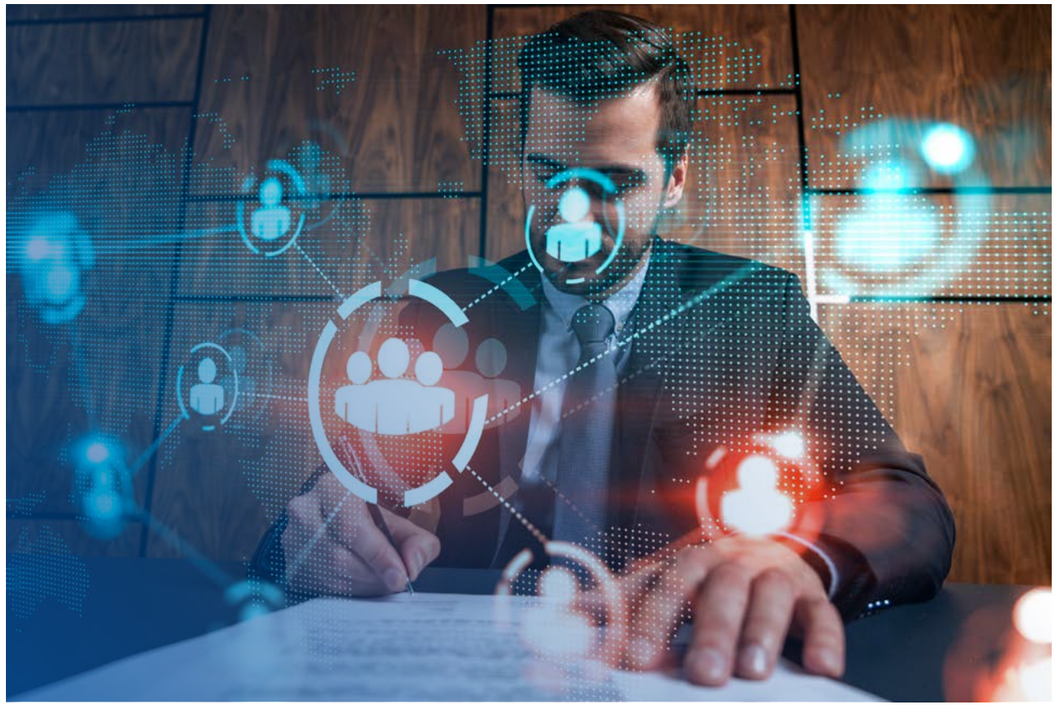
Inside INTELLIGENCE | SECURITY | INVESTIGATIONS

Numero Aziendale +41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

DOSSIER PERSONAL REPUTATION ITALIA

Il report consente la valutazione reputazionale di potenziali partner commerciali, candidati manager e figure apicali in fase pre-assuntiva, dei quali si effettua anche la verifica del background curriculare e della compliance nella condotta professionale.

1° LIVELLO	Ricerca dati ufficiali su Camere di commercio (anagrafica - partecipazioni in società – cariche ricoperte attuali e/o cessate – negatività)	DOSSIER PERSONAL REPUTATION BASE
	Ricerca informazioni su Fonti aperte	
	Verifiche presso Agenzia del Territorio e Conservatorie dei Registri immobiliari (verifica terreni e fabbricati - ispezioni ipotecarie)	
	Ricerca su DATABASE Internazionali	
2° LIVELLO	Attività di HUMINT (HUMan INTelligence)	DOSSIER COMPANY REPUTATION AVANZATO



DOSSIER COMPANY REPUTATION ESTERO

L'attività di intelligence di INSIDE è in grado di rilevare i **rischi insiti nelle relazioni imprenditoriali e interpersonali a livello globale**, rischi riguardanti la vita d'affari e che i trascorsi fatti di cronaca, cui i soggetti sono legati, possono comportare per chi apre relazioni con sconosciuti; i dati così raccolti sono utilizzati per comporre profili altamente strutturati.

1° LIVELLO	**Informazioni da registri pubblici:** • Anagrafica completa • Attività prevalenti • Dipendenti • Sedi secondarie (uffici/unità locali attive) • Eventuale gruppo di appartenenza • Soci/Esponenti • Cariche (attive o cessate) degli esponenti in altre aziende • Dati di Bilancio, ove disponibile • Eventi negativi • Trasferimenti/cessioni – incorporazioni – fusioni ecc. • Notizie storiche	DOSSIER COMPANY REPUTATION BASE
	Informazioni da fonti aperte su: • Società Target • Eventuale gruppo di appartenenza • Soci/Esponenti	
	Evidenze da DATABASE Internazionali sul conto di: • Società Target • Eventuale gruppo di appartenenza • Soci/Esponenti	
	Litigation, Bankruptcy, Regulatory and Law Enforcement Checks (da fonti accessibili e solo sulla denominazione/Partita IVA del target)	
	Focus ESG	
2° LIVELLO	**Attività di HUMINT (HUMan INTelligence)**	DOSSIER COMPANY REPUTATION AVANZATO

I NOSTRI SERVIZI

Investigazioni private

Tradimento e infedeltà coniugale

L'investigazione consente di **individuare** ed accertare, attraverso foto, video e relazioni dettagliate, **qualsiasi comportamento inaccettabile** nei confronti del proprio coniuge, che renda intollerabile la prosecuzione del matrimonio.

Se hai dubbi sulla fedeltà del tuo coniuge rivolgiti a **professionisti del settore**, che con discrezione e professionalità ti aiuteranno a trovare la soluzione migliore per risolvere i tuoi problemi e per **tutelare i tuoi diritti** nel caso di comportamento fedifrago da parte del partner.

Questo tipo di indagine è utile al coniuge che vuole **dimostrare l'infedeltà del proprio partner**. A conclusione dell'attività investigativa verrà rilasciata una **relazione dettagliata valida in tribunale** e l'identificazione della persona coinvolta nell'infedeltà.

Revisione assegno divorzile e di mantenimento

L'investigazione consente di poter richiedere una **revisione dell'assegno di mantenimento**, in relazione ad una mutata situazione economica e/o alle esigenze dei figli.

Se il tuo ex coniuge percepisce un reddito diverso da quello dichiarato, anche in nero, puoi affidarti a professionisti del settore per richiedere una revisione dell'assegno. Ti forniremo le prove necessarie per **far valere i tuoi diritti in sede giudiziaria**.

Questa attività investigativa risulta utile a chi vorrebbe una revisione del proprio assegno di mantenimento grazie ad una **mutata situazione economica dell'ex partner** (che ha trovato lavoro, anche in nero) oppure per mutate esigenze dei figli.

Affidamento esclusivo minori

L'investigazione ha la finalità di far **ottenere in tribunale**, al genitore che si rivolgerà ad INSIDE, **l'affidamento dei figli**. L'indagine consentirà di **scoprire** eventuali **comportamenti poco consoni**, cattive frequentazioni e/o la non idoneità dei luoghi in cui far crescere i figli.

Controllo giovani e minori

L'investigazione consente a genitori e tutori di minori, di **conoscere abitudini e frequentazioni dei figli**. Se sei preoccupato per lo strano comportamento di tuo figlio, se pensi che possa far uso di droga e/o alcool, o che possa essere incappato in "cattive compagnie", non esitare e contattaci subito per conoscere la verità ed intervenire nel modo più corretto.

Questa attività investigativa risulta utile ai genitori, o ai tutori di minori, preoccupati per il mutato atteggiamento del figlio. L'indagine è volta a scoprire frequentazioni e abitudini del giovane, con lo scopo di **salvaguardare la sua incolumità nel modo più corretto ed efficace**.

I NOSTRI SERVIZI

Indagini antifrode

INSIDE grazie all'ausilio dei suoi professionisti affianca le società di assicurazione, salvaguardandone gli interessi patrimoniali, al fine di ricercare e raccogliere ogni elemento utile ad accreditare l'ipotesi di reato ed acquisire le prove necessarie per un eventuale procedimento giudiziale, civile e penale, così da ottenere il giusto e dovuto risarcimento per i danni subiti.

In particolare, al fine di **documentare la veridicità del sinistro** per il quale viene richiesta la liquidazione del risarcimento dei danni, le compagnie assicurative affidano a INSIDE l'incarico di effettuare **indagini** in merito, fornendo le linee guida più consone alle proprie esigenze.

Il **primo step** consiste **nell'audizione di tutte le parti coinvolte** (assicurato, controparte, eventuali testimoni), al fine di ottenere loro "dichiarazioni spontanee" possibilmente autografe e sottoscritte.

Importantissime per ricostruire l'intera vicenda sono le **documentazioni fotografiche** nonché ogni altro elemento utile a ricostruire l'intera dinamica del sinistro (verbali delle FF.OO, referti medici, ecc.), il tutto da svolgersi in collaborazione con i singoli professionisti coinvolti nella vicenda quali periti, geometri, studi legali, agenzie infortunistiche.

Al termine delle indagini, gli investigatori redigono una **relazione tecnica**: si tratta di un documento all'interno del quale vengono descritti il lavoro svolto ed i risultati con esso ottenuti. La relazione può essere impiegata dal mandante delle indagini con valore probatorio (per ottemperare all'onere della prova) nell'ambito di un eventuale processo giudiziario.

Indagini antifrode assicurativa per danni materiali

Grazie alla propria rete internazionale di collaboratori, INSIDE è in grado di **supportare le compagnie assicurative nella gestione dei sinistri e dei furti** riguardanti l'oggetto delle polizze (vetture, ma anche oggetti di valore, dispositivi e sistemi informatici). Gli accertamenti, le analisi e la raccolta di informazioni, spendibili nell'ambito della trattazione delle pratiche di indennizzo e/o di risarcimento, vengono svolti nel pieno rispetto delle normative vigenti in materia di tutela della privacy (Legislazioni Nazionali e Regolamento U.E. n°679/2016), **fornendo** contestualmente u**n contesto probatorio certo** che consente al Cliente di gestire consapevolmente i rischi e mitigarne l'impatto.

Indagini antifrode assicurativa per danni fisici

Le unità operative di INSIDE garantiscono interventi tempestivi ed efficaci nelle attività di osservazione, statica e/o dinamica, di persone laddove vi sia il sospetto che le patologie per le quali è stata richiesta l'attivazione delle coperture assicurative non siano fondate. I servizi di osservazione sono effettuati rispettando le prescrizioni di legge in materia ed in conformità con le Legislazioni Nazionali ed il Regolamento U.E. n°679/2016 in materia di tutela della privacy.

