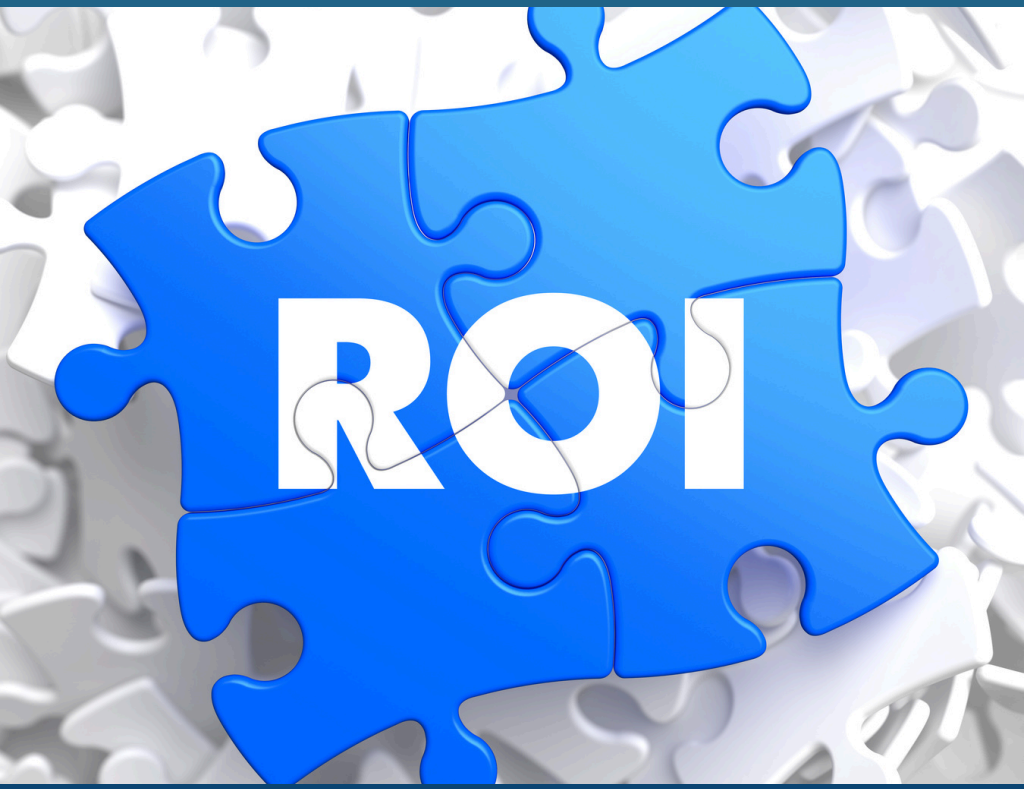
Numero 7 - luglio 2025

PROTEGGERE IL KNOW-HOW

STRATEGIE DI COUNTERINTELLIGENCE PER IL MONDO AZIENDALE



MIRKO LAPI

INDICE

Mirko Lapi è Consulente e Formatore specializzato in Open Source Intelligence (OSINT), sicurezza delle informazioni e sviluppo del pensiero critico applicato ai processi decisionali. Ha prestato servizio nelle Forze Armate italiane per 27 anni, di cui 16 anni all'interno del II Reparto Informazioni e Sicurezza dello Stato Maggiore della Difesa, dove ha lavorato come analista presso il Centro Intelligence Interforze dello Stato Maggiore della Difesa e come docente di Intelligence presso il Centro Interforze di Formazione Intelligence (CIFIGE). È Professore a contratto di Open Source Intelligence (OSINT) presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Foggia. Inoltre, ricopre il ruolo di Professore a contratto di Cyber Security per il Corso di Laurea Magistrale in Ingegneria dei Sistemi Intelligenti presso la Facoltà di Ingegneria, Università Campus Bio-Medico di Roma.

