

Veille Économique
Enquêtes sur les assurances
Enquêtes Sur Les Sociétés
Sécurité Informatique
Data Protection Officer
Sécurité

**Votre certitude
se trouve juste là**

À propos de nous	2
------------------------	---

3

Veille Économique

Diligence préalable et conformité	3
Gouvernance, Gestion des Risques et Conformité	3
Contrôle de la conformité	4
Enquêtes de recouvrement de créances	5
Intelligence Étranger	6
Dossier d'Enquête de Diligence Préalable	6

9

Enquêtes sur les assurances

Insurance Anti Fraud Intelligence - Enquêtes sur les assurances	9
Insurance Intelligence pour dommages matériels	9
Insurance Intelligence pour dommages physiques	9

10

Enquêtes sur les Sociétés

Enquêtes sur les Salariés	10
Enquête sur l'Infidélité d'Entreprise	10
Enquêtes avant embauche	11
Enquête sur sur l'absentéisme	12
Abus en matière d'absence au travail (loi 104)	13
Enquêtes sur le Travail dissimulé	14
Enquête sur les vols	14
Sécurité Anti-sabotage	14
Enquêtes sur les partenaires et les concurrents	15
Concurrence Déloyale	15
Manquement à l'obligation de loyauté des partenaires	16
Contre-espionnage industriel	16

17

Digital Security

Cyber Sécurité	17
Évaluation et Atténuation de la Vulnérabilité	17
Test d'Intrusion	18
Test d'Intrusion d'Application Internet	18
Détection et Analyse des Menaces	19
Identification du Piratage Informatique	19
Contre-espionnage Informatique	19
Délégué à la protection des données	20
Expertise Judiciaire Numérique et Mobile	28
Expertise Judiciaire des Réseaux	28
Expertise Judiciaire des Bases de Données	28
Expertise Judiciaire Informatique	28
Expertise Judiciaire Mobile	28
Bonifications environnementales et électroniques	29

30

Sécurité

Sécurité	30
Security Manager	30
Maritime Security	31
Conseil Stratégique pour la Sécurité	31
Évaluation des risques	31
Rapport sur les Risques par Pays	31
Protection des Personnalités	32
Chauffeur Sécurité	32
Sécurité des voyages	32

À propos de nous

INSIDE, conformément à la législation, aux principes d'éthique professionnelle et aux règles de gouvernance d'entreprise, recueille, sur le territoire national et international, des informations utiles aux entreprises dans la gestion du risque (ou risk management), donc dans l'évaluation des risques économiques, financiers et de réputation des organismes et personnes physiques avec lesquels une entreprise est susceptible d'établir des relations d'affaires.

Cet ensemble d'informations permet de mettre en place des stratégies et des techniques appropriées pour prévenir les pièges caractérisant les différents secteurs du marché (industries pharmaceutiques, automobiles, d'assurance, financières, administration publique...) pouvant intéresser aussi bien les petites entreprises que les grandes sociétés.

Les rapports publiés peuvent également concerner les PPE, à savoir les personnes politiquement exposées, ayant exercé par le passé des fonctions publiques et étant donc plus facilement exposées au risque de perpétration de certains crimes tels que la corruption, la malversation, le blanchiment d'argent...

INSIDE assiste les organisations pour une meilleure connaissance de leurs partenaires commerciaux, en orientant les activités de ces dernières vers des choix plus éclairés, à travers une série de services parfaitement conformes à la législation et au respect des obligations légales et d'audit (dispositions du Foreign Corrupt Practices Act - FCPA, Bribery Act du Royaume-Uni, loi anti-blanchiment – AML, Anti-Money Laundering, USA PATRIOT Act et lutte contre le financement du terrorisme – CFT, Countering the Financing of Terrorism). Les recherches effectuées - pouvant concerner tous les secteurs du marché et toute organisation, quelle que soit sa taille - permettent un contrôle approfondi des possibles relations commerciales, mettant en évidence les risques de corruption découlant d'une analyse géopolitique du cas.

Les rapports fournissent des informations sur l'entreprise et ses dirigeants, les activités, son histoire, la gestion, les conflits d'intérêts, le passif financier, les affaires juridiques et judiciaires (risques de conformité), le risque de réputation. Ils comprennent également des vérifications sur les déclarations des administrateurs, le caractère conforme face à la loi anti-blanchiment (AML), aux contrôles anti-corruption et la conformité au règlement FCPA et UKBA, aux sanctions contre l'Iran, aux procédures de due diligence préalable internationale et américaine.

Le recours aux rapports INSIDE est généralement recommandé dans le cadre de vérification de crimes financiers, mais pas seulement : les recherches d'INSIDE représentent une solution viable en présence d'un risque géopolitique (Pays à haut risque) relatif à une transaction ou à un individu, pour des contrôles sur la chaîne d'approvisionnement et de due diligence, avant d'effectuer d'importants investissements de type fusion ou acquisition, et pour un programme de conformité intégré.

INSIDE procède elle-même aux enquêtes, permettant ainsi de maintenir un niveau de qualité élevé et des délais optimum. Elle fait appel à un grand nombre d'opérateurs situés sur les cinq continents, avec plus de 60 langues internationales parlées. Elle dispose également de professionnels natifs des lieux d'enquête, capables donc de comprendre les nuances de la langue souvent incompréhensibles pour qui n'appartient pas à une culture donnée. Les informations et données recueillies « open source » sont nombreuses et de qualité, sachant que les différentes sources utilisées sont constamment mises à jour sur la base d'informations officielles étrangères.

Nous sommes associés à...



CERTIFICATION ISO 9001:2015



Veille Économique

Diligence préalable et conformité

Nos rapports sont les outils les plus appropriés pour vérifier la valeur et l'état de santé de partenaires commerciaux et de salariés potentiels.

Prenez des décisions éclairées et efficaces pour éviter que votre entreprise n'encoure des risques économiques, des dommages financiers et des préjudices de réputation. Découvrez nos services et choisissez le type de rapport qui vous convient le mieux.

Gouvernance, Gestion des Risques et Conformité

Dossier de Réputation de la société

Ce dossier contient des informations issues de sources extérieures, concernant les entités juridiques.

L'évaluation porte sur **le degré d'exposition au risque des personnes morales ou organismes**, et donc de leurs dirigeants. Il est notamment procédé à l'étude de l'historique des activités de ces entités (risque opérationnel) et du parcours en termes de réputation (risque de réputation), des conditions économiques, du risque de conformité (procédures juridiques et judiciaires).

Elle comprend de plus l'indication de tous les événements de nature commerciale ayant concerné l'entité en question durant les 5 à 10 dernières années (procédures judiciaires, protestations, procédures de faillite, enregistrements et transcriptions légales), les vérifications de nature patrimoniale et, pour les seules sociétés anonymes, l'analyse des indices financiers provenant de la comparaison des postes des derniers états financiers.

Les informations légales publiques de l'entreprise sont ensuite complétées par **les résultats recueillis sur place** et les indications obtenues de la part des opérateurs économiques du secteur d'expertise spécifique.

Le dossier est ensuite clôturé avec un **avis sur la fiabilité** (opinion concernant le crédit susceptible d'être accordé).



Contrôle de la conformité

Contrôle de la conformité et vous saurez tout sur vos clients

Le service permet de contrôler la clientèle, en vérifiant plus particulièrement sa présence dans des bases de données spécifiques, dont la liste figure ci-dessous :

Listes Anti-Terrorisme

Ces listes sont établies par les législateurs et institutions des différents pays.

Listes Anti-Blanchiment Italie

Ces listes contiennent plus de 400 000 noms de personnes physiques et entités impliquées dans des crimes de ce type sur le territoire italien, et sont conformes aux dispositions législatives internationales en la matière.

Listes PIL

Ces listes contiennent les noms de politiciens locaux italiens (régionaux, provinciaux, municipaux).

Listes Pep Internationales

Ces listes contiennent plus de 400 000 noms de personnes politiquement exposées, dans plus de 240 pays, identifiées selon les directives du GAFI (Groupe d'Action Financière Internationale) contre le blanchiment d'argent et les normes internationales applicables en la matière.

Listes des Sites de Jeu Illégal

Ces listes indiquent les sites de redirection et les sociétés internationales possédant des sites sans autorisation AAMS (Administration Autonome des Monopoles d'État).