Siamo esperti nell'individuazione delle **frodi assicurative (LFA) (LCA), Cassa Malati (LAMal)** e dei **furti**. Grazie alle nostre competenze e al nostro **metodo innovativo Data Cross Investigation**, è possibile identificare le minacce più rapidamente, velocizzando i tempi di indagine, riducendo i vostri oneri e migliorando l'efficienza della gestione dei sinistri. **Questo per le Assicurazioni significa che:**

- Contrastiamo le frodi e tuteliamo gli interessi patrimoniali della società di assicurazione
- Disponiamo di un team investigativo specializzato: Divisione Insurance Anti Fraud Intelligence
- I nostri investigatori sono ex Agenti Ispettori di Polizia
- Ottimizziamo e velocizziamo i tempi d'indagine
- Produciamo prove certe da produrre in sede giudiziaria
- Forniamo supporto telefonico immediato nell'ambito di tutte le attività d'indagine

I NOSTRI SERVIZI

Bonifiche Elettroniche

Bonifica ambientale microspie

L'OBIETTIVO: GARANTIRE LA SICUREZZA DELLE TUE INFORMAZIONI

Non è raro per chi si trova ai vertici di importanti organizzazioni subire furti di strategie di business, informazioni aziendali di fondamentale importanza, nonché nominativi di fornitori o clienti. Tali furti possono risultare quasi inspiegabili agli occhi di chi li subisce. Spesso la soluzione si trova sotto gli occhi di tutti ma allo stesso tempo risulta invisibile: minuscoli apparecchi occultabili ovunque, **rilevabili** solamente dalle migliori strumentazioni. **Microspie**, altrimenti conosciute come **cimici**.

Ma come individuare e rimuovere questi insidiosi dispositivi?

INSIDE, agenzia investigativa operante nel settore security a 360°, ha pensato anche a questo organizzando la Divisione Bonifiche Elettroniche. I tecnici di questa peculiare divisione garantiscono la totale **bonifica ambientale da microspie**, a livello aziendale e privato, mediante l'utilizzo di strumenti di rilevazione altamente professionali.

La divisione Bonifiche elettroniche è in grado di rilevare:

- **spy software**, per sorvegliare le attività svolte su pc;
- **spy phone software**, per sorvegliare le attività svolte su telefoni cellulari;
- **microspie audio/video**, facilmente occultabili ovunque;
- **microfono laser**, che consente l'ascolto a distanza, rilevando le vibrazioni sonore attraverso i vetri;
- **microregistratore audio digitale**, occultabile ovunque, anche all'interno di un veicolo;
- **rilevatore GPS**, installato all'interno o all'esterno di un veicolo, in grado di fornire la posizione istantanea dello stesso e di tracciare il percorso seguito con relative soste;
- **rilevatore GPS e microspia audio**, per la localizzazione satellitare e la trasmissione delle conversazioni avvenute all'interno dell'abitacolo;
- **intercettazioni telefoniche**;
- **registratori audio/video**, occultabili sul nostro interlocutore.

CHE COS'È PRECISAMENTE UNA MICROSPIA?

Una microspia è un dispositivo elettronico di piccolissime dimensioni capace di catturare audio, video ed immagini e, in alcuni casi, ritrasmetterli ad un apposito ricevitore tramite onde radio. Può essere dotata di un microfono, di una videocamera e perfino di un rilevatore GPS ed attivata tramite controllo remoto o VOX.

Ecco i dettagli di questi peculiari sistemi:

- **controllo remoto:** le microspie che presentano questa funzionalità vengono attivate e disattivate mediante un apparecchio di comando a distanza;
- **VOX:** questo sistema consente l'attivazione della microspia solo in presenza di voci, suoni e rumori.

Esistono molteplici tipologie di microspia e, grazie alle più moderne tecnologie, le loro funzionalità sono in continua evoluzione.

TIPOLOGIE DI MICROSPIA

Durante la bonifica ambientale i tecnici della nostra agenzia investigativa sono in grado di rilevare microspie di qualsiasi tipo. Nel mercato delle apparecchiature di spionaggio esistono numerosissime tipologie di microspia, ma possiamo raggrupparle in 4 macro-aree.

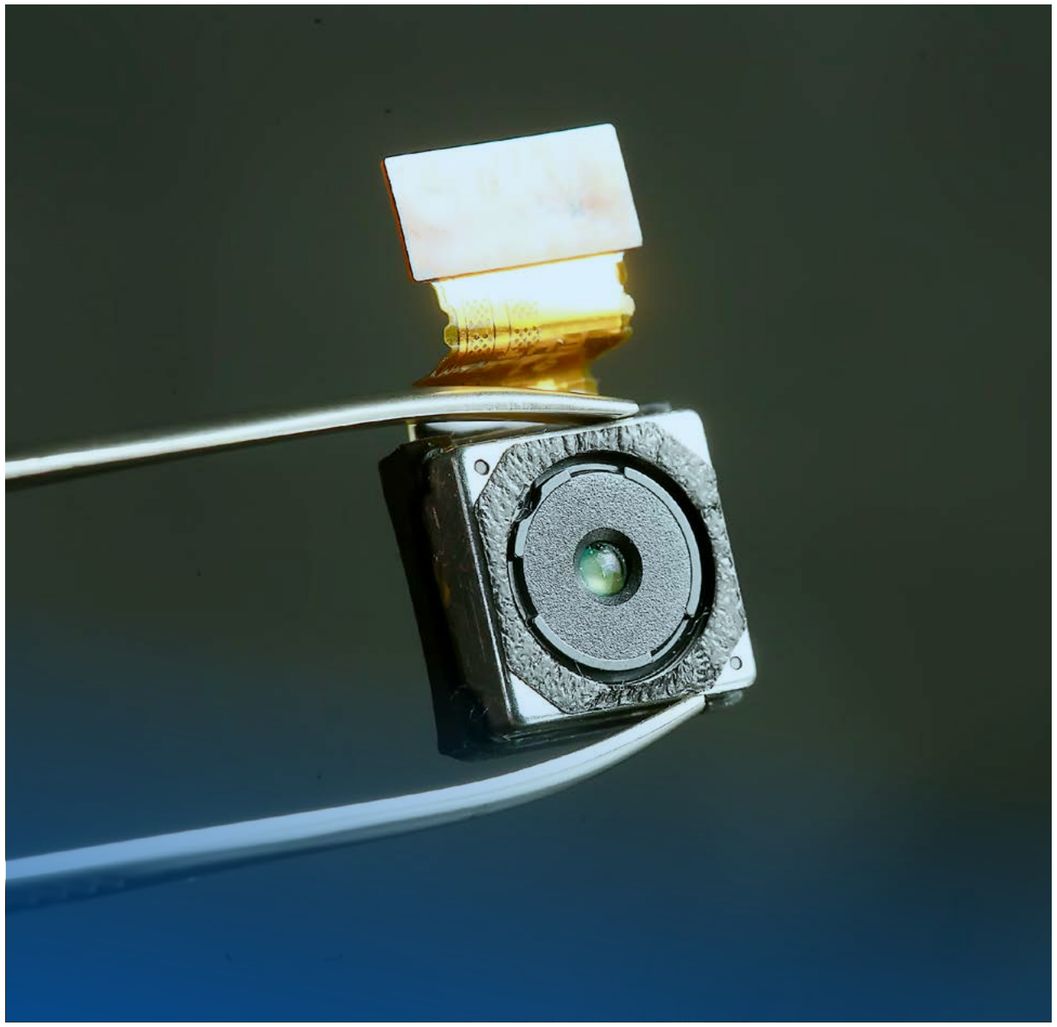
Ecco di seguito quali:

- **microregistratori audio:** presentano microfoni molto sensibili a suoni e rumori ed una batteria dall'autonomia molto elevata, capace di mantenere un microregistratore attivo anche per diverse settimane;
- **microspie ambientali audio/video:** in questo caso la trasmissione è in diretta grazie alle onde radio o alla rete GSM/UMTS. Nel primo caso è previsto l'utilizzo di un ricevitore e la trasmissione dipende dall'antenna, dunque è limitata. Per quanto riguarda il secondo caso invece la trasmissione si appoggia alla rete della telefonia mobile (viene installata una SIM card all'interno della microspia) ed è illimitata;
- **microregistratori audio-video:** in questo caso la microspia presenta sia il microfono che la telecamera, e registra sia voci, suoni e rumori che immagini;
- **microspie GPS/rilevatori GPS:** queste microspie sono in grado di fornire la localizzazione e seguire gli spostamenti. Possono anche presentare un microfono per la trasmissione audio.

DOVE CERCARE LE MICROSPIE?

Una microspia, grazie alle sue dimensioni estremamente ridotte, può essere installata e nascosta ovunque. Le microspie ambientali ed i microregistratori sono facilmente applicabili su vestiti, controsoffitti, scatole di derivazione. Anche le prese di corrente e le chiavette USB possono rappresentare un ottimo nascondiglio per questi microscopici dispositivi.

I rilevatori GPS vengono comunemente installati nelle automobili, permettendo all'autore dello **spionaggio** di essere informato sulla posizione e sugli spostamenti del mezzo. Individuare l'ubicazione di una microspia all'interno di un'azienda, un'abitazione o un'automobile è impossibile ad occhio nudo per i non esperti. Proprio per questo quando si sospetta la presenza di microspie all'interno di uno o più ambienti è necessario l'intervento dei tecnici INSIDE, esperti conoscitori di microspie e del funzionamento degli strumenti del settore investigazioni.



LA PROCEDURA

Le operazioni di bonifica ambientale da microspie vengono svolte in due tempi. Prima di tutto viene ispezionato l'ambiente esterno tramite controllo visivo del perimetro ed una scansione della radiofrequenza. In secondo luogo vengono condotte peculiari **investigazioni** all'interno dell'edificio o dell'automobile, che comprendono:

- l'installazione di contromisure volte ad ostacolare il funzionamento delle microspie;
- l'utilizzo della termo-camera per esaminare approfonditamente gli ambienti ed individuare l'ubicazione dei dispositivi di spionaggio;
- l'analisi delle frequenze da 10 kHz a 6 GHz;
- l'utilizzo di dispositivi ad infrarossi per l'individuazione di microcamere;
- il controllo di ogni oggetto risultante manomesso o sospetto.