Contatti
email: corsi@proteggimi.com
tel: +390656556406 - +393714567087

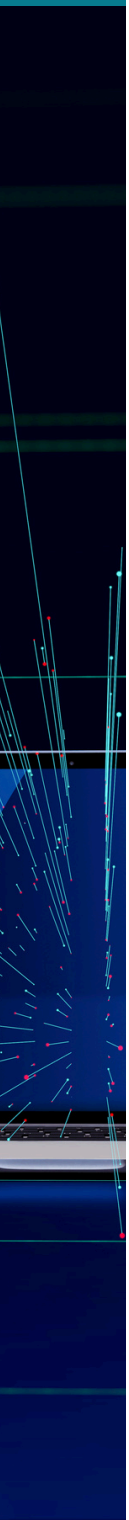
EXECUTIVE SUMMARY

Nell'economia della conoscenza, il vantaggio competitivo di un'organizzazione risiede sempre più nei suoi asset intangibili: know-how, segreti commerciali e proprietà intellettuale. Questi asset possono essere bersaglio di minacce sofisticate e pervasive, che vanno dallo spionaggio industriale orchestrato da concorrenti e attori statali, ai rischi interni e agli attacchi informatici mirati. La perdita di questo patrimonio non si traduce solo in un danno economico, ma può determinare l'erosione di una posizione di mercato e anche vanificare anni di investimenti.
In questo white paper voglio quindi delineare un approccio strategico e proattivo alla protezione degli asset informativi, basato sui principi della Counterintelligence aziendale (di seguito CI). Nello specifico quello che voglio proporre è un framework olistico che va oltre la sicurezza tradizionale, integrando misure difensive, una profonda comprensione dell'elemento umano e un utilizzo più consapevole dei dati interni ed esterni per generare intelligence.

Vengono quindi presentati quattro pilastri fondamentali:

1. **Misure di sicurezza fondamentali:** L'implementazione delle "misure ragionevoli" (legali, tecniche, fisiche e procedurali) necessarie non solo per la protezione pratica, ma anche per la tutela legale dei segreti commerciali.
2. **L'elemento umano:** La gestione del rischio *insider* e la creazione di una cultura della sicurezza resiliente, capace di riconoscere e resistere a tattiche di manipolazione come il social engineering.
3. **Intelligence-Driven Defense (Interna):** Un approccio innovativo che trasforma la documentazione di compliance (es. GDPR, DUVRI) in una fonte di intelligence per identificare vulnerabilità e flussi di dati critici interni.
4. **Intelligence-Driven Defense (Esterna)**: L'integrazione dell'Open Source Intelligence (OSINT) per comprendere proattivamente il panorama delle minacce esterne, analizzare la propria superficie d'attacco e soddisfare requisiti normativi emergenti, come il controllo sulla Threat Intelligence della norma ISO/IEC 27001:2022.

L'obiettivo è fornire ai leader aziendali una roadmap per sviluppare un programma di CI integrato, capace non solo di prevenire perdite, ma di agire come un abilitatore strategico, salvaguardando il valore e promuovendo una resilienza organizzativa duratura.



IL NUOVO CAMPO DI BATTAGLIA AZIENDALE

Nell'economia digitale contemporanea, il valore delle aziende risiede sempre più negli asset intangibili piuttosto che in quelli fisici. Il know-how, i dati, la proprietà intellettuale e le informazioni riservate rappresentano il cuore pulsante dell'innovazione e del vantaggio competitivo. Il know-how specifico di un'organizzazione, quell'insieme di conoscenze pratiche, processi, formule e dati non brevettati ma gelosamente custoditi, permette di distinguersi sul mercato, ottimizzare le operazioni e sviluppare prodotti o servizi unici. La sua protezione non è semplicemente una questione tecnica o legale, ma un imperativo strategico fondamentale per la sopravvivenza e il successo a lungo termine.

La perdita di questo patrimonio informativo, spesso accumulato con anni di investimenti in ricerca, sviluppo ed esperienza, può avere conseguenze devastanti. Non si tratta solo di una perdita economica diretta, ma della potenziale cessione involontaria di un vantaggio competitivo faticosamente costruito, mettendo a repentaglio la posizione di mercato dell'azienda.