Liste Noire et Liste de Surveillance

Ces listes contiennent les noms des personnes recherchées par les autorités nationales ou internationales, telles que la DIA, le FBI, Interpol ou les gouvernements, des personnes figurant dans les listes judiciaires ou dans celles d'organismes gouvernementaux, ou encore des individus faisant l'objet d'ordonnances émises par les autorités financières telles que la FINMA, ou organismes de surveillance.



Enquêtes de recouvrement de créances

Enquête a 360° pour Recouvrement de Créances

Le service est recommandé en cas de différend et permet d'**évaluer la situation économique et financière** effective du débiteur, avant même d'entreprendre des poursuites judiciaires susceptibles de se révéler vaines en cas d'indigence reconnue ou autres restrictions.

Concernant les **PERSONNES PHYSIQUES**, les informations fournies sont les suivantes:

- Identification complète et adresse du domicile
- Recherche de nouvelles lignes téléphoniques publiées outre celles éventuellement communiquées
- Détermination et confirmation des activités professionnelles (employé/travailleur indépendant/à la retraite)
- Informations d'état des lieux
- Vérification des intérêts du sujet dans toute société en Italie
- Recherche d'investissements du sujet dans des sociétés de capitaux sur le territoire national
- Extrait du registre des propriétés nationales/biens immobiliers
- Recherche des biens immobiliers en location
- Recherche de véhicules voiture/moto à son nom
- Vérification des protestations et actes préjudiciables (tribunaux et services de conservation des registres fonciers)
- Références bancaires
- Avis final de recouvrabilité

Concernant les **PERSONNES MORALES**, les informations suivantes seront fournies :

- Identification juridique du sujet par le biais du Registre des entreprises
- Confirmation de présence d'activités réelle sur place et/ou recherche des éventuel(s) nouveau(x) siège(s)
- Informations à partir de sources confidentielles sur place
- Recherche de nouvelles lignes téléphonique publiées outre celles éventuellement fournies par le débiteur
- Adresse du domicile déclaré du représentant légal
- Recherche de véhicules voiture/moto à son nom
- Extrait du registre des propriétés nationales/biens immobiliers
- Recherche des biens immobiliers en location
- Recherche d'adjudication de marchés

Enquête a 360° pour Recouvrement de Créances avec Information Financiere

Une trousse d'information contenant les informations fournies par le service "Enquête sur 360° pour la collecte de la dette" et de l'**information financière** intégrée découlant de l'activité de **Human Intelligence**, ou à partir d'une collecte d'informations auprès des établissements de crédit, visant à identifier les relations bancaires de personne physique ou morale recherchée.



Intelligence Étranger

Nos services de sélection vous permettent de certifier vos partenaires commerciaux et vos fournisseurs à l'échelle internationale.

Nos services de sélection vous permettent de certifier vos partenaires commerciaux et vos fournisseurs à l'échelle internationale.

Dossier d'Enquête de Diligence Préalable

Protection contre les atteintes à la réputation et les dommages financiers

L'activité de renseignements d'INSIDE est en mesure de **détecter les risques en matière de relations d'affaires et interpersonnelles à l'échelle mondiale**, mais également les risques liés à la vie commerciale et aux faits impliquant les sujets en examen, lesquels sont susceptibles d'avoir un impact sur quiconque entreprend une relation avec une entité étrangère. Les informations recueillies sont utilisées pour composer des profils hautement structurés.

Pour les organisations, le contrôle de diligence préalable représente une technique de **protection contre les dommages à la réputation** et les dommages financiers. Il permet en effet d'effectuer des vérifications d'antécédents sur des individus ou des organismes dans le monde entier afin de sensibiliser les entreprises quant à leurs partenaires d'affaires. Ce service est effectué par des spécialistes présents dans le monde entier et parlant plus de 60 langues (incluant des locuteurs natifs capables de saisir les nuances linguistiques souvent imperceptibles à qui n'appartient pas à la culture d'un pays donné).

Le sujet est varié : contrôles anti-corruption, anti-blanchiment, contrôles préliminaires aux opérations de type fusions, acquisitions ou joint-ventures, contrôles de la chaîne d'approvisionnement, contrôles de diligence préalable sur les agents, consultants, distributeurs, investisseurs immigrés (demandes de résidence fiscale), sur des sujets liés à des pays à haut risque et autres individus fortunés...

Les enquêtes couvrent plus de 240 pays, avec des centaines de référents actifs 24 heures sur 24, 7 jours sur 7.

Les recherches concernent également les individus ou entités figurant dans toutes les listes de personnes passibles de sanctions, listes de surveillance, listes des autorités de surveillance et forces de l'ordre, et s'intéressent aux faits de criminalité financière, terrorisme et criminalité organisée en général.



Il s'agit souvent de personnes déjà impliquées dans des procédures pénales, mais non encore condamnées, et susceptibles de porter atteinte à la réputation d'une entreprise. Ce type de phénomène associatif pourrait s'avérer d'autant plus coûteux que les éventuelles sanctions financières imposées suite à des violations de conformité.

Les activités de recherche répondent également aux obligations de diligence préalable des régimes KYC (Know Your Customer – Connaître votre client), AML (Anti Money Laundering – Anti-blanchiment d'argent), CFT (Countering the Financing of Terrorism – Contrer le financement du terrorisme) et PEP (Politically Exposed Person – Personne politiquement exposée).

Les informations recueillies et figurant dans le dossier, lesquelles font l'objet de mises à jour et de contrôle qualité continus, sont d'origine publique:

- médias mondiaux (plus de 100.000 sources);
- informations issues de registres publics locaux et internationaux;
- sources spécifiques pour chaque pays et par secteur;
- sources d'informations en langue étrangère;
- informations stockées dans nos bases de données;
- sources mondiales d'information de conformité;
- informations accessibles au public mais difficiles à trouver;
- signalements négatifs sur médias internationaux;
- environ 400 listes d'individus passibles de sanctions, liste de surveillance, listes des autorités de surveillance et forces de l'ordre (les enquêtes INSIDE permettent souvent d'identifier des personnes à haut risque avant même que leur nom ne figure dans les listes officielles).

Les informations sont analysées en détail, divisées et associées entre elles (en effet, souvent, il s'agit de gérer une énorme quantité de données) grâce à des procédures de screening de pointe et autres procédés de recherche soignés. Elles font en outre l'objet de contrôles qualité stricts. Tout ceci permet de simplifier les processus de conformité, avec notamment des économies de coûts en termes de temps de résolution, accélérant ainsi le rythme des opérations.

Pour soutenir les activités de screening AML et CFT, certaines fonctions permettant d'obtenir des informations spécifiques sont prévues:

- **Sanctions en temps réel:** il s'agit d'une solution relative au respect des procédures de paiement permettant d'obtenir des informations actualisées sur les sanctions imposées aux organismes effectuant des contrôles sur les transferts d'argent à durée de vie critique;



- **Intérêt Économique Iran (IEI):** permet aux entreprises de suivre les clients, employés et partenaires d'affaires en général, afin de détecter les risques de violations des sanctions contre l'Iran;
- **Intelligence country-check ou Contrôle international:** fournit des informations de niveau international sur les aspects économiques, politiques et criminels en soutien aux activités de diligence préalable en matière de blanchiment d'argent;
- **informations sur le secteur maritime IHS:** permet d'obtenir des informations sur l'identité, la structure (actuelle et historique) et l'emplacement des navires de compagnies armatrices, ainsi que des informations relatives à tous les navires marchands à moteur en service avec tonnage équivalent ou supérieur à 100 GT;
- **US SAM (System for Award Management – Système de gestion des octrois):** fournit des informations sur les personnes faisant l'objet de restrictions ou d'exclusion de relations avec le gouvernement américain.

Le dossier fournit un cadre complet du risque: informations sur les organisations, sur leurs propriétaires, leurs dirigeants, leurs liens avec la politique et le crime organisé, sur les conflits d'intérêts.

Ce dossier est rédigé en anglais dans un court laps de temps (de 10 à 15 jours ouvrables) pour des coûts contenus (car INSIDE s'occupe personnellement de leur traitement).

Le service est matériellement présenté sous forme de tableau : les tableaux facilitent la compréhension des informations et l'évaluation des risques, d'autre part, les liens ayant permis de trouver les informations sont également fournis et permettent de les vérifier.

En conclusion, une fiche de synthèse et une section de renseignements commerciaux ont été prévus.

Les méthodes utilisées sont orientées vers une discrétion absolue: les personnes visées par l'enquête ne savent pas faire l'objet d'une enquête.