In seguito all'individuazione delle microspie queste vengono rimosse e, se richiesto dal cliente, vengono applicati sigilli di sicurezza ambientali.

Al termine della bonifica ambientale da microspie INSIDE fornisce ai clienti **report dettagliati** e meticolosi riguardanti tutte le operazioni svolte dai tecnici della Divisione Bonifiche Elettroniche.

LA STRUMENTAZIONE DEI TECNICI INSIDE

La strumentazione dei tecnici INSIDE è rappresentata da dispositivi di rilevazione digitali ed analogici, estremamente sensibili alla presenza di microspie. Ecco di seguito quali sono:

ANALIZZATORE DI SPETTRO

Questo apparato permette di verificare tutte le frequenze comprese tra i 100 KHz ed i 12,4 Ghz presenti in un determinato ambiente e quindi individuare la presenza di qualsiasi tipologia di trasmettitore (Digitale, Analogico, AM, FM, Carrier, Sub-carrier, SBB, Scrambled, Frequency Hopping, Spread Spectrum, Bluetooth, Wi-Fi, GSM, UMTS, LTE e 5G).
Con questo dispositivo è possibile anche registrare l'analisi effettuata e demodulare, ovvero ascoltare ciò che la microspia percepisce, sempre che questa sia analogica.

APPARATO MULTIFUNZIONE

Questo dispositivo è il più recente apparato multifunzione a livello mondiale per la rilevazione di emissioni RF come Wi-Fi (2.4 e 5 GHz), Bluetooth, telefoni e moduli cellulari (2G, 3G, 4G e 5G). Il suo kit comprende varie antenne e sonde per la rilevazione di molteplici dispositivi illeciti.
Oltre a qualsiasi tipologia di radio-trasmissione (compresa tra i 10 kHz e i 12 GHz) è possibile analizzare:

- Linee Telefoniche;
- Linee Elettriche (Trasmettitori a Onde Convogliate);
- Trasmettitori IR;
- Trasmettitori Ultrasonici;
- Trasmettitori a perdita acustica tra i 300 Hz ed i 20 KHz.

1. Analisi delle Linee Telefoniche
2. Analisi delle Linee Elettriche
3. Ricerca Trasmettitori IR
4. Ricerca Trasmettitori Ultrasonici

INIBITORE DELLE RADIOFREQUENZE DI RETE

Questa tipologia di apparato permette di inibire momentaneamente tutte le frequenze GSM, DCS, UMTS (3G) e LTE (4G) utilizzate dalle microspie e dai trasmettitori A/V.
Una volta disattivato l'inibitore viene identificato l'aggancio alla BTS con l'apparato " Rilevatore di Aggancio BTS" indicato di seguito.
N.B. è indispensabile utilizzare un inibitore di grosse dimensioni e notevole potenza (minimo 100 W) per avere la certezza di riuscire ad inibire tutti i segnali.

RILEVATORE DI AGGANCIO BTS

Con questo dispositivo è possibile rilevare il PING di aggancio ponte BTS quindi individuare la presenza di microspie, microcamere o trasmettitori GSM, DCS, 3G e 4 G non solo in trasmissione ma anche in st-by. Questo apparato è dotato di 1 modulo wideband da 0 a 14 GHz, 5 moduli GSM-DCS-UMTS-LTE, 2 moduli Wi-Fi e Bluetooth 2.4 GHz e 5 GHz.
Questa apparecchiatura multi banda consente un rapido controllo su tutti quei dispositivi che trasmettono in radiofrequenza.
Essendo uno strumento portatile permette di identificare, approssimarsi e quindi trovare la fonte di una determinata radio trasmissione (microspia, micro-camera via radio, trasmettitore A/V).

Numero Aziendale +41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

RILEVATORE DI AGGANCIO BTS 5G

Con questa apparecchiatura è possibile rilevare il ping di aggancio ponte BTS quindi individuare la presenza di tutti i dispositivi (Micro Audio, Micro Video, Trasmettitori A/V e Localizzatori GPS) di ultimissima generazione che utilizzano la tecnologia 5G con copertura multibanda mondiale.
Grazie a questa strumentazione possiamo rilevare questi dispositivi sia attivi che NON in trasmissione. Oltre al GSM, 3G, 4G e 5G è possibile rilevare tutti i dispositivi che utilizzano trasmissioni in Wi-Fi e Bluetooth a 2,4 e 5 GHz.

RILEVATORE DI GIUNZIONI NON LINEARI

Con questo dispositivo è possibile individuare tutte le apparecchiature elettroniche che non trasmettono in radio-frequenza (microregistratori, microspie, trasmettitori A/V e microcamere anche spente e non alimentate) ovvero spente, in stand-by o non alimentate.
Questo apparato è uno dei rilevatori di giunzioni non lineari più innovativi sul mercato ed è in grado anche di rilevare una microspia (anche spenta) affogata nel cemento.

TERMOCAMERA

Questa termocamera Flir permette di individuare un minima differenza di temperatura quindi trovare tutte quelle apparecchiature elettroniche che emanano calore.
Flir è una termocamera estremamente evoluta è in grado di indentificare un apparato che irradia calore con un differenziale termico di appena 0,06 °C.

RILEVATORE OTTICO DI MICROCAMERE

Questa apparecchiatura è progettata per rilevare e localizzare micro-camere, anche di piccolissime dimensioni, come "pinhole", a prescindere dal loro stato (on / off) e dal tipo di segnale video.
Il metodo di rilevazione si basa sull'acquisizione ottica e permette di rilevare micro-camere per effetto della riflessione inversa.

Inside INTELLIGENCE | SECURITY | INVESTIGATIONS

Numero Aziendale +41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

ANALIZZATORE DI APPARATI Wi-Fi

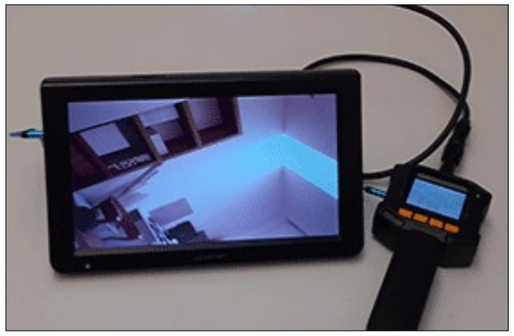
Vi sono dei trasmettitori audio e audio/video che utilizzano la trasmissione Wi-Fi in modo fraudolento per trasferire informazioni, la tecnologia estremamente avanzata permette di nascondere l'SSID.
Con questa apparecchiatura è possibile rilevare tutte le trasmissioni Wi-Fi sia in chiaro che con SSID nascosto (Hidden).

RILEVATORE WIRELESS di MICROCAMERE – WiFi IP

Il Rilevatore Wireless di Microcamere opera a 1.2 GHz – 2.4 GHz – 5.8 GHz (specifici per microcamere attive in trasmissione via radio).
Questa apparecchiatura rileva anche le trasmissioni video delle Telecamere IP operanti sulle bande Wi-Fi.
Questo strumento permette di visualizzare su uno schermo ciò che una potenziale microcamera in radio-trasmissione sta inquadrando.

APPARECCHIATURE PER L'ESAME FISICO

Come da protocollo TSCM gli ambienti delineati dal cliente ed il suo contenuto vengono accuratamente ispezionato visivamente, le prese elettriche vengono smontate e le apparecchiature elettroniche contenute controllate.



MICROSCOPIO DIGITALE ELETTRONICO

Con questo strumento è possibile ingrandire le immagini riprese da 40x a 1000x in modo da poter controllare la non manomissione delle apparecchiature contenute nell'area analizzata.

INSPECTION CAMERA A LED

Telecamera con braccio telescopico e monitor per ispezione.

INSPECTION CAMERA

Telecamera con braccio flessibile e monitor per ispezione. Il Fornitore si riserva di utilizzare gli strumenti che ritiene maggiormente idonei al caso in specie.

Bonifica Telefonica (cellulari e tablet)

Il **servizio di bonifica telefonica antispy** è finalizzato a **verificare la presenza di sistemi d'intercettazione, software spia, trojan, keylogger su cellulari, smartphone, tablet e telefonini**, tramite strumentazione di mobile e malware analysis e a documentare eventuali tracce lasciate dagli autori malintenzionati.

La **bonifica dello smartphone, quindi del cellulare** è una procedura tecnica che spesso viene commissionata dai nostri clienti in presenza di situazioni personali, familiari o professionali che manifestano aspetti di elevata criticità.

L'esame tecnico viene svolto eseguendo dei protocolli specifici, quindi analizzando in primis il software e successivamente l'hardware del dispositivo. Al fine di esaminare tutte le applicazioni, i programmi e la funzionalità elettronica del device, utilizziamo attrezzature e software d'avanguardia.

Il nostro metodo di bonifica è valido su qualsiasi marca e modello di smartphone, cellulare, tablet, qualunque sia il suo sistema operativo. Al termine dell'attività viene rilasciato un **report con valenza legale**.

Bonifica Computer (PC / Mac)

Il **servizio di bonifica di computer, notebook, portatili** è finalizzato a **verificare la presenza di sistemi d'intercettazione e/o spy software,** consentendo di rilevare la presenza di malware con un elevato grado di affidabilità in ragione del tipo di software spia installato e talvolta anche l'identificazione dell'autore dell'intercettazione. Non bastano antivirus, firewall o antispyware per scoprire eventuali keylogger o spyware installati sul proprio PC, anche perché ormai i vari sistemi utilizzabili per mettere sotto controllo un PC sono sempre più disponibili sul mercato, sempre più semplici da utilizzare e con prezzi sempre più economici.

Esistono diversi metodi per identificare **software di spionaggio**: quello basato su firme e quello basato sull'analisi del traffico di rete e del comportamento del sistema, dei processi in esecuzione, della memoria RAM, delle attività sull'hard disk (metodo empirico/euristico).

Gli spy-software spesso lasciano delle tracce che si possono identificare e seguire per reperire informazioni circa la data e l'ora d'installazione, dati relativi alla licenza di acquisto da parte di chi sta spiando il computer, dati di chi ha messo sotto controllo il PC della vittima.

La nostra strumentazione ci permette di **analizzare ogni sezione dei sistemi operativi più diffusi** (iOS, Android, Windows, MacOS, Linux) e viene mantenuta costantemente aggiornata dai nostri tecnici grazie alla collaborazione con le più importanti software house del settore.