In un mondo sempre più interconnesso e caratterizzato da un'agguerrita competizione globale, le minacce a questi asset intangibili sono diventate sempre più sofisticate e pervasive, spaziando dallo spionaggio industriale orchestrato da concorrenti o attori statali, ai rischi interni derivanti da dipendenti infedeli o negligenti, fino agli attacchi informatici mirati.
Il passaggio da un'economia basata prevalentemente su beni materiali a una fondata sulla conoscenza impone quindi un cambiamento radicale nell'approccio alla sicurezza. I modelli tradizionali, focalizzati sulla protezione perimetrale fisica, risultano inadeguati a fronteggiare minacce che mirano all'esfiltrazione di dati e conoscenze. A tal riguardo è necessario distinguere nettamente tra le attività legittime di Competitive Intelligence, che si basano sulla raccolta etica di informazioni pubbliche, e lo spionaggio aziendale, che impiega mezzi illegali per ottenere informazioni riservate.
Mentre la Competitive Intelligence è una pratica di business essenziale, lo spionaggio espone l'azienda a gravi rischi legali, finanziari e reputazionali. Comprendere questo confine è il primo passo per costruire difese efficaci

e garantire che le proprie attività rimangano entro i limiti della legalità.

Il panorama delle minacce e l'alto costo dell'inazione

La protezione del know-how aziendale richiede la consapevolezza dei diversi attori che possono tentare di appropriarsene illecitamente. Le minacce provengono da molteplici fonti, ognuna con motivazioni e metodi specifici:

- Concorrenti: Sono tra gli attori più ovvi. Le aziende possono spiare i loro rivali per ottenere vantaggi competitivi, accelerare la ricerca e sviluppo, comprendere le strategie di mercato, acquisire elenchi di clienti o rubare proprietà intellettuale.
- Insider (minacce interne): Rappresentano uno dei rischi più significativi e difficili da contrastare. Possono essere dipendenti scontenti, corrotti, negligenti o ex dipendenti che portano con sé conoscenze riservate. Il loro pericolo principale risiede nel fatto che operano legittimamente all'interno dei perimetri di sicurezza e dispongono di accessi autorizzati,

rendendo le loro attività malevole difficili da distinguere dalle normali operazioni quotidiane.

- Entità di Intelligence straniere: Servizi segreti governativi o organizzazioni collegate che mirano ad acquisire tecnologie avanzate, segreti industriali o informazioni economiche sensibili per rafforzare la propria economia o capacità militare/intelligence, utilizzando metodi sofisticati come attacchi informatici persistenti (APT) e operazioni di *Human Intelligence*.
- Attori cibernetici: Gruppi criminali organizzati, hacktivisti o singoli hacker malintenzionati che colpiscono per profitto, estorsione (*ransomware*) o danno reputazionale, utilizzando tecniche di hacking, malware e phishing.

La sottrazione di know-how infligge danni profondi e multidimensionali. Gli impatti finanziari includono la perdita di vantaggio competitivo, la vanificazione degli investimenti in R&S, i costi legali e di *remediation* e non ultime implicazioni normative e multe (es. GDPR).

Gli impatti reputazionali si manifestano nella perdita di fiducia di clienti, partner e investitori, danneggiando il brand a lungo termine. Infine, gli impatti strategici possono portare al fallimento di progetti, all'interruzione delle operazioni e, in settori critici, a rischi per la sicurezza nazionale.

La natura spesso ritardata e difficilmente quantificabile di questi danni rende la protezione del know-how un investimento strategico essenziale, non un semplice costo operativo.

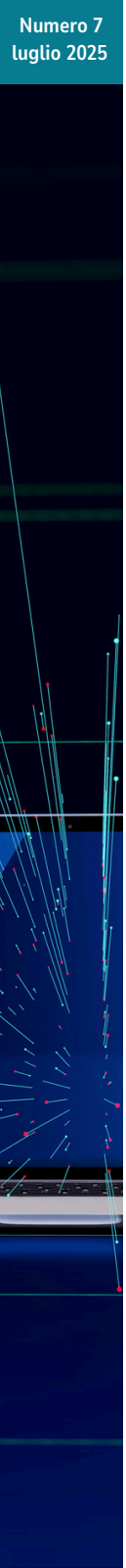
La soluzione: Un framework di aziendale

Per contrastare efficacemente queste minacce, le aziende devono adottare un approccio proattivo e strutturato: la CI aziendale. Tale attività si definisce come l'insieme delle informazioni raccolte e delle attività condotte per identificare, valutare, neutralizzare e, in alcuni casi, sfruttare le attività di intelligence ostili che mirano ai segreti aziendali.