Parmi les rapports les plus spécifiques:

- conformité anti-blanchiment (AML);
- vérification des déclarations des administrateurs;
- vérifications anti-corruption et de conformité aux lois anti-corruption américaines (FCPA) et britanniques (UKBA);
- sanctions contre l'Iran;
- Diligence préalable internationale et américaine.



Insurance Anti Fraud Intelligence

Insurance Anti Fraud Intelligence - Enquêtes sur les assurances

INSIDE Agency peut accompagner les compagnies d'assurance dans la gestion des sinistres et des vols concernant l'objet des polices

Des preuves certaines qui permettent une gestion consciente des risques

Insurance Intelligence pour dommages matériels

DOMMAGES MATÉRIELS (vol et réclamations)

Grâce à son réseau international de collaborateurs, **INSIDE** est en mesure d'aider les compagnies d'assurances à gérer les **sinistres** et les **vols** concernant l'objet des polices (voitures, mais aussi objets de valeur, appareils et systèmes informatiques). Les enquêtes, analyses et collectes d'informations, qui peuvent être utilisés dans le contexte de la réparation et/ou des pratiques de compensation, sont effectués dans le strict respect de la réglementation en vigueur concernant la protection de la vie privée (législations nationales et Règlement de l'UE n° 679/2016), fournissant contextuellement un **contexte probant certain** permettant au Client de gérer consciemment les risques et d'atténuer leur impact.

Insurance Intelligence pour dommages physiques

DOMMAGES PHYSIQUES (accidents et maladies branche assurance)

Les unités opérationnelles d'INSIDE Agency garantissent des interventions rapides et efficaces dans les activités d'observation, statiques et/ou dynamiques, de personnes soupçonnées de ne pas être atteintes des pathologies pour lesquelles l'activation de la couverture d'assurance a été demandée. Les services d'observation sont fournis conformément aux dispositions légales applicables et aux législations nationales et au règlement de l'UE n° 679/2016 relatif à la protection de la vie privée.



Enquêtes sur les Sociétés

Enquêtes sur les Salariés

Évaluez la fiabilité de vos salariés au moyen d'enquêtes visant à protéger et à préserver les actifs de l'entreprise et à déceler toute inconduite.

Nous vous fournirons des solutions complètes et personnalisées selon vos besoins.

Enquête sur l'Infidélité d'Entreprise

La réglementation sur le manquement à l'obligation de loyauté vise à protéger l'entreprise contre tout comportement particulièrement déloyal de la part des salarié ou de partenaires pouvant nuire à l'entreprise ou la désavantager, tel que des actes d'espionnage et/ou de sabotage ou d'autres actes professionnellement incorrects commis par des partenaires ou des dirigeants.

En cas de suspicion de manquement à l'obligation de loyauté, INSIDE AGENCY engage une série de procédures d'enquête à l'encontre du partenaire ou du salarié visant à mettre en évidence et à documenter tous les comportements qui sont considérés comme incorrects et préjudiciables à l'entreprise et qui violent l'obligation de loyauté professionnelle précitée.

L'obligation de loyauté s'inscrit dans le cadre plus large du devoir de coopération du salarié, qui le place dans une position de collaboration et non d'hostilité envers l'entreprise.

Violation des obligations de loyauté et des engagements de confidentialité

L'art. 2105 du code civil impose une obligation de loyauté aux salariés en interdisant de « traiter des affaires pour leur propre compte ou pour le compte de tiers en concurrence avec l'entrepreneur » et de « divulguer des informations concernant l'organisation et les méthodes de production de l'entreprise ou de les utiliser de manière à lui porter préjudice ».

Dans le premier cas, il est fait référence à l'interdiction d'exercer des activités, pendant et en dehors des heures de travail, qui pourraient de quelque manière que ce soit entrer en conflit avec celles de l'employeur. L'interdiction s'applique



en particulier aux salariés qui, en raison des fonctions qu'ils exercent, peuvent entrer en conflit avec les intérêts de l'entreprise en impliquant éventuellement une clientèle commune à l'employeur.

Dans le second cas, il est fait référence à l'ensemble des informations confidentielles strictement liées à la sphère de l'entreprise qui peuvent concerner l'organisation de l'entreprise, les flux économiques, les commandes, les clients, les relations avec les fournisseurs, les états financiers, les salariés et tout autre événement interne qui peut être préjudiciable s'il est divulgué, y compris en termes de perte de compétitivité vis-à-vis des entreprises concurrentes.

Exécution d'une activité professionnelle non déclarée auprès de tiers et perception de revenus dissimulés tout en bénéficiant d'allocations dans le cadre d'un plan social.

Le comportement du salarié qui, pendant la période où il bénéficie d'allocations dans le cadre d'un plan social, exerce des activités de travail non déclarées auprès d'un autre employeur, est considéré comme un manquement à l'obligation de loyauté ; par conséquent, le salarié peut être licencié pour faute en tant qu'auteur d'un comportement si grave qu'il ne permet pas, même temporairement, la poursuite de la relation de travail.

Mauvais usage des actifs et des outils de l'entreprise

Le mauvais usage ou l'utilisation à des fins personnelles des biens de l'entreprise ou, plus généralement, du matériel informatique appartenant à l'entreprise, constitue un facteur de risque pour l'employeur, non seulement en termes de maintien de l'intégrité du matériel utilisé, mais surtout en termes de sécurité des données dont le salarié dispose.

INSIDE AGENCY vérifie et documente les comportements qui mettent en évidence l'utilisation possible d'actifs et d'outils de l'entreprise à des fins autres que celles prévues.

Enquêtes avant embauche

L'inclusion d'un nouveau professionnel au sein d'une structure (par exemple un nouveau directeur) est considérée comme un investissement majeur pour la société. Un choix hasardeux et exempt des précautions nécessaires pourrait cependant permettre l'attribution d'un poste stratégique à la mauvaise personne et, avec le temps, avoir des répercussions d'un point de vue logistique, économique/financier sur l'entreprise, sans oublier l'effet négatif en termes de réputation.

INSIDE met toute une série d'activités d'enquête à disposition des membres des hautes directions d'entreprise chargés de procéder à ce type de sélection. Ces mesures sont **en totale conformité avec les dispositions de l'article 8 de la loi 300/70 (Statut des travailleurs)**, et ont pour but d'évaluer la capacité du candidat.

Plus précisément, il s'agit d'un **dossier d'investigation «personnalisé» sur la personne physique et/ou le partenaire d'entreprise**, visant à déterminer sa fiabilité en tant qu'interlocuteur dans les relations commerciales et/ou fonctions professionnelles et/ou sociétaires.

Tous les indicateurs de validité et de fiabilité du sujet sont pris en compte, au même titre que les informations recueillies sur place concernant d'éventuels préjudices commerciaux et/ou personnels.

La confiance que l'employeur doit pouvoir placer dans un salarié est une condition préalable au succès d'une entreprise.



Enquête sur sur l'absentéisme

L'article 2119 du Code civil prévoit la possibilité de résilier un contrat "avant son expiration naturelle si le contrat est à durée déterminée, ou sans préavis, si le contrat est à durée indéterminée, en présence d'un motif empêchant la poursuite, même temporaire, du rapport".

Toutefois cependant, l'employeur rencontre de grandes difficultés quant à faire valoir ses droits en absence de **preuves réelles et documentées**.

INSIDE mène des enquêtes ciblées visant à trouver et documenter tout élément de preuve pertinent permettant de légitimer le licenciement d'un employé peu correct, en particulier en identifiant les causes d'absence et/ou de comportement opportuniste et incompatible avec la relation de travail, afin de démontrer:

- **Existence de faits et de raisons valables justifiant les absences pour maladie du salarié:**

Le comportement du salarié qui a agi frauduleusement envers l'employeur en simulant un état de maladie constitue une violation de contrat de nature à porter préjudice à la poursuite, même temporaire, de la relation de travail. La vérification d'une telle circonstance donne à l'employeur le droit de licencier le salarié pour faute.

Inside Agency possède les compétences et le professionnalisme nécessaires pour fournir à ses clients une assistance visant à satisfaire leurs besoins en matière de collecte et d'analyse de tous les éléments utiles à l'objet de l'enquête.