L'attività di bonifica informatica può essere svolta in due modalità:

- **Automatizzata**: si avvale della scansione della macchina alla ricerca di applicativi dal comportamento anomalo.
- **Approfondita**: analisi approfondita nei supporti di memoria, nella memoria RAM, all'interno della rete e tra gli applicativi.

Al termine dell'attività viene rilasciato un **report con valenza legale**.

I NOSTRI SERVIZI

Indagini informatiche

Con INSIDE potrai analizzare il tuo livello di sicurezza aziendale, rilevando le vulnerabilità dei sistemi informatici e proteggendoli da eventuali attacchi e minacce esterne.

Digital & Mobile Forensics

Il **Digital e Mobile Forensics (informatica forense)**, particolarmente adoperata nell'ambito dei crimini informatici, è una branca della scienza digitale forense legata alle prove acquisite da computer e altri dispositivi di memorizzazione digitale.

La prova informatica negli ultimi anni ha assunto un ruolo sempre più rilevante non solo nell'ambito delle indagini digitali ma, più in generale, nella quasi totalità delle attività investigative.

Tale attività è collegata all'analisi di dispositivi digitali attraverso **processi di analisi forense utili ad individuare, conservare, recuperare, studiare e presentare fatti o opinioni** sulle informazioni raccolte.

Nell'ambito della Digital & Mobile Forensics è fondamentale non alterare le informazioni e documentare i processi. I passaggi che caratterizzano l'attività di computer forensics possono essere riassunti nell'individuazione, preservazione, acquisizione, analisi e correlazione dei dati assunti, oltre che in una completa ed esaustiva documentazione di quanto effettuato nelle singole fasi. L'**acquisizione della prova informatica** è sicuramente la fase che presenta una maggior criticità, proprio perché deve garantire l'inalterabilità dell'elemento che viene ad essere repertato e la sua fissazione nel tempo.

La fase documentale rappresenta la conclusione di tutto il processo legato all'acquisizione della prova digitale in quanto fissa l'intero operato degli investigatori, dall'individuazione della traccia sino al momento del suo esame e della presentazione delle conclusioni.

Il processo di documentazione risulta fondamentale per garantire una corretta gestione della catena di custodia (chain of custody) dei reperti.

Per **chain of custody** si intendono tutte quelle operazioni, opportunamente documentate e dettagliate in ordine cronologico, che definiscono quando, come, dove e a quale scopo un reperto viene gestito.

INSIDE fornisce servizi di **consulenza forense di media digitali** volti alla cancellazione o al recupero di dati da supporti di memorizzazione danneggiati.

COMPUTER FORENSICS

L'**informatica forense**, particolarmente adoperata nell'ambito dei crimini informatici, è una branca della scienza digitale forense legata alle **prove acquisite da computer** e altri dispositivi di memorizzazione digitale.

Rientrano nelle competenze della computer forensics tutte le attività relative a:

- reati informatici in senso stretto (quale ad esempio il danneggiamento informatico);
- reati commessi per mezzo di dispositivi informatici (ad esempio la diffamazione via Facebook);
- ogni condotta per la quale un dato informatico può essere recuperato da uno o più sistemi informatici.

Tale attività è collegata all'**analisi di dispositivi digitali** attraverso processi di analisi forense utili ad individuare, conservare, recuperare, studiare e presentare fatti o opinioni sulle informazioni raccolte.

MOBILE FORENSICS

Telefoni cellulari, smartphone, tablet, dispositivi portatili sono sempre più utilizzati e contengono tantissime **informazioni personali**, come password, sms, conversazioni, e-mail e molto altro.

Con l'avanzare della tecnologia dei dispositivi mobili , la quantità e i tipi di dati che possono essere trovati su un dispositivo mobile sono in costante aumento. Le prove che possono essere potenzialmente recuperate da un telefono cellulare possono provenire da diverse fonti, tra cui la memoria del telefono, la scheda SIM e le schede di memoria collegate come le schede SD .

Grazie alle proprie competenze nel campo della Sicurezza IT e disponendo delle tecnologie più all'avanguardia presenti sul mercato, il team INSIDE **analizza le informazioni contenute all'interno dei dispositivi mobili** al fine di identificare, preservare, esaminare e documentare un'informazione digitale che potrebbe essere di fondamentale importanza.

NETWORK FORENSICS

La **Network Forensics** consiste nella cattura, registrazione ed analisi di comunicazioni di rete al fine di ottenere informazioni utili allo svolgimento di i**ndagini tecniche** in vari ambiti legali.

DATABASE FORENSICS

Il servizio di **Database Forensics** analizza i database ricercando eventuali dati e tabelle cancellati e/o manomessi, ricostruendo gli eventi che hanno causato un eventuale danno nonché identificando l'attività criminosa e le cause che hanno dato origine all'**incidente informatico**.

Vulnerability assessment and mitigation

A queste prime fasi d'intervento segue l'adozione di **contromisure** finalizzate al miglioramento della sicurezza dei vostri sistemi.

L'adozione del **VAM** deve essere organizzata periodicamente durante l'anno, in quanto la tecnologia è in continuo progresso e con essa anche gli strumenti per attaccare un sistema.

Il processo di **Vulnerability Assessment and Mitigation** si compone delle seguenti fasi:

- analisi della rete aziendale; rilevazione,
- ricognizione e classificazione di ogni apparato ad esso connesso;
- individuazione di potenziali vulnerabilità conosciute (es. certificati scaduti, software non aggiornato, ecc.);
- verifica delle criticità riscontrate;
- valutazione degli interventi necessari da espletare;
- verifica dell'efficacia delle azioni correttive eseguite.

La Divisione Cyber-Security di INSIDE sviluppa i seguenti livelli di VAM:

Bonifica Telefonica (cellulari e tablet): il servizio di bonifica telefonica antispy è finalizzato a verificare la presenza di sistemi d'intercettazione, software spia, trojan, keylogger su cellulari, smartphone, tablet e telefonini, tramite strumentazione di mobile e malware analysis e a documentare eventuali tracce lasciate dagli autori malintenzionati.

- **Bonifica Computer (PC / Mac)**: il servizio di bonifica di computer, notebook, portatili è finalizzato a verificare la presenza di sistemi d'intercettazione e/o spy software, consentendo di rilevare la presenza di malware con un elevato grado di affidabilità in ragione del tipo di software spia installato e talvolta anche l'identificazione dell'autore dell'intercettazione.
- **Vulnerability Scan**: l'attività consente di rilevare e neutralizzare eventuali dispositivi hardware o software installati sui sistemi o sulla rete che potrebbero inviare dati all'esterno, tenere traccia delle attivita?effettuate dall'utente, danneggiare i contenuti presenti, alterare il funzionamento del sistema operativo stesso.
- **Vulnerability Check**: scansione delle vulnerabilità integrata con una valutazione del rischio circa i potenziali danni che potrebbero derivare da un ipotetico attacco a quel sistema.
- **Phishing Simulation**: verifica del grado di consapevolezza relativo alla sicurezza IT e attività di formazione per tutto il personale aziendale finalizzata ad innalzare la consapevolezza nei confronti del rischio phishing.

Vulnerability Scan

Oggi **le aziende sono costantemente esposte al rischio di attacchi** ai loro sistemi **informatici**. Per questo un'**adeguata difesa** è di fondamentale importanza per conservare la propria competitività. L'attività consente di rilevare e neutralizzare eventuali dispositivi hardware o software installati sui sistemi o sulla rete che potrebbero inviare dati all'esterno, tenere traccia delle attività effettuate dall'utente, danneggiare i contenuti presenti, alterare il funzionamento del sistema operativo stesso.

L'analisi verifica le eventuali falle presenti, al fine di individuare, vulnerabilità agli attacchi conosciuti, ossia aree esposte ad essere violate da parte di soggetti malintenzionati.

Vengono analizzate da remoto una o più macchine per determinare se queste sono vulnerabili agli attacchi conosciuti e quindi potenzialmente esposte ad essere violate da parte di cracker.

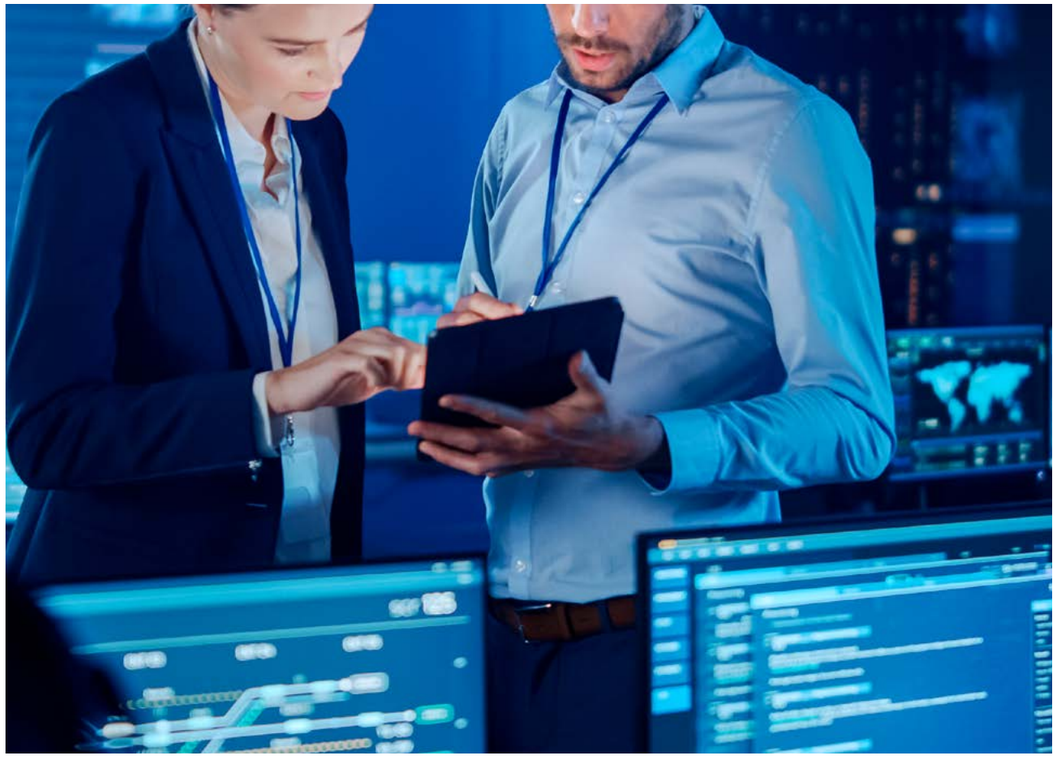
Può essere effettuata su:

- **Siti Web**: per individuare errori di configurazione del web server e di programmazione di un sito web.
- **Siti E-Commerce**: per individuare debolezze ed errori di configurazione del web server e di programmazione di un sito di E-Commerce.
- **Web Application**: per individuare errori di configurazione e vulnerabilità di una Web Application.
- **Router o Firewall(IP Pubblico)**: per individuare errori di configurazione di un Router o di un Firewall.
- **Server Web (o Server raggiungibili da remoto)**: per individuare errori di configurazione di un Server Web o di Server raggiungibili da remoto.