A differenza della sicurezza tradizionale, la Counteintelligence è focalizzata sull'avversario: non si limita a costruire difese, ma cerca attivamente di comprendere e interferire con i suoi sforzi di spionaggio.
Un programma CI si articola in due componenti principali:

- **CI difensiva (negazione):** Rappresenta la base della protezione e mira a impedire agli avversari di raccogliere informazioni. Include la sicurezza fisica, del personale, delle informazioni (INFOSEC) e delle comunicazioni (COMSEC), implementando controlli come la gestione degli accessi, la crittografia e la classificazione dei dati.
- **CI offensiva (inganno e neutralizzazione):** Adotta un approccio proattivo per comprendere, interferire e manipolare le operazioni avversarie. Nel contesto aziendale, questo si traduce in una profonda comprensione della minaccia, nel testing proattivo delle difese e, con le dovute cautele legali, nell'uso di tattiche di inganno (deception) come la creazione di honeypot digitali (sistemi-esca per depistare gli

attaccanti) o il rilascio controllato di informazioni fuorvianti per depistare gli avversari. L'adozione di una mentalità CI, basata su vigilanza costante, proattività e consapevolezza situazionale, è fondamentale per trasformare la sicurezza da una funzione reattiva a una responsabilità strategica condivisa.



PILASTRO 1: IMPLEMENTARE LE MISURE DI SICUREZZA FONDAMENTALI

Affinché un'informazione possa essere protetta legalmente come segreto commerciale, il suo detentore deve dimostrare di aver adottato "misure ragionevoli" per mantenerla segreta. Queste misure costituiscono il fondamento di qualsiasi programma di protezione.

Il Framework ISO/IEC 27001: Un approccio strutturato

Per tradurre in pratica l'implementazione delle "misure ragionevoli", le organizzazioni possono fare riferimento allo standard internazionale ISO/IEC 27001. Questa norma definisce i requisiti per stabilire, implementare, mantenere e migliorare continuamente un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS in inglese). L'obiettivo di un SGSI è proteggere la riservatezza, l'integrità e la disponibilità delle informazioni attraverso un approccio sistematico e basato sulla valutazione del rischio.

L'**Annex A** della norma fornisce un catalogo completo di controlli di sicurezza, raggruppati in quattro aree tematiche (Controlli organizzativi, sulle persone, fisici e tecnologici), che rappresentano un insieme di *best practice* riconosciute a livello globale. Questi controlli, che spaziano dalla gestione degli accessi alla sicurezza delle risorse umane, dalla sicurezza fisica alla gestione degli incidenti, forniscono una roadmap concreta per implementare le in questo white paper. Adottare un SGSI conforme alla ISO 27001, e idealmente certificarlo tramite un ente terzo indipendente, costituisce una solida prova dell'impegno dell'organizzazione e della sua diligenza nel proteggere il proprio patrimonio informativo, fornendo una base difendibile in caso di contenzioso e facilitando la conformità con altre normative come il GDPR.

Misure legali, tecniche, organizzative e fisiche

Oltre al framework fornito dalla ISO 27001, le misure chiave includono:

- Misure legali e contrattuali: L'uso sistematico di accordi di riservatezza (NDA) con dipendenti, partner e

fornitori è essenziale. I contratti di lavoro devono includere clausole specifiche di riservatezza e di assegnazione della proprietà intellettuale. Questi strumenti legali, supportati da leggi nazionali e internazionali come l'Economic Espionage Act (USA) o la Direttiva UE sui segreti commerciali, forniscono un deterrente iniziale e la relativa base per azioni legali.