- **Existence de faits et de raisons valables justifiant les absences du salarié dues à un accident:**

L'accident se distingue de la maladie par le fait qu'il s'agit d'un accident survenu pendant les heures de travail, sur le chemin du travail ou sur le chemin d'un lieu de travail à un autre. En effet, il arrive souvent que le salarié, en prétendant être victime d'un accident, s'abstienne du travail pour exercer une autre activité professionnelle ou pour se livrer à des activités totalement incompatibles avec l'incapacité temporaire et partielle présumée causée par l'accident, ou qu'il décide lui-même de prolonger la période d'absence nécessaire à la récupération, alors que celle-ci s'est déjà produite. Ce comportement constitue une violation de contrat de nature à porter préjudice à la poursuite, même temporaire, de la relation de travail. La vérification d'une telle circonstance donne à l'employeur le droit de licencier le salarié pour faute.

Inside Agency possède les compétences et le professionnalisme nécessaires pour assister ses clients dans la collecte et l'analyse de tous les éléments utiles et fiables par rapport à l'objet de l'enquête.

- **L'adoption par le salarié d'un comportement qui, eu égard à l'étendue et à la nature de la maladie ou de l'accident, est susceptible de nuire ou de retarder son rétablissement:**

Le salarié qui, au cours d'une maladie ou d'un accident, se comporte de manière à entraver le processus de guérison en contribuant au contraire à aggraver son état de santé, est susceptible d'être licencié dans la mesure où il y a manquement aux obligations contractuelles de diligence et de loyauté ainsi qu'aux devoirs d'honnêteté et de bonne foi de nature à mettre fin à la relation de confiance entre l'employeur et le salarié, qui est un élément essentiel de la relation de travail salarié, et à empêcher la poursuite, même temporaire, de cette relation.



Enquêtes sur les Sociétés

- **L'utilisation régulière et correcte des autorisations d'absence syndicales et parentales prévues par la loi n° 104/1992.**
- **L'utilisation régulière et correcte des permis syndicaux.**
- **La fausse attestation de la présence d'un salarié dans l'entreprise au moyen de l'apposition du badge par un collègue:**

La fausse attestation de la présence d'un salarié dans l'entreprise au moyen de l'apposition du badge par un collègue représente un comportement préjudiciable à la relation de confiance existant entre l'employeur et le salarié de nature à justifier le licenciement de ce dernier (art. 55 quater du décret législatif 165/2001). La carte de pointage est un document destiné à l'usage exclusif du titulaire non transférable à des tiers. Un comportement non conforme constitue une violation des devoirs de diligence et de bonne foi, ce qui justifie l'employeur à licencier pour faute l'auteur de l'inconduite.

Si l'on soupçonne que le salarié ne se trouve pas à son poste de travail, même s'il est présent dans le service, ou qu'il soit parti sans qu'un titre spécifique l'y autorise, l'employeur peut demander l'intervention d'experts pour vérifier la conduite contraire au droit du salarié.



Abus en matière d'absence au travail (loi 104)

L'abus ou la mauvaise utilisation des absences en raison de la prise en charge de membres de la famille porteurs d'un handicap, invalides ou non autosuffisants, justifie le licenciement pour faute du salarié qui exerce, au cours de ces permissions, d'autres activités que les soins et l'aide au parent dans le besoin.

Ce comportement, qui revêt des aspects de gravité et de dévalorisation morale et sociale, constitue un abus de la loi ainsi qu'une violation des principes d'honnêteté et de bonne foi, permettant à l'employeur de mettre en place des contrôles visant à vérifier l'usage abusif ou un usage à des fins autres que celles pour lesquelles la demande a été faite.



Enquêtes sur le Travail dissimulé

Des salariés qui sont absents pour cause de maladie travaillent pour un autre employeur, même s'il est un membre de leur famille. Un tel comportement est-il susceptible de licenciement pour faute ?

Il est constant dans la jurisprudence qu'elle admet la légitimité du licenciement pour faute dans tous les cas où le salarié exerce, pendant la période de maladie (ce qui est encore plus grave en cas de compensation non déclarée, de concurrence avec l'employeur ou de défaut de respecter l'obligation de confidentialité), une activité de travail incompatible avec la pathologie déclarée en retardant sa guérison et donc en retardant son retour au travail. Une telle conduite porte irrémédiablement atteinte à la relation de confiance qui devrait exister entre le salarié et l'employeur, puisqu'elle présuppose une violation des devoirs de diligence, de loyauté, de bonne foi et d'honnêteté que le salarié est tenu de respecter.

Le pourcentage de salariés qui sont absents de leur travail pour exercer une deuxième activité est assez significatif, au détriment de l'entreprise non seulement en termes économiques mais aussi en termes de productivité et de compétitivité sur le marché.

INSIDE AGENCY défend ses clients en cas d'attaques internes et/ou externes afin de garantir une protection adéquate des actifs de l'entreprise en identifiant les auteurs des infractions.

Enquête sur les vols

L'appropriation illicite d'actifs corporels et incorporels est l'un des problèmes les plus courants dans les entreprises en Italie et ailleurs. INSIDE AGENCY soutient les entreprises dans la collecte de preuves pour identifier les auteurs de comportements illicites en les encourageant à prendre des mesures préventives et adopter des instruments appropriés pour réduire les risques pouvant compromettre l'image de l'entreprise.

Le vol d'actifs d'entreprise justifie le licenciement pour faute quelle que soit la valeur et le volume des actifs volés. Ce qui importe, c'est le comportement malhonnête du salarié qui, en tant que tel, a un impact sur la relation de travail en intégrant les caractéristiques d'une «conduite susceptible de jeter le doute sur le bon accomplissement de sa mission à l'avenir, car elle est symptomatique d'une certaine attitude du salarié à l'égard des obligations qu'il a assumées».

Sécurité Anti-sabotage

Le salarié qui endommage, y compris avec l'appui de personnes extérieures à l'entreprise, les biens d'équipement de l'entreprise tels que les machines, les bureaux et les systèmes informatiques ou incite ses collègues à des actes de sabotage, adopte une conduite qui est préjudiciable à la performance et à l'image de l'entreprise, entraînant la perte totale de fiabilité de celle-ci, et qui justifie l'adoption de sanctions disciplinaires sous la forme du licenciement pour faute.

Par le biais d'une enquête minutieuse, INSIDE AGENCY soutient les entreprises dans la recherche de la vérité en leur proposant d'adopter des mesures appropriées pour prévenir de tels phénomènes et protéger les actifs de l'entreprise.



Enquêtes sur les partenaires et les concurrents

Protégez votre entreprise contre les actions déloyales de vos partenaires ; lutez contre la concurrence déloyale avec notre appui.

Nous avons la bonne solution pour toutes les éventualités en fournissant des rapports de haute valeur juridique.

Concurrence Déloyale

Les cas de concurrence déloyale et de contrefaçon des produits/marques sont des phénomènes de plus en plus diffusés en Italie, notamment en raison de la présence démesurée des pays de l'Est, et principalement la Chine, insérant sur nos marchés des produits ignorant toutes les normes internationales.

Il est important de préciser que selon le Code civil italien (article 2598), outre les dispositions relatives à la protection des signes distinctifs et des droits de brevet, un acte de concurrence déloyale est effectivement commis par toute personne

- *utilisant les noms ou signes distinctifs susceptibles de générer des confusions avec des noms ou des signes distinctifs légitimement utilisés par d'autres, ou imitant servilement les produits d'un concurrent, ou effectuant de toute autre façon des actes impliquant une confusion avec les produits et l'entreprise d'un concurrent;*
- *diffusant des nouvelles et commentaires sur les produits et activités d'un concurrent impliquant son discrédit ou s'appropriant les mérites de produits ou des activités d'un concurrent;*
- *utilisant directement ou indirectement tout autre moyen non conforme aux principes d'intégrité professionnelle susceptibles de porter préjudice à une autre entreprise*

INSIDE, après une analyse minutieuse du cas, mettra en place une série d'enquêtes ainsi que des expertises visant à **vérifier un cas de concurrence déloyale et/ou la contrefaçon de produits** ayant impliqué des dommages économiques et d'image à la société détenant la marque et le savoir-faire relatif.



Enquêtes sur les Sociétés

Manquement à l'obligation de loyauté des partenaires

Les enquêtes sur le manquement à l'obligation de loyauté de vos partenaires vous permettent de savoir exactement si un partenaire entretient des relations conflictuelles avec la société à laquelle il appartient, par exemple en divulguant des informations strictement confidentielles à des tiers ou en se comportant d'une manière contraire aux devoirs qu'il doit accomplir en sa qualité de partenaire. L'enquête vous permettra d'identifier le partenaire déloyal tout en évitant de dangereuses fuites d'informations vers l'extérieur, afin de préserver et valoriser le savoir-faire de l'entreprise.