A seguito degli interventi correttivi per correggere le vulnerabilità emerse durante la scansione iniziale può essere effettuata una **Scansione di Controllo (Vulnerability Scan di Controllo)**, al termine della quale viene rilasciato un report delle risultanze.

La Scansione di controllo deve essere effettuata entro 30 gg dalla Scansione iniziale.

La scansione comprende la realizzazione del **report finale** della Scansione delle Vulnerabilità del Server Host e delle singole Web Application.



Phishing Simulation

Il phishing è un business molto lucrativo. Gli attacchi hanno registrato una crescita record negli ultimi anni, e un programma efficace di sensibilizzazione sulla sicurezza costituisce parte integrante di tutte le strategie di difesa in profondità.
Per la maggior parte delle aziende, gli utenti finali sono il punto di attacco più esteso e più vulnerabile. Negli attacchi che si possono attualmente osservare, gli utenti vengono costantemente bombardati da tentativi di spearphishing e stratagemmi di ingegneria sociale.
Capire le vulnerabilità dei tuoi utenti è essenziale per fornire formazione sulla sicurezza adeguata e identificare i più ampi rischi di sicurezza informatica per la tua azienda.
Il progetto dura sei mesi e si articola come segue:

Fase 1: Fase di inizio progetto
- definizione degli obiettivi.
- definizione dei 3 template d'attacco in base a livelli di criticità crescenti.
- Organizzazione temporale delle attività.

Fase 2: Attacco #1 e Report #1
Fase di attacco con 3 invii in più giorni (3 template d'attacco).
Al termine della fase d'attacco verrà redatto il report che espone le metriche definite durante la pianificazione.

Fase 3: Formazione in e-learning
Erogazione del percorso formativo in e-learning per correggere le lacune emerse dal 1° Report d'attacco.

Fase 4: Test di valutazione
Test di valutazione a seguito del percorso formativo per valutare se e come è cambiata la sensibilità dei dipendenti verso questa tipologia di attacchi. Il test è utile per valutare anche il grado di coinvolgimento che questa tipologia di attività genera nei dipendenti stessi.

Numero Aziendale
+41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

Fase 5: Attacco #2 e Report #2
Fase di attacco con 3 invii in più giorni (3 template d'attacco).
Al termine della fase d'attacco verrà redatto il report che espone le metriche definite durante la pianificazione.

Fase 6: Analisi finale e formazione integrativa
Analisi finale per valutare quanto e come è migliorata la percezione di pericolo ed il grado di attenzione dei dipendenti verso questi temi.
È prevista una sessione di formazione integrativa per i soggetti che risultano al di sotto di un dato livello minimo di apprendimento.

Penetration Test

L'obiettivo è quello di **evidenziare le debolezze della piattaforma**, fornendo il maggior numero di informazioni sulle **vulnerabilità tecnologiche** che ne hanno permesso l'**accesso non autorizzato**: si tratta sostanzialmente di mettersi dalla parte dell'hacker, il quale, sfruttando le vulnerabilità rilevate, è in grado di ottenere ogni informazione necessaria per l'accesso all'infrastruttura informatica.

Il servizio di Penetration Test è da considerarsi obbligatorio per adempiere il principio di Accountability del GDPR.

L'attività di **penetration testing** può essere svolta in due modalità:
- **approccio cd. blind**, prevedendo la simulazione di un attacco "alla cieca", cioè senza che al nostro team di pen-tester vengano fornite informazioni sull'infrastruttura informatica oggetto di attacco;
- **approccio cd. tandem**, prevedendo la simulazione di attacco in cui vengono fornite al team informazioni sull'infrastruttura informatica oggetto di attacco.

Il test, svolto dai nostri esperti specializzati nel settore, si compone di 7 fasi tutte volte ad individuare le vulnerabilità di una infrastruttura informatica:

Information Gathering
L'Information Gathering è il primo step per effettuare un penetration test. Tale fase consiste nella **ricerca di tutte le informazioni essenziali per lo svolgimento del test**, informazioni di cui in seguito il tester si servirà per eseguire l'attacco al sistema o alla rete informatica. Alcuni degli strumenti più utilizzati in questa fase sono: Osint, Domainhostingview, Ipnetinfo, Theharvester, Dns Analysis, Google, Maltego, Recon-Ng.

Footprinting
È la fase di **raccolta delle informazioni** espletata attraverso particolari tecniche di analisi che includono l'ingegneria sociale, la ricerca su internet e il cosiddetto "Dumpster-Diving".

Discovery and Scanning
Si prevede l'esecuzione di **scansioni automatizzate e semi-automatizzate** non invasive condotte avvalendosi di alcuni strumenti tra cui Nessus, Nmap, Net Discovery, Ids/Ips Identification, Burpsuit, al fine di **rilevare la presenza di vulnerabilità** note all'interno dell'infrastruttura informatica oggetto di analisi.

Numero Aziendale
+41 (0) 91 921 30 30
www.insideagency.ch | info@insideagency.ch

Vulnerability Assessment
Il Vulnerability Assessment è un processo per mezzo del quale si ricercano e **si valutano eventuali vulnerabilità e minacce**, in termini di sicurezza, del sistema informatico o della rete oggetto di analisi. Tutte le vulnerabilità riscontrate sono oggetto di analisi da parte dei nostri professionisti i quali individuano le vulnerabilità reali e i falsi positivi. I nostri esperti utilizzano strumenti automatizzati i quali dispongono di un proprio database in grado di fornire informazioni accurate su tutte le vulnerabilità, siano esse più o meno recenti.

Exploitation
Durante questa fase vengono "sfruttate" le vulnerabilità individuate durante il Vulnerability Assessment. In particolare, gli exploit sono dei programmi che approfittano delle vulnerabilità del sistema per fornire dei privilegi amministrativi all'attaccante. Vengono dunque messi in atto **processi volti all'intrusione** dei sistemi nonché all'eventuale evasione delle misure di sicurezza presenti, di tipo tecnologico e procedurale.

Post-Exploitation
Consiste nella **raccolta delle informazioni ottenute** (comprese le password) e dei privilegi acquisiti durante l'Exploitation.

Report
Individuate tutte le vulnerabilità presenti nel sistema o nella rete, i nostri esperti saranno in grado di fornire **informazioni dettagliate sulle vulnerabilità esistenti**. A questo punto si procede alla redazione e alla successiva consegna al cliente del **rapporto informativo** che espone in modo analitico, completo ed oggettivo le attività svolte, le vulnerabilità emerse e il loro indice di gravità, i possibili rischi che queste possono comportare e i rimedi da adottare.

Physical Penetration Test

Il **Physical Penetration Test consiste nella simulazione di uno scenario di minaccia reale** in cui un soggetto malintenzionato tenta di compromettere le barriere fisiche di un'azienda per ottenere l'accesso a infrastrutture, edifici, sistemi, dipendenti e aree sensibili contenenti dati.

L'obiettivo è quello di rilevare con metodologia investigativa le vulnerabilità della sicurezza complessiva di un'azienda prima che eventuali soggetti malevoli siano in grado di scoprirle e sfruttarle. Attraverso l'identificazione di questi punti deboli è possibile attuare misure di mitigazione adeguate a rafforzare la sicurezza generale tutelando il Business dell'azienda.

La metodologia applicata prevede 6 fasi:

1. **Information Gathering**: acquisizione di dati utili in merito al sistema in esame. Avviene attraverso i sopralluoghi e la ricognizione delle strutture e delle procedure inerenti il personale presente, l'intervista alle risorse e l'analisi delle informazioni reperite nelle c.d. fonti aperte (O.S.INT. – Open Source Intelligence).
2. **Threat modeling**: processo di identificazione, classificazione e analisi delle potenziali minacce con valutazione del rischio e previsione delle contromisure.
3. **Vulnerability analisis**: ricerca ed analisi delle vulnerabilità.
4. **Exploitation**: sfruttando le vulnerabilità individuate, si creano punti di accesso ad un sistema o ad una risorsa bypassando le restrizioni di sicurezza.
5. **Post Exploitation**: attività finalizzate a mantenere il controllo delle strutture oggetto dell'attività, successiva all'accesso e bypassate le restrizioni di sicurezza.
6. **Report**: relazione sulle attività svolte con dettaglio delle risultanze.

Managed Detection and Response (MDR)

A livello globale, l'elevato danno causato alle aziende dalla progressiva crescita di minacce informatiche, rende necessaria l'implementazione di opportune prassi di sicurezza informatica aziendale. In gioco non c'è solo la continuità operativa, ma anche la capacità di poter continuare a competere sui mercati nazionali ed internazionali.

L'obiettivo è la CyberResilienza: l'identificazione delle attività critiche e degli scenari di rischio più probabile con l'implementazione delle capacità di rilevare eventi di sicurezza sospetti, prevedendo anche piani di emergenza.

Il **Managed Detection and Response (MDR)** è un servizio finalizzato ad ottenere la **CyberResilienza** in maniera gestita, supportando le aziende impossibilitate a gestire internamente i processi per la prevenzione e la gestione degli incidenti informatici. La formula della Managed Detection and Response, che prevede in estrema sintesi l'**esternalizzazione delle attività di security**, consente di affrontare questo passaggio evolutivo in un quadro di sostenibilità economica: la sua adozione consente di migliorare l'efficacia degli stessi sistemi di protezione.

In qualità di **provider di servizi MDR, INSIDE** fornisce analisti altamente competenti, specializzati nell'utilizzo di strumenti di sicurezza all'avanguardia e mette a disposizione dei clienti un menu di servizi progettati per migliorare le difese di un'azienda e ridurre al minimo i rischi, senza l'oneroso investimento che richiederebbe la costruzione di un team interno e l'acquisto di strumenti dedicati.