- Misure tecniche (INFOSEC): La spina dorsale della protezione digitale si basa su tre elementi chiave. 1)Il controllo degli accessi, governato dal principio del minimo privilegio, garantisce che gli utenti accedano solo alle informazioni strettamente necessarie. 2)La crittografia protegge i dati sia a riposo (su server e dischi) sia in transito (su reti), rendendoli illeggibili a chi non è autorizzato. 3)La sicurezza della rete, tramite firewall, sistemi di rilevamento delle intrusioni (IDS/IPS) e monitoraggio, protegge l'infrastruttura da attacchi esterni.
- Misure organizzative e procedurali: È fondamentale identificare e classificare gli asset informativi critici, creando un inventario del know-how da proteggere.

Devono essere definite policy chiare sulla gestione delle informazioni, supportate da procedure sicure di onboarding e offboarding del personale. Il principio del *Need-to-Know* deve essere applicato rigorosamente, limitando l'accesso alle informazioni sensibili solo a chi ne ha immediata necessità per un compito specifico, indipendentemente dal ruolo.

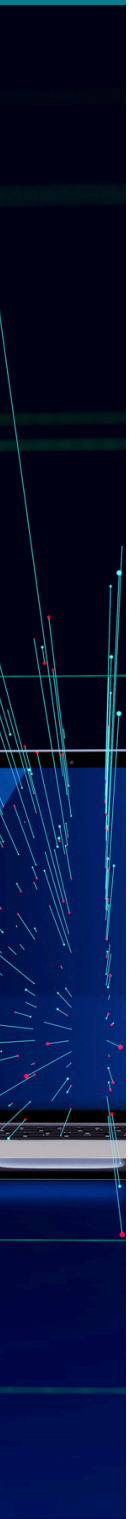
- Misure di sicurezza fisica: La protezione fisica di edifici, aree riservate (data center, laboratori) e documenti cartacei rimane essenziale. Controlli d'accesso, gestione dei visitatori e politiche come la "*Clean Desk*" prevengono il furto fisico e l'accesso non autorizzato che possono portare a compromissioni digitali.

Checklist delle misure di protezione ragionevoli

Categoria Misura	Misure specifiche	Priorità indicativa	Dipartimento Responsabile (Esempio)
Organizzativa / Procedurale	Definizione policy sicurezza (info handling, classificazione, uso IT)	Alta	Security / IT / Legal / HR
	Programma formazione e consapevolezza (rischi, policy, phishing, social engineering)	Alta	HR / Security / IT
	Implementazione classificazione dati e marcatura	Media	IT / Security / Business Units
	Applicazione principio - *to-Know* e minimo privilegio	Alta	IT / HR / Security / Manager
	Procedure sicure di onboarding (screening, accordi) e offboarding (revoca accessi, restituzione asset)	Alta	HR / IT / Security / Legal

Categoria Misura	Misure specifiche	Priorità indicativa	Dipartimento Responsabile (Esempio)
Legale / Contrattuale	Utilizzo Accordi di Riservatezza (NDA) con dipendenti e terze parti	Alta	Legal / HR / Procurement
	Clausole di riservatezza e assegnazione IP nei contratti di lavoro	Alta	Legal / HR
Tecnica / IT Security	Gestione identità e accessi, autenticazione forte (MFA)	Alta	IT Security
	Crittografia dati (at rest, in transit)	Alta	IT Security / IT Operations
	Sicurezza di rete (Firewall, IDS/IPS, segmentazione, monitoraggio)	Alta	IT Security / Network Operations
Fisica	Controllo accessi (edifici, aree riservate, aree Top Management)	Alta	Physical Security / Facilities
	Sicurezza durante viaggi ed eventi (protezione dispositivi, conversazioni)	Media	All Traveling Employees / Security

Torna all'indice



PILASTRO 2: L'ELEMENTO UMANO, LA PRIMA LINEA DI DIFESA

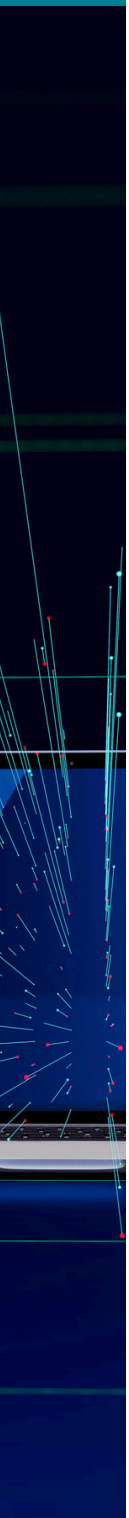
Le persone rappresentano spesso l'anello più debole della catena di sicurezza, ma anche la più grande opportunità di difesa. Un programma CI efficace deve porre un'enfasi centrale sull'elemento umano.