Contre-espionnage industriel

De plus en plus souvent, les entreprises sont confrontées au délicat problème de l'espionnage industriel mis en place par des individus ou des organisations qui en sont chargées, dont le but principal est d'exploiter le travail d'autrui pour obtenir illégalement des bénéfices et des avantages en utilisant des outils technologiques, des stratégies et des méthodologies très différentes les unes des autres : par exemple, le vol de données, d'objets, de projets, de plans, de brevets, de logiciels, de listes de noms, de listes de clients, d'études de marché.

De plus en plus souvent, l'espionnage est mené par les salariés ou grâce à leur coopération. Il est donc important d'utiliser des techniques de contre-espionnage pour faire face efficacement à ces phénomènes.

Recourir au contre-espionnage signifie donc protéger votre entreprise. INSIDE AGENCY est en mesure de vous fournir des solutions spécifiques et personnalisées pour chaque besoin, grâce à des contrôles ciblés de la vulnérabilité des salariés, des collaborateurs et des partenaires menés en utilisant des outils technologiques de pointe.



Digital Security

Cyber Sécurité

Vérifier le degré de vulnérabilité de votre système informatique

Identifier les interventions adaptées pour sécuriser les biens informatiques grâce à nos services de sécurité informatique, qui apportent une solution à chaque besoin.

Évaluation et Atténuation de la Vulnérabilité

La méthode d'évaluation et atténuation de la vulnérabilité (ACV) adoptée par le service Cyber Security d'INSIDE, consiste en une série d'activités non-invasives visant à **évaluer l'efficacité et le degré de robustesse des systèmes de sécurité adoptés** par votre entreprise, en identifiant les vulnérabilités connues en cas d'attaque informatique. Ces premiers stades d'intervention sont suivis par la mise en place de mesures destinées à l'amélioration de la sécurité de vos systèmes.

L'adoption du VAM doit être organisée périodiquement tout au long de l'année, dans la mesure où la technologie est en constante progression au même titre que les outils d'attaque des systèmes.

Le service Cyber Security d'INSIDE développe les niveaux de VAM suivants:

- **Base de données:** notre analyse se concentre en particulier sur les bases de données principalement utilisées par les entreprises (SQL Server Microsoft, Oracle, SyBase Server, etc...). L'intervention passe par l'utilisation d'instruments et de logiciels hautement sophistiqués, et prévoit une analyse automatique de ces bases de données, visant à identifier et à analyser les points faibles, soit les plus faciles à attaquer. Chaque entreprise « conserve » les informations internes dans ces bases de données. Ces dernières, faisant l'objet de réorganisations constantes afin d'optimiser leur exploitation, sont exposées à des attaques malveillantes de la part des concurrents.
- **Réseau téléphonique:** les attaques au réseau téléphonique sont communément appelées WarDial. Ces attaques informatiques sont fréquemment utilisées car le réseau téléphonique est plus vulnérable à la présence de mouchards (bugs). L'intervention se concentre sur le balayage de l'intégralité du réseau téléphonique composé de centrales téléphoniques, modems, appareils téléphoniques, etc.



Test d'Intrusion

Évaluer la sécurité d'un système ou d'un réseau

Le test d'intrusion est un service d'évaluation de la sécurité d'un système ou d'un réseau, passant par la simulation d'une attaque par un agent de menace interne ou externe. L'objectif est de mettre en évidence les faiblesses de la plate-forme, en fournissant le plus d'informations possibles sur les vulnérabilités ayant permis l'accès non autorisé : il s'agit essentiellement de se mettre à la place du hacker, lequel, par le biais des vulnérabilités, est en mesure d'obtenir toutes les informations nécessaires pour accéder à des informations privilégiées.

Test d'Intrusion d'Application Internet

Test de la sécurité informatique sur les applications web

Avec l'avènement du commerce électronique, les entreprises utilisent toujours plus le web pour promouvoir et vendre leurs produits et/ou services. Le service Cyber Security d'INSIDE développe donc des activités de prévention et de sécurité sur toutes les applications internet dont disposent les entreprises.

L'intervention consiste en le balayage et la surveillance de toutes les sections de l'application internet, avec une attention particulière à celles protégées par un nom d'utilisateur et un mot de passe lesquels, dans l'éventualité d'un crack, permettraient l'accès aux services offerts par le biais des protocoles HTTP ou HTTPS.

L'intervention concerne les champs de sécurité suivants:

- Balayage des données sensibles envoyées par le biais de l'application, données exposées au risque d'interception par des personnes malveillantes, en examinant le code HTML, les scripts, ou les autres informations pouvant être obtenues à partir d'éventuels mécanismes de débogage;
- Analyse approfondie des champs interactifs entre l'application et l'utilisateur, de manière à identifier les éventuelles lacunes créées par des saisies (in) volontaires;
- Procédures d'authentification;
- Résolution de problèmes liés à une session spécifique, comme par exemple l'expiration du délai, la déconnexion, le détournement, la connexion par le biais d'adresses non vérifiées, etc...;
- Validation et altérabilité des données;
- L'exécution de commandes dans des zones inattendues de l'application, lesquelles peuvent, par exemple, par le biais de chaînes SQL spécifiques, conduire à la manipulation directe de la base de données, avec possibilité d'acquisition, modification et suppression des données y figurant;
- Interactions inappropriées ou incorrectes avec le système d'exploitation (shell escape).



Détection et Analyse des Menaces

Protégez votre entreprise contre tout dispositif matériel ou logiciel hostile (tel que les virus) pouvant endommager ou transmettre des données sensibles à l'extérieur par le biais de notre procédure de contrôle et de vérification. Contactez-nous dès maintenant pour bénéficier de conseils gratuits.

Identification du Piratage Informatique

La révolution numérique est en train de changer le monde du travail. De plus en plus souvent, les entreprises utilisent de nouvelles technologies comme le cloud, les technologies mobile, les données volumineuses ou l'IoT, ce qui les rend de plus en plus vulnérables aux cyberattaques. Il est donc essentiel de savoir si vos informations ont été manipulées ou sont surveillées d'une manière ou d'une autre. Les activités d'identification du piratage informatique menées par INSIDE AGENCY décèlent les traces d'une intrusion en recueillant correctement les éléments de preuves nécessaires pour documenter l'incident.

Contre-espionnage Informatique

INSIDE AGENCY détecte le degré de vulnérabilité des systèmes informatiques de ses clients et, après avoir effectué une analyse diagnostique minutieuse, identifie les interventions utiles à la sécurisation du parc informatique.

Afin de fournir le meilleur support possible, INSIDE AGENCY a réuni les meilleures compétences dans le domaine de la sécurité, en fournissant des services de conseil spécifiques pour l'exécution de chaque activité d'analyse, dans le but de protéger les actifs les plus importants ou le savoir-faire de l'entreprise.

Les manières dont les informations illégales peuvent être trouvées sont en constante expansion. La révolution numérique a favorisé la naissance de ce qu'on appelle l'espionnage informatique, qui touche les particuliers mais encore plus souvent les entreprises. Comment pouvons-nous nous protéger? Le mot d'ordre est la prévention.

En menant des enquêtes de contre-espionnage scrupuleuses, INSIDE AGENCY identifie et élimine le danger, détectant les actions d'espionnage possibles.



Délégué à la protection des données

Garantissez à votre entreprise la sécurité nécessaire pour éviter les risques associés à la violation des données personnelles.

Des professionnels hautement spécialisés et formés aux dernières réglementations pour vous fournir les conseils nécessaires en matière de protection des données

Délégué à la protection des données

Un délégué à la protection des données toujours disponible pour votre entreprise

Un expert toujours disponible pour votre entreprise capable de garantir la sécurité et la conformité ?

Notre service Délégué à la protection des données (DPD) vous permet de disposer d'un personnel professionnel, hautement spécialisé et formé aux dernières réglementations, toujours à votre disposition pour vous conseiller sur la formation et la mise à jour de vos employés, garantissant ainsi la sécurité nécessaire pour prévenir tout risque lié à une violation des données, ainsi que pour vous aider à respecter toutes les obligations imposées par la législation européenne et à évaluer tout changement dans les processus de production, susceptible d'avoir une incidence sur le respect des réglementations générales en matière de protection des données.

Qui est le délégué à la protection des données ?