Un ruolo di primo piano, per esempio, è rivestito dai servizi di Threat Intelligence che consentono di monitorare costantemente le nuove minacce e di adattare gli strumenti di protezione per farvi fronte. La nostra attività, sotto questo profilo, garantisce l'accesso a una maggiore quantità di dati e, di conseguenza, si concretizza in una maggiore efficacia nel contrasto al cyber crimine.

Grazie al costante monitoraggio degli eventi di sicurezza in rete, i servizi di Managed Detection and Response consentono di adeguare l'infrastruttura aziendale ai requisiti previsti dalle normative (GDPR) in tema di gestione dei Data Breach, assicurando la piena soddisfazione degli standard previsti dal legislatore.

Di seguito i servizi disponibili:

CYBER SECURITY AWARENESS

La migliore strategia di difesa di fronte ad attacchi informatici sempre più sofisticati e mirati è sicuramente la cyber security awareness, la formazione in tema di sicurezza informatica. La maggior parte degli incidenti di sicurezza, infatti, è dovuta ad errori umani a conferma del fatto che il cosiddetto "fattore H", il fattore umano, rimane il punto debole della cyber security in azienda.

Alcune stime parlano, addirittura, di un 80-90% di incidenti informatici riconducibili a errori umani o comportamenti errati del personale. Errori involontari, dovuti a negligenza e disattenzione del personale interno all'azienda, ma anche intenzionali compiuti da lavoratori infedeli che effettuano operazioni di sabotaggio ai danni della propria organizzazione.

Per questo motivo abbiamo realizzato una serie di **percorsi formativi, su temi di uso quotidiano, necessari a creare la corretta consapevolezza di come, alcuni comportamenti, siano pericolosi per l'intera azienda e possano vanificare sforzi e investimenti**.

Il servizio proposto si basa su una piattaforma di eLearning che si compone di tre sottosistemi:

1. AWARENESS
È un innovativo sistema di e-learning pensato specificatamente per il personale non specialistico delle organizzazioni pubbliche e private. Il primo sistema che si fonda su metodologie di formazione che tengono conto delle modalità di apprendimento digitale che risultano maggiormente efficaci. Il sistema è stato progettato per coinvolgere tutta l'organizzazione in un percorso di apprendimento educativo e stimolante, che si caratterizza per un approccio "a rilascio costante e graduale":

2. PHISHING
È una soluzione innovativa di training Anti Phishing che produce risultati efficaci grazie alla sua particolare metodologia addestramento esperienziale. Basato su automazione e machine learning , la soluzione è rivolta a tutto il personale delle organizzazioni pubbliche e private, esso consente di mantenere "allenate" due importanti caratteristiche difensive umane: la prontezza e la reattività. Questo risultato viene raggiunto mediante la simulazione di campagne di Phishing cui vengono sottoposti tutti gli utenti (una mail al mese). Mail diverse verranno mandate dal sistema ai diversi utenti ed il livello di difficoltà di ogni esercitazione varierà per ogni utente sulla base delle reali prestazioni di ogni utente. Il sistema si propone come la naturale integrazione ai programmi formativi della soluzione di Awareness, aumentando la reattività dell'individuo di fronte ad attacchi basati su tecniche di Phishing. Considerando che i maggiori pericoli per la sicurezza delle organizzazioni sono "in agguato" nelle caselle e-mail dei loro dipendenti e collaboratori, le simulazioni di attacco Phishing, messe in atto dalla soluzione, "personalizzate" sulla base delle caratteristiche peculiari di ogni singolo utente, preparano dipendenti e collaboratori a modificare i comportamenti e ad individuare con prontezza mail di phishing.

3. CYBER CHANNEL (opzionale)
È una piattaforma che pubblica su base mensile video di alta qualità, della durata di 5-8 minuti l'uno, che analizzano dei casi di attacchi/frodi cyber. I format utilizzati sono diversi (Cyber Detective, Break News, Sit-Com). Ogni video è poi dotato di un documento di approfondimento che analizza più nel dettaglio il fatto cyber affrontato nel video.

CYBER SECURITY CONTROL ROOM (CSCR)

La Cyber Security Control Room (CSCR) è il servizio di **gestione della sicurezza informatica in outsourcing** pensato per le aziende che non hanno al loro interno una struttura organizzata per la presa in carico delle tematiche legate al mondo della Cyber Security.

Gli operatori della CSCR sono in grado di gestire la sicurezza delle reti e degli asset delle aziende con l'obiettivo di **difendere proattivamente le infrastrutture da minacce informatiche provenienti sia dall'interno dell'azienda che dall'esterno**.

Il servizio permette di eseguire azioni pro-attive, prevenendo e mitigando gli attacchi informatici provenienti dalla rete Internet e dagli asset aziendali.

Ciò è possibile grazie all'analisi di tutte le fonti log di interesse prodotte dagli asset per la difesa dell'infrastruttura aziendale e di una serie di informazioni provenienti da fonti aperte (Open Source Intelligence), residenti all'interno di un database di intelligence.

Viene **erogato tramite personale altamente specializzato e certificato**, dedicato al controllo della vostra infrastruttura e dotato di strumenti specialistici per effettuare anche indagini forensi qualora fosse necessario.

MANAGED DETECTION & RESPONSE (MDR)

I servizi gestiti di **rilevamento e risposta incidenti**, Managed Detection and Response (MDR) prevedono un'attività di **monitoraggio delle minacce H24/7**, il rilevamento eventi di incidente e la capacità di mitigazione e risposta.

Sfruttano una combinazione di:
- Tecnologie implementate agli strati host e di rete;
- Analisi avanzate;
- Intelligenza sulle minacce (threat intelligence);
- Competenze di professionisti e analisti nell'indagine e nella risposta dell'incidente.

La soluzione tecnica è in grado di **proteggere le workstation, i server e i dispositivi mobili del cliente dalle minacce note e sconosciute** e dispone di **funzionalità avanzate**, come l'analisi comportamentale e l'intelligenza artificiale, che aumentano notevolmente la capacità di rilevare e rispondere ad attività malevole.

I servizi vengono erogati attraverso una piattaforma proprietaria che garantisce il monitoraggio di tutti gli endpoints, dai server agli apparati mobile. Il servizio di Detection & Response è attivo H24/7, curato da analisti esperti.

I due momenti principali sono la:

1. DETECTION: l'analisi approfondita ad ampio spettro consente di bloccare e contenere l'attacco.

2. REMEDIATION: attività finalizzata alla messa a punto di soluzioni di riparazioni del sistema da eseguirsi attraverso la piattaforma proprietaria.

Il nostro approccio prevede che nella risposta agli incidenti un notevole contributo sia fornito dalla Theat Intelligence e dall'Artificial Intelligence.

Infatti la grande mole di informazioni sulle minacce provenienti dalle fasi di Detection e rilevate dai comportamenti dell'aggressore, attraverso la Theat Intelligence e l'Artificial Intelligence, acquistano valore predittivo, utile a comprendere come si muoverà l'avversario, i suoi obiettivi e le sue motivazioni.

La nostra piattaforma unifica la gestione della protezione da minacce per PC, Mac, dispositivi mobili e server, in modo che tutti gli endpoint siano adeguatamente protetti. La piattaforma raccoglie dati e monitora in tempo reale tutti i dispositivi presenti nell'environment ed attraverso i propri agent fornisce gli strumenti per proteggere gli endpoint, compresi i dispositivi mobile.

Gli agent (o moduli attivi) agiscono in triplice direzione:

1. DETECTION & REMEDIATION:

- Analisi e correlazione dei dati raccolti dai sensori presenti negli endpoint;
- Individuazione delle minacce e della storia completa dell'attacco;
- Ricerca in tempo reale in Database proprietario contenente decine di milioni di eventi che consente una risposta pressoché immediata (pochi secondi) dopo il Triage;
- Esecuzione di una delle seguenti riposte:
  - Remediation
  - Killing dei processi
  - Impedimento all'esecuzione del file
  - Rimozione dei meccanismi di persistenza
  - Messa in quarantena del file
  - Rimozione chiavi di registro
  - Isolamento della macchina
  - Aggiunta del dominio/indirizzo IP dell'attaccante al Database

2. MODULO DI SUPPORTO:

Le sue funzioni sono:

- Sostituzione o supporto all'antivirus di terze parti
- Rilevazione nuove minacce o in evoluzione prima che vengano eseguite attraverso la Machine Learning
- Memory Exploit Mitigation: blocco delle vulnerabilità zero-day
- Blocco Ransomware prima che venga eseguita la crittografia
- Blocco degli attacchi fileless, attraverso PowerShell o .NET
- Controllo diretto degli endpoint: gestione centralizzata delle funzioni strategiche degli endpoint, quali l'accesso a dispositivi USB, l'accesso alla rete, controllo dello stato della crittografia del disco.

3. MOBILE AGENT:

Operante su dispositivi Android e IOS e fornisce protezione ai dispositivi basandosi sull'analisi comportamentale per individuare attività sospette, quali quelle di app mobili, connessioni di rete anomale e vulnerabilità proprie del sistema operativo.

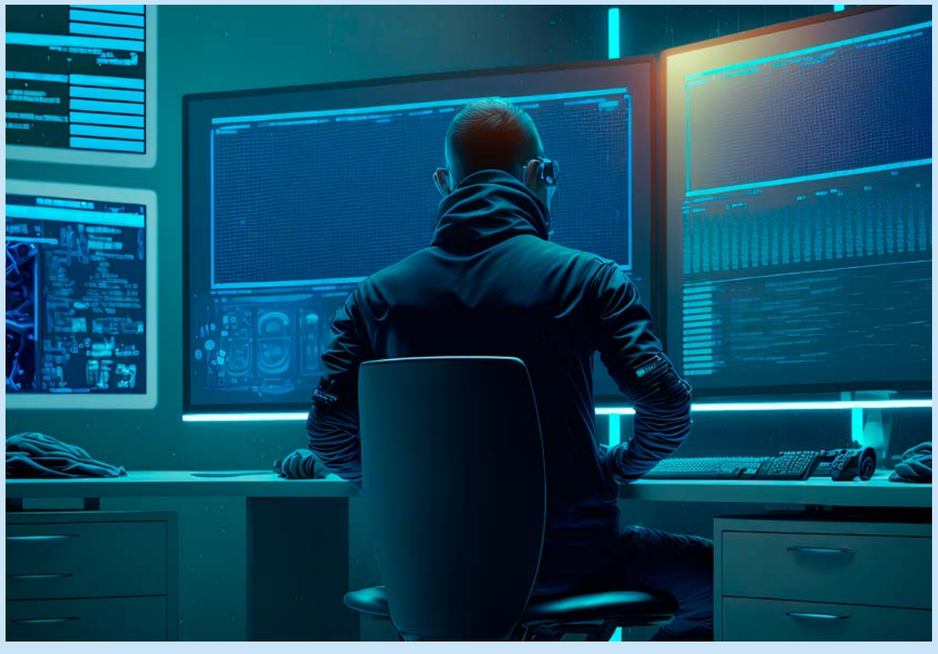
FOCUS RANSOMWARE

I Ransomware sono **una particolare tipologia di virus che si sta diffondendo negli ultimi anni**. Il loro comportamento consiste nell'**infettare un device criptando tutti i dati dell'utente** (Documenti, Immagini, ecc) in esso contenuti e, successivamente chiedendo un riscatto che, dietro pagamento, permette di riavere tutti i propri dati in chiaro.