Gestire il rischio insider: Le minacce interne, siano esse malevole, negligenti o compromesse, sono particolarmente insidiose. È necessario comprendere le motivazioni (finanziarie, ideologiche, vendetta) e riconoscere i potenziali indicatori comportamentali (red flags), pur valutandoli con estrema cautela e nel rispetto della privacy. La mitigazione si basa su processi HR equi, controlli tecnici sugli accessi e, soprattutto, sulla promozione di una cultura di lealtà ed etica.

PRevenire il Social Engineering: Tattiche come il phishing, spear phishing e l'elicitazione (l'arte di estrarre informazioni tramite conversazioni apparentemente innocue) bypassano le difese tecniche per manipolare direttamente i dipendenti.

La difesa risiede nella consapevolezza e nel pensiero critico. I dipendenti devono essere formati a verificare le identità, a mettere in discussione richieste insolite e a segnalare attività sospette.

Costruire una cultura della sicurezza: La sicurezza deve diventare un valore condiviso e una responsabilità di tutti. Ciò si ottiene attraverso una formazione continua, coinvolgente e pertinente, che utilizzi simulazioni e role-playing per sviluppare competenze pratiche. La comunicazione efficace, il supporto visibile del top management e la creazione di canali di segnalazione sicuri e "no-blame" sono essenziali per trasformare la forza lavoro in una rete di sensori umani.



PILASTRO 3: INTELLIGENCE-DRIVEN DEFENSE - SFRUTTARE I DATI INTERNI

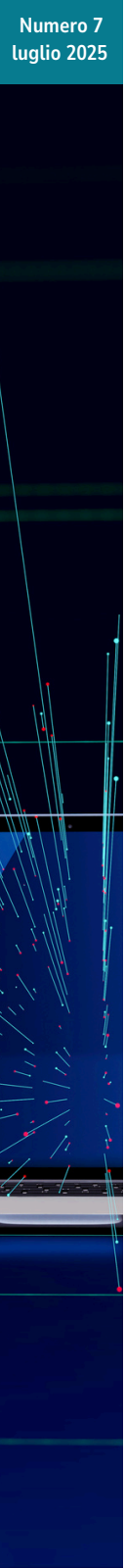
Un approccio innovativo e potente alla CI consiste nel trasformare la documentazione interna, spesso creata per obblighi di compliance, in una fonte di intelligence per la sicurezza. Questi dati a duplice uso offrono una visione senza precedenti dei rischi e delle vulnerabilità.

Dati di conformità GDPR: Documenti come i Registri delle attività di Trattamento (RoPA) e le Valutazioni d'Impatto sulla Protezione dei Dati (DPIA) mappano in dettaglio i flussi di dati sensibili, chi vi accede, dove sono conservati e quali controlli sono in atto.20 L'analisi di questi documenti rivela concentrazioni di rischio, accessi eccessivi e potenziali punti di esposizione per il know-how.

Analisi del DUVRI (Contesto Italiano): Il Documento Unico di Valutazione dei Rischi da Interferenze (esempio), pur essendo focalizzato sulla sicurezza sul lavoro, mappa con precisione le interazioni con fornitori e appaltatori esterni. La sua analisi permette di identificare quali terze parti operano

in aree critiche, a quali processi o informazioni potrebbero essere esposte e se i controlli su di esse sono adeguati, fornendo insight fondamentali sul rischio della *supply chain*.