Parmi les innovations introduites par le règlement général sur la protection des données n° 2016/679 (mieux connu sous le nom de RGPD), il y a la nomination d'un Délégué à la protection des données, mieux connu sous l'acronyme DPD.

Les autorités et organismes publics, à l'exception des autorités judiciaires chargées de l'exercice des fonctions juridictionnelles, ainsi que tous les sujets (organisations et entreprises) qui, dans le cadre de leurs activités principales, traitent à grande échelle des données sensibles relatives à la santé ou à la vie sexuelle, génétiques judiciaires et biométriques, ou qui exercent des activités dans lesquelles les traitements nécessitent le contrôle régulier et systématique des parties intéressées (par exemple, les opérateurs de télécommunications, les opérateurs qui établissent des profils à des fins de marketing comportemental, les activités de localisation via application, la surveillance de l'état d'intégrité via des dispositifs portables et interconnectés, appelés dispositifs portables, programmes de fidélisation, etc., sont incluses dans cette hypothèse) doit obligatoirement désigner un Délégué à la protection des données.

Le Délégué à la protection des données est la personne qui, au sein d'une entreprise, qu'elle soit publique ou privée, observe, évalue et réglemente la gestion du traitement des données à caractère personnel, en garantissant un traitement conforme à la législation européenne et nationale sur le respect de la vie privée.

Dans le nouvel ordre juridique, le Délégué à la protection des données constitue un élément fondamental puisqu'en agissant en tant qu'intermédiaire entre les différentes parties impliquées, il favorise la croissance et le développement concurrentiel entre entreprises, tout en assurant le plein respect des dispositions du RGPD.



Les tâches du Délégué à la protection des données

L'article 39 du règlement de l'UE 2016/679 fournit une liste non exhaustive des tâches confiées au DPD. En particulier, chaque DPD doit :

- « Informer et conseiller le responsable du traitement, ainsi que les employés qui effectuent le traitement, au regard des obligations découlant du règlement UE n° 2016/679 ainsi que d'autres dispositions de l'Union ou des États membres relatives à la protection des données;
- Contrôler le respect du règlement susmentionné, d'autres dispositions de l'Union ou des États membres relatives à la protection des données et des politiques du responsable du traitement en ce qui concerne la protection des données à caractère personnel, y compris l'attribution des responsabilités, sensibilisation et formation du personnel impliqué dans les traitements et les activités de contrôle connexes;
- donner, sur demande, un avis sur l'analyse d'impact sur la protection des données et contrôler sa performance conformément à l'art. 35;
- coopérer avec l'autorité de surveillance;
- servir de point de contact pour l'autorité de contrôle pour les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener, le cas échéant, des consultations sur toute autre question.

Dans l'exercice de ses fonctions, le Délégué à la protection des données prend dûment en compte les risques inhérents au traitement, en tenant compte de la nature, du champ d'application, du contexte et des finalités de celui-ci. »

Délégué à la protection des données Tâches et qualités professionnelles

Le règlement UE 2016/679 ne fournit pas de liste des qualités professionnelles que doit posséder chaque Délégué à la protection des données pour remplir cette fonction. Toutefois, une connaissance adéquate de la législation applicable et des pratiques nationales et européennes dans le domaine de la protection des données, ainsi qu'une mise à jour constante des questions connexes doivent être considérées comme pertinentes et nécessaires à l'accomplissement de sa tâche.

La maîtrise des compétences acquises dans le secteur et une bonne connaissance des traitements effectués ainsi que des systèmes d'information et des besoins de sécurité et de protection des données exprimés par le responsable sont également fondamentales.

INSIDE vous fournira le DPD idéal, un profil de haut niveau indépendant et autonome, une formation adéquate, une connaissance efficace et approfondie de la législation sur la protection de la vie privée et des pratiques opérationnelles.

La nomination d'un Délégué à la protection des données :

- n'est pas une simple formalité mais doit avoir lieu de manière concrète et efficace ;
- doit être adaptée au contexte juridique et organisationnel de l'entreprise ;
- doit concerner un sujet indépendant et autonome qui, au sein de la même entreprise, n'aura donc pas à remplir d'autres rôles ;
- doit garantir la protection de la sécurité de l'entreprise.



RGPD - Sanctions

Le règlement général sur la protection des données introduit des **pénalités et des amendes**.

Afin de déterminer la sanction à appliquer, une série de facteurs seront pris en compte, tels que la gravité, la **durée de la violation**, le nombre de parties intéressées, le niveau du préjudice subi, le caractère intentionnel de l'infraction, **toutes les actions entreprises atténuer les dommages** et le degré de coopération avec l'autorité de surveillance.

Si les règles ne sont pas respectées, le règlement identifie deux plafonds d'amende.

La première limite prévoit des amendes d'un maximum de **10 millions d'euros** ou, dans le cas d'un engagement, de 2 % du chiffre d'affaires mondial annuel.

Cette première catégorie d'amende serait appliquée par les responsables du traitement dans le cas d'analyses d'impact, comme le prévoit le règlement.

Le montant maximal des amendes atteint **20 millions d'euros**, soit 4 % du chiffre d'affaires annuel mondial.



PASSWORD MAC SCRIPT
LINUX ZERO DAY
ANDROID OS
WINDOWS OS
CYBERCRIME
SECURITY AUDIT
CYBER HACKER
OWASP
BACKUP COMPUTER HACKING
FORENSICS SECURITY
GDPR EVALUATION
PATCH & UPDATES
WEB APPLICATION
PENETRATION TEST
MALWARE SECURITY CONSULTING
VIRUS
RANSOMWARE
SECURITY AUDIT
ETHICAL HACKING
TEST PHISHING
PRIVACY
NETWORK ANALYSIS
PENETRATION TEST VAM
SECURITY
VULNERABILITY ASSESSMENT
SOCIAL ENGINEERING
RISK MANAGEMENT
CODE
CHF

**Les premières informations pour
la défense de votre entreprise**

Exemples de cyberattaques

Mauvais usage des actifs et des outils de l'entreprise

La société stocke toutes ses données dans iCloud. Un pirate informatique peut accéder à un **ransomware** et l'utiliser pour chiffrer toutes les données stockées. À ce stade, l'accès à la société n'est plus autorisé et **la production s'arrête**.



Attaque des systèmes de contrôle Operation Technology (OT)

Au moyen d'un courriel frauduleux, un pirate informatique récupère les données utilisateur de certains employés d'une entreprise hautement numérisée (appelée **phishing** ou hameçonnage). De cette manière, le pirate informatique entre dans le réseau de connexion de l'entreprise en manipulant certains paramètres de production. La manipulation ne sera pas détectée immédiatement, ce qui entraînera **une production de produits défectueux**.



Falsification du système informatique

Un pirate informatique pénètre dans le système d'information d'une entreprise (**phreaking**) et le manipule pour exploiter à son avantage les ressources de l'entreprise (par exemple, espace d'hébergement, bande passante, électricité, adresses IP, etc.). À la fin du mois, on retrouve **des milliers d'euros de charges**.



Vol de données confidentielles

Un professionnel stocke des données sur ses clients sur son serveur. Bien que des mesures de sécurité adéquates aient été prises, un pirate informatique, utilisant un courriel manipulé, installe un **cheval de Troie** dans le système. Comme le malware n'est détecté que plus tard, le pirate informatique aura le temps de **copier les informations confidentielles des clients**.



Interruption des ventes en ligne

À la suite d'une **attaque par déni de service** dirigée contre le canal de vente en ligne d'un détaillant d'accessoires pour femme, les clients ne peuvent plus accéder au site Internet dédié. Il faut environ 15 jours pour faire face à l'attaque. Les **ventes en ligne sont interrompues**.



Les dernières tendances

Malware sans macro

Les cybercriminels exploitent des documents Office malveillants pour tromper leurs victimes. Les attaques **DDE (Dynamic Data Exchange)** ont figuré au quatrième trimestre dans la liste des dix principaux programmes malveillants : les pirates ont de plus en plus exploité les problèmes de cette norme **Microsoft Office** pour exécuter du code. Également appelés « **macro-less malware** », ces documents malveillants utilisent souvent PowerShell et des scripts flous pour contourner les défenses du réseau. En outre, deux des dix principales attaques de réseau du T4 ont impliqué des exploitations de Microsoft Office, soulignant encore la tendance croissante aux attaques malveillantes sur les documents.