Da quando i Ransomware sono stati individuati per la prima volta la loro **diffusione** è stata **esponenziale** e sono stati intercettati **diverse tipologie** di questi particolari worm virus. Tra i più importanti sono noti i seguenti:

- Reveton
- CryptoLocker
- TorrentLocker

Questa tipologia di virus non è da sottovalutare e, in alcune realtà, è in grado di bloccare l'operato di un'azienda o di causarne forti perdite finanziarie e di immagine. Dall'analisi del comportamento dei Ransomware si è rilevato che **il mezzo più utilizzato per la loro diffusione sono le email** dove celandosi dietro un finto fornitore di servizi vengono inviati allegati che, una volta aperti, avviano l'infezione del Pc e la criptazione di tutti i dati.



Red Team (Offensive Security)

La **Offensive Security** adotta un **approccio offensivo – ma etico – di hacking**, proattivo e antagonistico per proteggere sistemi informatici, reti e individui dagli attacchi. La sicurezza convenzionale, a volte indicata come "sicurezza difensiva", si concentra su misure reattive, come l'applicazione di patch al software e la ricerca e la correzione delle vulnerabilità del sistema.

Le misure di sicurezza offensiva si concentrano sulla ricerca degli autori e in alcuni casi sul tentativo di disabilitare o almeno interrompere le loro operazioni, fornendo una visione "dall'esterno" di sistemi, reti, software e procedure aziendali.

L'attività si caratterizza per la capacità di **simulare un avversario reale** (crimine organizzato, azienda concorrente, lavoratore scontento) ed operare attenendosi quanto più possibile alla mentalità e alle risorse che lo stesso avrebbe a disposizione.

Gli ambiti presi in considerazione sono:

- **Tecnologico**: violazione del perimetro, dei servizi esposti, applicazioni web, router, appliances
- **Umano**: social engineering contro lo staff
- **Fisico**: accesso a edifici o proprietà aziendali

Lo scopo è dunque quello di **fornire una fotografia del livello di rischio reale** a cui una azienda o ente è soggetto.

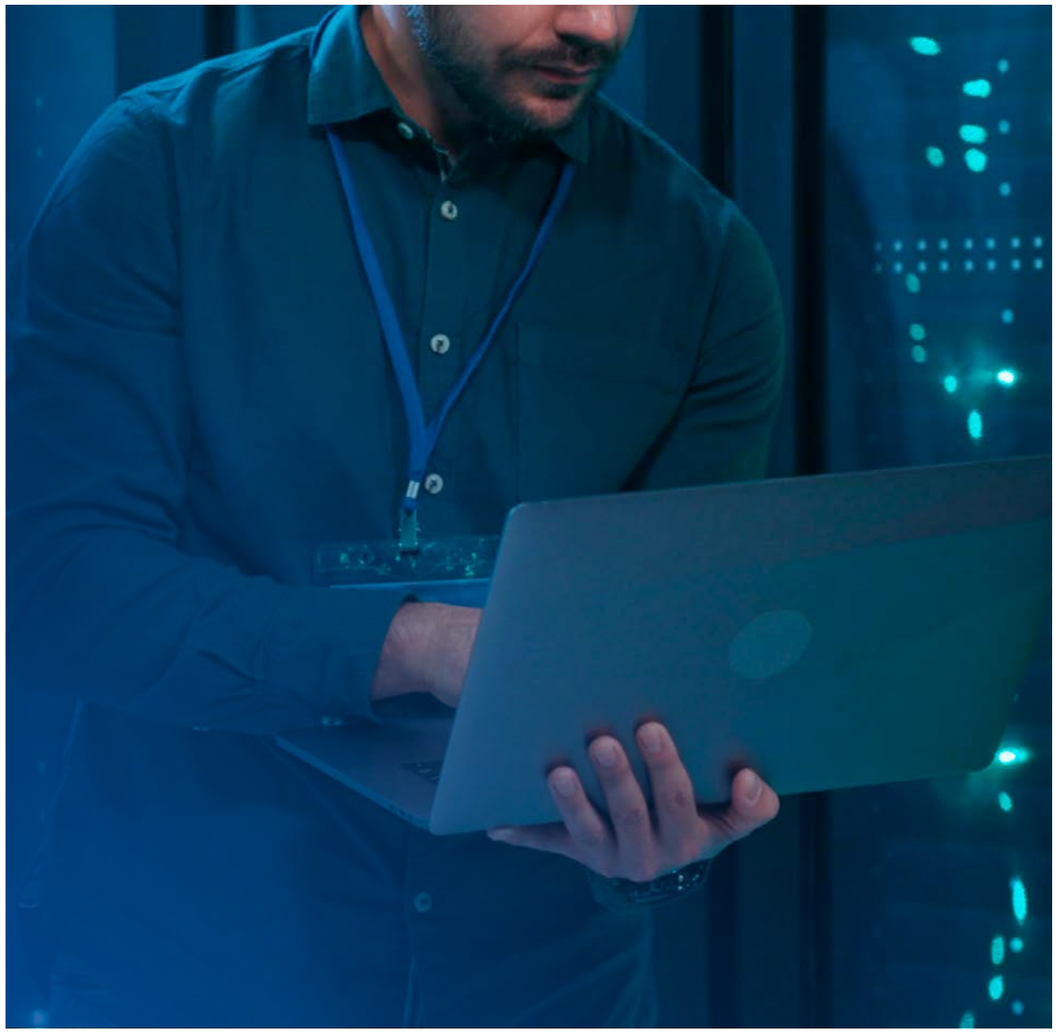
Le fasi sono molto simili a quelle di un Penetration Test tradizionale, sebbene più strutturate. Il Penetration Test ha lo scopo di individuare e validare il maggior numero di vulnerabilità presenti sui sistemi di un'azienda. Non fornisce alcun tipo di indicazione rispetto a quali potrebbero essere le azioni intraprese da un reale attaccante.

L'Offensive Security **condotto da un team di ethical hackers** è in grado di **mostrare** invece quali possano essere **le modalità operative di un attaccante** che voglia avere accesso alle informazioni aziendali. L'attacco sfrutta anche la **componente umana**, che spesso è la vulnerabilità principale nella sicurezza delle organizzazioni: quanti dipendenti potrebbero aprire una e-mail di phishing o cliccare sul link presente o addirittura compilare un form? Le conseguenze di queste azioni sarebbero danni economici per la fuoriuscita di dati sensibili ovvero danni di immagine.

Il test viene **condotto in modalità BlackBox** la quale prevede l'attaccante non disponga di alcuna informazione preventiva sui sistemi target che non siano di pubblico dominio. In questo modo le vulnerabilità sfruttate saranno quelle rilevabili dall'esterno dalla rete, esattamente come in una situazione reale di attacco.

Le fasi:

- **Reconnaissance**: approfondita ricerca di informazioni sull'azienda target per la preparazione dell'attacco.
- **Weaponization**: preparazione del materiale specifico da utilizzare per il test, come payload, trojan, campagne di social engineering o hardware da installare durante gli accessi fisici.
- **Delivery**: avvio delle operazioni di attacco pianificate, campagne di social engineering (attraverso lo sfruttamento delle vulnerabilità del fattore umano tramite tecniche di Phishing, Impersonation, Baiting, ecc) o analisi delle vulnerabilità presenti sui sistemi.
- **Exploitation**: questa fase ha l'obiettivo di compromettere i sistemi, violare la sicurezza fisica (sfruttando le falle presenti nei sistemi di controllo) e logica del target.
- **Installation**: è la fase in cui il team esegue azioni di preparazione per il mantenimento dell'accesso alle risorse compromesse con tentativi di privilege escalation, installazione di payload o fino alla duplicazione delle chiavi di accesso fisico alle strutture target.
- **Maintain Access**: è la fase di mantenimento dell'accesso remoto ai sistemi compromessi, con lo scopo di eseguire in seguito le attività conclusive del test.
- **Actions**: finalizzazione dell'assessment: generalmente consiste in una esfiltrazione di dati sensibili, tuttavia può coinvolgere una serie di azioni specifiche, in base allo scopo concordato con il cliente.
- **Process Evaluation**: validazione dell'efficacia dei processi di security fisica e logica aziendale attraverso l'analisi dei risultati ottenuti durante il test.



I NOSTRI SERVIZI

Security

Security manager

Il **Security Manager** supporta direttamente l'azienda studiando, sviluppando e attuando strategie e piani operativi, al fine di prevenire e fronteggiare situazioni che possono danneggiare l'azienda.

La **Divisione Security** di INSIDE mette a disposizione dei propri clienti la **competenza di professionisti esperti e certificati** nell'ambito del Security Management, per gestire gli aspetti tecnici, organizzativi, economici ed umani connessi alla sua funzione.

All'interno delle Organizzazioni, indipendentemente dall'ambito in cui operano, l'equilibrio gestionale può essere alterato da una serie di eventi di diversa natura: ogni tipo di organizzazione è infatti costantemente esposta a minacce di natura dolosa, colposa o accidentale, in relazione ai processi produttivi, alle azioni dei dipendenti, ai rapporti con l'esterno e, più in generale, all'essere parte di un mondo globalizzato caratterizzato dall'incertezza e dalla conflittualità.

Diventa essenziale, perciò, la tutela del patrimonio tangibile e intangibile, comprese le persone sia dell'Organizzazione sia quelle che con questa interagiscono.