Integrare sistematicamente i risultati di queste analisi nel framework di gestione del rischio aziendale (es. ESRM) permette di evitare duplicazioni, aumentare il ROI della compliance e ottenere una visione più profonda e accurata delle vulnerabilità operative, trasformando un obbligo normativo in un vantaggio strategico per la sicurezza.



PILASTRO 4: INTELLIGENCE-DRIVEN DEFENSE (ESTERNA) - IL RUOLO STRATEGICO DELL'OSINT

Se il pilastro precedente guarda all'interno, una difesa basata sull'intelligence deve necessariamente guardare anche all'esterno. L'Open Source Intelligence (OSINT) è la disciplina che si occupa della raccolta e dell'analisi di informazioni provenienti da fonti pubblicamente disponibili per produrre intelligence attuabile. L'integrazione dell'OSINT in un programma CI aziendale è fondamentale per comprendere il panorama delle minacce esterne e la propria esposizione.

OSINT e Threat Intelligence (Controllo ISO 27001 A.5.7)

L'importanza strategica dell'OSINT è stata formalmente riconosciuta anche nella versione 2022 della già citata ISO/IEC 27001, attraverso l'introduzione del controllo A.5.7 - Threat Intelligence. Questo controllo richiede esplicitamente alle organizzazioni di raccogliere e analizzare informazioni relative alle minacce alla sicurezza delle informazioni per produrre "threat

intelligence". L'obiettivo è trasformare dati grezzi su vulnerabilità, tattiche degli avversari o indicatori di malware in insight contestualizzati e attuabili per rafforzare le difese e guidare la gestione del rischio.
L'OSINT è una delle fonti primarie per alimentare questo processo. Attraverso il monitoraggio di fonti aperte, un'organizzazione può identificare proattivamente minacce emergenti, nuovi vettori di attacco e tendenze rilevanti per il proprio settore, soddisfacendo così i requisiti del controllo A.5.7 e implementando una difesa più informata e predittiva.

Applicazioni pratiche dell'OSINT nella sicurezza aziendale

L'OSINT ha molteplici applicazioni pratiche che vanno oltre la semplice conformità:

- Valutazione della superficie d'attacco esterna**:** L'OSINT permette di vedere la propria organizzazione come la vedrebbe un attaccante, identificando asset esposti su Internet, porte aperte, configurazioni cloud errate o credenziali e chiavi API accidentalmente pubblicate.

- Due Diligence e rischio terze parti: Prima di avviare partnership, fusioni o assunzioni chiave, l'OSINT consente di condurre valutazioni approfondite su aziende e individui, verificandone la reputazione, i precedenti e le potenziali connessioni rischiose.
- Competitive Intelligence: Sebbene distinta dallo spionaggio, l'analisi OSINT delle attività dei concorrenti (lanci di prodotti, assunzioni, comunicati stampa) può fornire preziosi insight strategici e di mercato, nel pieno rispetto della legalità.
- Monitoraggio delle minacce e rilevamento fughe di dati: L'OSINT è inoltre utile per monitorare il dark alla ricerca di menzioni dell'azienda, dei suoi domini o di dati potenzialmente esfiltrati, consentendo una reazione più rapida a una fuga di informazioni.

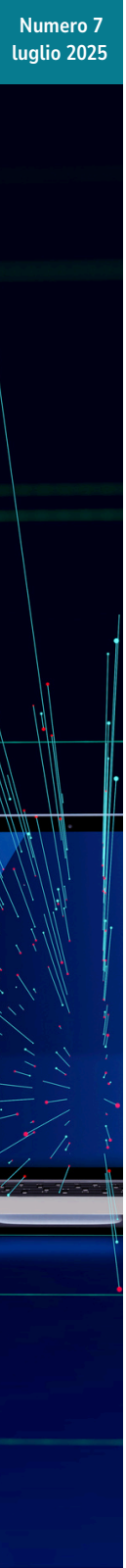
Il Processo OSINT: Strumenti e considerazioni etiche

Un'efficace attività OSINT segue un processo strutturato: definizione degli obiettivi, raccolta delle informazioni, elaborazione, analisi e diffusione dell'intelligence prodotta. La raccolta avviene da una vasta gamma di fonti, tra cui social media, notiziari, registri pubblici, siti web aziendali e database accademici.