Zero Day

Le nombre total d'attaques de logiciels malveillants a considérablement augmenté, tandis que les variantes de **malware zero-day** ont augmenté de 167 % en 2017. Près de la moitié des logiciels malveillants ont échappé aux solutions antivirus de base. Cette croissance suggère que les criminels utilisent des techniques d'évasion sophistiquées capables de faire passer les attaques au-delà des services antivirus traditionnels, ce qui souligne encore davantage l'importance des défenses basées sur le comportement.

Script

Les attaques basées sur des scripts détectées par des signatures pour les menaces JavaScript et Visual Basic Script, telles que les **téléchargeurs** et les **droppers**, représentaient la majorité des programmes malveillants l'année dernière. Les utilisateurs doivent reconnaître la popularité de ces attaques et prêter une attention particulière aux scripts malveillants des pages Internet et aux pièces jointes des e-mails de tous types.



Liste de contrôle de cybersécurité

- ✓ Nommer un **responsable informatique**
- ✓ Gérer les niveaux d'autorisation pour fournir ou limiter les **droits d'accès**
- ✓ Gérer les **mots de passe**
- ✓ Préparer un **plan de défense** contre les attaques DoS et DDoS
- ✓ Former et sensibiliser à l'adoption de **mesures de sécurité adéquates**
- ✓ Effectuer **des sauvegardes quotidiennes** en stockant les données en toute sécurité
- ✓ Créer et stocker des **copies de sécurité** du logiciel utilisé dans les processus de production dans des emplacements sécurisés
- ✓ Identifier **les mesures de sécurité techniques** à adopter (par exemple, IPS et/ou IDS, pare-feu, filtres anti-virus, anti-spam, etc.)
- ✓ Identifier **les mesures de sécurité physiques** à adopter (par exemple, accès physique aux serveurs surveillés)
- ✓ Effectuer des contrôles appropriés par des **tests spécifiques anti-malware**
- ✓ Installer des **correctifs et des mises à jour** régulièrement
- ✓ **Protéger les données sensibles** en utilisant le cryptage
- ✓ Effectuer périodiquement **des contrôles de sécurité** sur l'infrastructure informatique, les sites Internet et les applications pour appareils mobiles (**VAM, VAPT, WAPT**)



Certifications



OWASP

Le Guide de test OWASP est une structure permettant de **tester la sécurité des applications et des infrastructures réseau**.



OSSTMM

Le Guide de test OWASP est une structure permettant de **tester la sécurité des applications et des infrastructures réseau**.



eCPPT

L'eCPPT (Elearn Security Certified Penetration Tester Professional) **est la seule certification pratique disponible sur le marché pour évaluer la sécurité des infrastructures informatiques**.



eWPT

EWPT (ELearn Security Web Penetration Tester) **est la seule certification pratique disponible sur le marché pour évaluer la sécurité des applications Internet**.



CERTIFIED ETHICAL HACKING

Le Certified Ethical Hacker est un **professionnel qui comprend et sait identifier les faiblesses et les vulnérabilités des systèmes** et utilise les mêmes connaissances et outils qu'un **Black Hacker**.



COMPUTER HACKING FORENSIC INVESTIGATOR

Le **Computer Hacking Forensic Investigator** certifie le professionnel en criminalistique numérique



Expertise Judiciaire Numérique et Mobile

Analysez le contenu de votre téléphone, ou récupérez vos données sur support numérique grâce aux meilleurs instruments professionnels disponibles.

Nous avons réuni les meilleures compétences dans le domaine de la sécurité au sein d'une ligne dédiée. Découvrez nos services de conseil en matière criminalistique en matière de médias numériques pour effacer ou récupérer des données sur des supports de stockage endommagés. Contactez-nous dès maintenant pour extraire les données de vos appareils.

Expertise Judiciaire des Réseaux

L'expertise judiciaire des réseaux consiste en la saisie, l'enregistrement et l'analyse des communications des réseaux afin d'obtenir des renseignements utiles pour les enquêtes techniques dans divers domaines juridiques.

Expertise Judiciaire des Bases de Données

Le service d'expertise judiciaire des bases de données analyse les bases de données en recherchant les données et les tableaux supprimés et/ou altérés, en reconstituant les événements qui ont causé des dommages et en identifiant l'activité criminelle et les causes qui ont donné lieu à l'accident informatique.

Expertise Judiciaire Informatique

L'informatique judiciaire, particulièrement utilisée dans le domaine de la criminalité informatique, est une branche de la criminalistique numérique liée aux éléments de preuve obtenus à partir d'ordinateurs et d'autres dispositifs de stockage numérique. Cette activité a pour but d'analyser des dispositifs numériques par le biais d'analyses judiciaires visant à identifier, stocker, récupérer, étudier et présenter des faits ou des opinions sur les informations recueillies.

L'équipe d'INSIDE AGENCY mène des enquêtes approfondies d'expertise judiciaire des ordinateurs dans le but de recueillir et d'analyser des preuves valides à des fins juridiques en matière civile, commerciale, pénale et fiscale. Suite à leur intervention, les experts rédigent un rapport d'expertise détaillé et peuvent également être présents en tant que témoins dans un procès éventuel.

Expertise Judiciaire Mobile

Les téléphones mobiles, les smartphones, les tablettes et d'autres appareils mobiles sont de plus en plus utilisés et contiennent beaucoup d'informations personnelles, telles que les mots de passe, les messages texte, les conversations, les courriels et bien plus encore.

L'équipe d'INSIDE AGENCY, grâce à son expertise en sécurité des TI et les technologie de pointe dont elle dispose, analyse les informations contenues dans les appareils mobiles afin d'identifier, de préserver, d'examiner et de documenter l'information numérique qui pourrait être d'une importance primordiale.



Bonifications environnementales et électroniques

Avez-vous des craintes concernant la confidentialité? Protégez vos données et vos projets d'affaires grâce à nos services d'assainissement électronique de bureaux et d'autres locaux.

Contactez-nous dès maintenant pour protéger la confidentialité des données relatives à de votre entreprise.

Services de Bonifications environnementale et électronique

Ce service, disponible aussi bien en Italie qu'à l'étranger, permet à toute personne soupçonnant d'être espionnée de protéger sa vie privée. Grâce à l'utilisation d'instruments numériques et analogiques hautement professionnels

Ce service, disponible aussi bien en Italie qu'à l'étranger, permet à toute personne soupçonnant d'être espionnée de **protéger sa vie privée**.

Grâce à l'utilisation d'instruments numériques et analogiques hautement professionnels, Inside Agency réussit à assainir les bureaux et d'autres locaux en très peu de temps.

Des techniciens internes, dûment formés et qualifiés, effectuent une première inspection préliminaire, en procédant immédiatement à l'assainissement proprement dit. Enfin, ils rédigent un rapport sur l'ensemble des activités réalisées.

À la demande du client, les techniciens du Service d'assainissement électronique sont en mesure d'appliquer **les scellés de sécurité** sur les faux plafonds, les boîtes de jonction, les planchers surélevés, etc.

Le Service d'assainissement électronique est en mesure de mener les actions suivantes :

- logiciel espion; pour surveiller les activités effectuées sur PC, et logiciel de telephone espion, pour surveiller les activités des telephones portables;
- mouchards audio/vidéo, faciles à dissimuler n'importe où
- microphone laser, permet l'écoute à distance, avec détection des vibrations sonores à travers le verre
- micro-enregistreur audio numérique, dissimulable partout, également à l'intérieur d'un véhicule
- détecteur GPS, une fois installé à l'intérieur ou à l'extérieur d'un véhicule, il permet de détecter la position instantanée du véhicule et de retracer le chemin parcouru et les différents arrêts
- détecteur GPS et mouchard audio, pour la localisation satellite et la transmission des conversations ayant lieu à l'intérieur du véhicule
- écoute téléphonique
- enregistreurs audio/vidéo, dissimilables sur notre interlocuteur



Sécurité

Sécurité maritime, sécurité des conducteurs, services de protection des personnes et bien plus encore: nous garantissons la sécurité des personnes, des ressources et des infrastructures.

Nous mettons à votre disposition les moyens les plus appropriés pour prévenir les risques potentiels encourus par une entreprise ou ses salariés en identifiant et en gérant les situations de crise. Découvrez tous nos services de sécurité, dont chacun répond à un besoin spécifique.

Security Manager

Le responsable de la sécurité soutient directement l'entreprise par l'étude, le développement et la mise en œuvre de stratégies et de plans opérationnels, afin de prévenir et de faire face aux situations qui peuvent nuire à l'entreprise.