L'approccio integrato alla sicurezza aziendale di INSIDE consente alla società di **disporre in un'unica soluzione di tutti i servizi dell'ambito Security,** compresi la Business Intelligence, le Investigazioni Aziendali e la Cyber Security, evitando il ricorso a terzi per attività di **analisi reputazionale** delle controparti, di **indagini a tutela del patrimonio e dei diritti aziendali** (ad esempio nei casi di assenteismo da parte dei dipendenti) nonché per i servizi di messa in sicurezza delle infrastrutture informatiche.

Il **Security Management** così concepito previene e contrasta le minacce ai beni, agli interessi e all'immagine dell'azienda a 360°: INSIDE effettua un monitoraggio e una valutazione costante dei rischi connessi alle attività e predispone con il supporto della Governance le misure più adatte alla neutralizzazione ed al contenimento degli eventi dannosi.

Tra le **principali funzioni** del Security Manager:

- salvaguardia e messa in sicurezza delle strutture aziendali;
- gestione e tutela del personale;
- formalizzazione di processi interni di sicurezza aziendale;
- difesa dell'immagine e della reputazione aziendale;
- risoluzione di controversie legali;
- valutazione circa l'affidabilità di opportunità commerciali;
- definizione di strategie per il contenimento dei costi;
- organizzazione di eventi e meeting aziendali;
- conseguimento delle certificazioni professionali richieste dallo specifico ambito di operatività;
- instaurazione di rapporti con organi istituzionali e/o politici per la gestione di affari particolarmente delicati;
- tutela di reti informatiche, archivi informatici e/o cartacei nonché di ogni altra documentazione e/o informazione di carattere riservato;
- prevenzione di attacchi informatici in grado di mettere in pericolo il know-how aziendale.

Consulenza risk management e analisi del rischio

ANALISI E VALUTAZIONE DEL RISCHIO

Consente di determinare i rischi, quantitativi e qualitativi, in termini probabilistici, derivanti da potenziali **sorgenti di pericolo**, mediante una mappatura del Vostro dispositivo di sicurezza (inteso quale insieme di tecnologie, uomini, processi e infrastrutture impiegati per la sicurezza), con una valutazione di ogni singola area analizzata e un'analisi del gap risultante tra il dispositivo in essere e quello da Voi atteso, ovvero, effettuata anche l'**analisi della minaccia (threat analysis o threat assessment)**, è possibile misurare il gap tra il dispositivo in essere e il dispositivo necessario per fronteggiare la minaccia con adeguati suggerimenti per mitigare o trasferire il rischio.

Le tipologie di rischio dipendono dallo specifico obiettivo perseguito dall'impresa. Si tratta di rischi:

- operativi;
- finanziari;
- strategici;
- di immagine;
- informativi;

Tutto questo calibrando sempre **efficienza, efficacia e sostenibilità**, e in conformità a quanto previsto dallo **standard ISO/IEC 27002 i**n materia di **sicurezza dell'informazione**.

RISK ASSESSMENT

Il Risk Assessment, o analisi del rischio, è uno specifico processo del Risk Management, diretto all'identificazione dei rischi, da classificare all'interno di un documento denominato "Draft Generale dei Rischi", al fine di garantire la **salvaguardia degli asset aziendali e finanziari**. In generale, si può ricorrere alla metodologia del Risk Assessment ogniqualvolta si intenda misurare la pericolosità di un evento indesiderabile definendo la priorità o l'urgenza delle misure necessarie per prevenirlo e/o monitorarlo. Dopo aver individuato le priorità, si identificano dapprima i beni, gli asset e le attività da tutelare, poi le minacce e i relativi rischi a questi connesse; infine si individuano strategicamente le misure per ridurre tali rischi.

Physical Security Assessment

Il **Physical Security Assessment** è un'**attività di verifica volta a determinare il livello di sicurezza complessivo dell'azienda**, non solo logico, bensì anche fisico, a tutela dei beni patrimoniali e delle persone, della riservatezza dei dati, delle conversazioni e delle comunicazioni.

Si tratta di un'attività multidisciplinare che **riguarda l'analisi e la verifica dei protocolli di sicurezza logica e fisica** delle infrastrutture aziendali.

L'evoluzione delle minacce, dinamiche e modalità con le quali le stesse possono verificarsi sono alla base dei Risk Assessment, che hanno lo scopo di evidenziare lo stato delle cose del dispositivo in essere, le **vulnerabilità presenti e le soluzioni da implementare per ridurre al minimo il rischio**, ovvero la probabilità che un evento dannoso si verifichi all'interno della propria azienda.

Le operazioni di Physical Security Assessment si distinguono in 3 diverse fasi:

1. Colloquio preliminare col cliente mediante questionari ed interviste: la finalità è duplice, individuare i processi di business critici al fine di garantirne la sicurezza e continuità e portare alla luce eventuali incident accaduti nel passato e relativi track record delle contromisure e procedure adottate sulla base dell'esperienza vissuta.Risultano di fondamentale importanza per verificare il livello di security aziendale, oltre che per contrastare lo specifico evento già accaduto.

2. Verifica volta a rilevare all'interno e all'esterno dell'azienda, le vulnerabilità presenti nei sistemi di sicurezza, negli impianti, nelle procedure di accesso e nella rete informatica attraverso la mappatura degli asset, delle vulnerabilità, dei possibili rischi e della loro entità.

In particolare nel corso dell'attività vengono effettuate le seguenti operazioni:

- Verifica di funzionamento dei sistemi antintrusione esterni ed interni alla struttura aziendale.
- Controllo dell'efficienza dei sistemi di videosorveglianza con riguardo alle policies di accesso ai sistemi ed ai contenuti, anche in ottica di compliance al GDPR.
- Verifica del funzionamento dei sistemi di controllo degli accessi nelle varie aree aziendali e dei privilegi assegnati al personale in virtù dei ruoli e delle mansioni.
- Test di assessment sugli edifici al fine di valutare la possibilità di elusione dei sistemi antintrusione.
- Bonifiche elettroniche, volte ad individuare sistemi di intercettazione ambientale e telefonica.
- Al termine delle attività viene rilasciata al cliente una relazione contenente gli esiti dell'attività.

3. Sviluppo delle strategie per la risoluzione delle criticità emerse con lo sviluppo delle contromisure atte a ridurre o mitigare eventuali rischi impattanti sul business specifico e con la verifica delle possibili soluzioni implementabili in ottica antintrusione e antintercettazione delle comunicazioni sia a livello logico che fisico che in ordine all'adozione di protocolli di accesso riservati alle risorse dell'azienda.

Executive Protection

Il servizio di executive security garantisce la **protezione di soggetti ritenuti suscettibili di attentati o violenze**, ed eventualmente di loro familiari, prestando loro assistenza durante viaggi o più semplicemente nello svolgimento dell'ordinaria attività professionale, senza tuttavia intaccarne la privacy. Il **piano di protezione** è personalizzato in base alle esigenze del Cliente, e commisurato in relazione al tipo e alla gravità del pericolo cui è potenzialmente sottoposto il soggetto, assicurando la difesa in qualsiasi momento, durante ogni spostamento sul territorio nazionale ed internazionale, su percorsi stradali, aeroportuali e marittimi, e presso la sede di lavoro nonché il domicilio. A tal scopo il personale della **Divisione Security di INSIDE** risponde a rigorosi requisiti psico-fisici e si presta ad una costante preparazione fisica, oltre all'aggiornamento sulle novità giuridico-normative, tecniche e psicologico-sociali in materia.

Security Driver

La Divisione Security di INSIDE, con la massima riservatezza, discrezione e professionalità, propone il **servizio di driver o autista di sicurezza** per ogni specifica esigenza.

Il servizio può essere richiesto per:

- incarichi a lungo termine
- singoli eventi
- esigenze di sicurezza personali di manager, politici, ecc
- viaggi
- spostamenti da aeroporti
- congressi o fiere
- trasferimenti e protezione di individui con necessità di trasporto di oggetti personali di valore.

Il **personale è altamente qualificato**, anche grazie alla costante e periodica formazione in materia di guida sicura.

Inside
INTELLIGENCE | SECURITY | INVESTIGATIONS

INSIDE INTELLIGENCE & SECURITY INVESTIGATIONS S.A.
Via Serafino Balestra, 27 - CH-6900 LUGANO Tel. +41 (0) 91 921 3030
www.insideagency.ch - info@insideagency.ch

Autorizzazione rilasciata dalla Polizia Cantonale - Repubblica e Cantone Ticino
in base alla Legge sulle prestazioni private di sicurezza ed investigazione (LPPS)
del 9 Novembre 2020 per lo svolgimento delle attività di Investigazione,
Raccolta informazioni inerenti le persone

Inside

INTELLIGENCE | SECURITY | INVESTIGATIONS

www.insideagency.ch
info@insideagency.ch

HEADQUARTER

SWITZERLAND - LUGANO
Via Serafino Balestra, 27
LUGANO, 6900

Numero Aziendale
+41 (0) 91 921 30 30

UFFICI NEL MONDO

ITALY - MILAN
Corso Venezia, 8
20121 - MILANO
Tel. +39 02 82 39 67 69

ITALY - ROME
Via Ludovisi, 35
00187 - ROMA
Tel. +39 06 42 03 73 97

UK - LONDON
Crown House, 72
Hammersmith Rd
W14 8TH - Hammersmith
Tel. +44 20 3608 3481

USA - NEW YORK
6800 Jericho Turnpike
Syosset
11791 - NEW YORK
Tel. + 1 929 476 0740

HONG KONG
25 Westlands Rd., Quarry Bay
Berkshire House, 24th
2402-07 - HONG KONG
Tel. +852 5808 2950

SOUTH AFRICA - CAPE TOWN
First Floor, Willowbridge
Centre, 39 Carl Cronje Dr
7530 - CAPE TOWN
Tel. +27 87 550 23 25

RUSSIA - MOSCOW
31st floor, stroenie 1, bld. 3,
Begovaya str,
125284 - MOSCOW
Tel. +7 495 118 1472

EMIRATES - DUBAI
Level 2
Central 1 Building
Dubai World Trade Center
Tel. +971 4 523 2471

BRAZIL - SAÕ PAULO
Top Center Paulista
Paulista Avenue, 854
Bela Vista - 10th floor
01310-913 - SÃO PAULO
Tel. +55 11 3197 5914