La Direction sécurité d'Inside Agency met à la disposition de ses clients l'expertise de spécialistes et de professionnels de la sécurité certifiés afin de gérer les aspects techniques, organisationnels, économiques et humains qui relèvent de sa compétence.

Les principales fonctions du responsable de la sécurité sont les suivantes :

- la protection et la sauvegarde des structures d'entreprise ;
- la gestion et la protection du personnel ;
- la formalisation des processus internes de sécurité de l'entreprise ;
- la défense de l'image et de la réputation de l'entreprise ;
- la résolution de litiges ;
- l'évaluation de la fiabilité des opportunités commerciales ;
- la définition des stratégies de maîtrise des coûts ;
- l'organisation d'événements et de réunions d'entreprise ;
- la réalisation des certifications professionnelles requises par la zone d'opérations ;
- l'établissement de relations avec les organismes institutionnels et/ou politiques pour la gestion des affaires particulièrement délicates ;
- la protection des réseaux informatiques, archives informatiques et/ou papier ainsi que de tout autre document et/ou informations confidentielles ;
- la prévention de cyber-attaques pouvant nuire au savoir-faire de l'entreprise.



Sécurité Maritime

Sécurité maritime et services de lutte contre le piratage dans des zones à haut risque

La **Division Sécurité d'INSIDE** prévient le risque d'attaques, d'enlèvements ou de détournement de **cargos ou de passagers** en mettant en place des mesures de défense, notamment dans les zones considérées à haut risque, telles que les eaux somaliennes.

Le service est garanti par l'équipe de sécurité, les outils et les technologies dissuasives, la formation des équipages, et en conformité avec les normes de l'industrie:

- Code ISPS (Code international pour la sûreté des navires et des installations portuaires)
- Règlement SOLAS (Safety of life at Sea)
- Convention des Nations unies sur le droit de la mer de 1982
- Règlement international sur les drapeaux et les ports
- Conventions et accords de l'Organisation Maritime Internationale (OMI)

Conseil Stratégique pour la Sécurité

Chez INSIDE, la Division Sécurité fournit des **services personnalisés** (sur les objectifs d'affaires ou pour la prévention des risques) **pour la sécurité des biens et des ressources impliqués dans les processus d'affaires**, permettant ainsi aux entreprises d'adopter la bonne stratégie de contrôle des risques: une gestion efficace de la sécurité des actifs informationnels contribue considérablement à la conduite sûre des activités productives et à la réussite de l'entreprise.

L'activité de conseil stratégique pour la sécurité permet de connaître et d'évaluer le niveau de conformité par rapport au cadre réglementaire; **d'analyser et de gérer les risques de sécurité** physique, logique, organisationnelle et de continuité des activités; d'améliorer les processus de **sécurité de l'information**.

Évaluation des risques

Elle permet de déterminer les risques, sur le plan quantitatif et qualitatif, en termes de probabilités, dérivant des sources potentielles de danger, grâce à une cartographie de votre dispositif de sécurité (défini comme un ensemble de technologies, d'hommes, de processus et d'infrastructures utilisés pour la sécurité), avec une évaluation de chaque zone analysée et une analyse de l'écart entre le dispositif souhaité et le dispositif attendu, c'est-à-dire **l'analyse de la menace (threat analysis)**, il est possible de mesurer l'écart entre le dispositif en vigueur et le dispositif nécessaire pour répondre à la menace avec des suggestions adaptées pour atténuer ou transférer le risque.

Le tout en calibrant toujours efficacité, efficacité et durabilité et en conformité avec la norme ISO/IEC 27002 en matière de sécurité de l'information.

Rapport sur les Risques par Pays

Évaluation du risque de non-paiement de la part de sociétés étrangères

Le service vise à évaluer le risque de non-paiement par les entreprises d'un pays donné, puis d'aider le client à prendre des décisions informées dans le cadre de ses **activités commerciales internationales**, dans le but de l'accompagner dans sa stratégie de **croissance internationale**.

La méthodologie adoptée par la **Division Sécurité de la société INSIDE** consiste à analyser de nombreux indicateurs économiques, quantitatifs et qualitatifs afin de fournir un cadre exhaustif sur la situation économique, l'environnement politique et économique des affaires, les risques commerciaux et financiers potentiels.



Protection des Personnalités

Services de protection contre la violence ou les attaques contre les personnes

Le service assure la **protection des personnes considérées comme exposées à des attentats ou à des violences**, et éventuellement de leurs familles respectives. Ils sont assistés pendant leurs déplacements ou dans l'exercice de leurs activités professionnelles, tout en préservant leur vie privée.

Le **plan de protection** est adapté aux besoins du client et à la gravité du risque auquel il est potentiellement exposé. Sa défense est assurée à tout moment, lors de ses déplacements sur le territoire national et dans le monde, sur les voies terrestres, aériennes et maritimes, ainsi que sur son lieu de travail et son domicile.

À cette fin, le personnel de la **division sécurité de la société INSIDE** répond à des exigences très strictes d'un point de vue psycho-physique et se soumet à un entraînement physique continu. Il se tient informé des nouveautés juridiques et réglementaires, de l'évolution des techniques et de l'approche psychologico-sociale dans son domaine.

Chauffeur Sécurité

Des professionnels hautement qualifiés pour la protection individuelle

La **Division Sécurité de la société INSIDE** propose des **services de chauffeurs**, en toute confidentialité, discrétion et avec le plus grand professionnalisme. Ce service répond à tous les besoins (missions de longue durée, événements uniques, déplacements sécurisés de dirigeants, d'hommes politiques, etc.): voyages, transferts de/vers les aéroports, à l'occasion de congrès, de salons, transferts (et protection) de personnalités ayant besoin de transporter des objets personnels de valeur.

Le personnel est hautement qualifié, grâce à une formation constante et périodique sur la **conduite sécuritaire**.

Sécurité des voyages

Organisez des voyages d'affaires en toute sérénité, même dans les pays les plus dangereux

Notre service vous permet de connaître et de prendre en considération les particularités d'un pays, sa situation politique, sociale et géologique, le niveau de criminalité et les problèmes de santé.

Service de Sécurité de Voyage

Le service vous permet de voyager en toute tranquillité même dans les zones à haut risque.

Nous pouvons :

- nous assurer que le client connaît et de prendre en considération les particularités d'un pays, sa situation politique, sociale et géologique, le niveau de criminalité et les problèmes de santé.
- aider le client dans la planification de ses déplacements



www.inside.agency
info@inside.agency

Numéro sans frais international
+800 9001 9001



ENTREPRISE CERTIFIÉE
ISO 9001:2015

BUREAU PRINCIPAL

SUISSE

Via Maggio, 1/C
6900 Lugano
T +41 (0)91 260 16 42
F +41 (0)91 228 03 95

BUREAUX DANS LE MONDE

ROYAUME-UNI

Crown House, 72 Hammersmith Rd
Hammersmith, London, W14 8TH
T +44 (0)20 75 59 13 11
F +44 (0)20 35 14 68 50

ITALIE

Via Monte di Pietà, 21
20121 Milano
T +39 (0)2 86 33 73 42
F +39 (0)2 94 75 26 15

HONG KONG

25 Westlands Road, Quarry Bay Berkshire
House, Unit 2402-07, 24th HONG KONG
T +852 (0)28 24 85 09
F +852 (0)37 19 81 11

USA

6800 Jericho Turnpike, Suite 120W
Syosset, New York, 11791
T +1 (0)516 393 58 52
F +1 (0)516 393 58 19

ITALIE

Via Ludovisi, 35
00187 Roma
T +39 (0)6 42 03 73 97
F +39 (0)6 94 80 17 11

AFRIQUE DU SUD

First Floor, Willowbridge Centre, 39
Carl Cronje Dr, Cape Town, 7530
T +27 (0)21 974 6276
F +27 (0)21 974 6101

RUSSIE

31st floor, stroenie 1, bld. 3,
Begovaya str, Moscow, 125284
T +7 (0)499 277 13 03
F +7 (0)499 287 66 00

EMIRATS ARABES UNIS

Building 3, Plot 598-676, Dubai Investment
Park, Green Community, DUBAI, 212880, EAU
T +971 (0)4 31 32 564
F +971 (0)4 80 19 101

BRÉSIL

Top Center Paulista, Paulista Avenue, 854
Bela Vista – 10^e floor, São Paulo, 01310-913, Brasile
T +55 (0)11 21 86 04 42
F +55 (0)11 21 86 02 99