Esistono numerosi strumenti, da semplici motori di ricerca con operatori avanzati ("Google Dorks") a piattaforme complesse, che aiutano ad automatizzare la raccolta e a visualizzare le connessioni tra i dati.

Tuttavia, come a più riprese ho evidenziato nei precedenti approfondimenti, è imperativo che tutte le attività OSINT siano condotte nel rigoroso rispetto dei quadri legali ed etici, in particolare delle leggi sulla privacy come il GDPR, evitando l'intrusione in dati personali senza un fondamento legittimo.

Torna all'indice



COSTRUIRE UN'ORGANIZZAZIONE RESILIENTE E SICURA

La protezione del know-how aziendale è una sfida strategica che richiede un impegno costante e un approccio olistico. L'implementazione di un programma di CI aziendale, integrato con la strategia di business e supportato dal vertice aziendale, è la chiave per affrontare questa sfida. Un programma CI aziendale maturo si basa su policy chiare, formazione continua, un piano di risposta agli incidenti ben testato e un ciclo di miglioramento continuo, come quello incarnato dal modello Plan-Do-Check-Act (PDCA), che è richiesto da standard come la ISO 27001. Tutto ciò si trasforma la sicurezza da un insieme di misure statiche a un processo dinamico e resiliente, capace di adattarsi a un panorama di minacce in continua evoluzione. In definitiva, proteggere il know-how non è compito di un singolo dipartimento, ma una responsabilità condivisa che deve permeare l'intera cultura organizzativa. Un programma di CI ben eseguito non solo previene perdite, ma contribuisce attivamente alla resilienza organizzativa.

Costruire una cultura etica, vigile e consapevole dei rischi è l'investimento più importante che un'azienda possa fare per salvaguardare i propri asset vitali. Un programma di CI ben eseguito non solo previene perdite, ma contribuisce attivamente alla resilienza organizzativa, garantendo la capacità di anticipare, resistere e prosperare di fronte alle avversità, assicurando così il successo e la competitività nel lungo periodo.

LINK DI APPROFONDIMENTO

Intellectual Property – Business Law: A Risk Management Approach
https://boisestate.pressbooks.pub/buslaw/chapter/intellectual-property/
Know-how protection 4.0 - Noerr
https://www.noerr.com/en/insights/a-whitepaper-know-how-schutz-40
Trade secret - Wikipedia
https://en.wikipedia.org/wiki/Trade_secret
Part III: Basics of trade secret protection - WIPO
https://www.wipo.int/web-publications/wipo-guide-to-trade-secrets-and-innovation/en/part-iii-basics-of-trade-secret-protection.html
Proprietary, Confidential Info, Trade Secrets, Know-How—Differences for Business Success
https://www.foxrothschild.com/publications/proprietary-confidential-info-trade-secrets-know-how-differences-for-business-success
Competitive Intelligence vs. Corporate Counterintelligence | Pragmatic Institute
https://www.pragmaticinstitute.com/resources/articles/product/keeping-your-secrets-responsible-counterintelligence-in-action/

LINK DI APPROFONDIMENTO

Wharton/ASIS Program for Security Executives: Making the Business Case for Security
https://executiveeducation.wharton.upenn.edu/for-individuals/all-programs/wharton-asis-program-for-security-executives/

How to Detect and Prevent Industrial or Corporate Espionage - Syteca
https://www.syteca.com/en/blog/prevent-industrial-espionage

Trade Secrets | Intellectual Property (IP) - Secretariat
https://secretariat-intl.com/services/intellectual-property/trade-secrets/

Trade Secrets Intellectual Property | PMI - Project Management Institute
https://www.pmi.org/learning/library/trade-secrets-intellectual-property-10443

Corporate Espionage: What You To Know - Splunk
https://www.splunk.com/en_us/blog/learn/corporate-espionage.html

Security: The -to-know principle | Microsoft Community Hub
https://techcommunity.microsoft.com/blog/azuresqlblog/security-the--to-know-principle/2112393

LINK DI APPROFONDIMENTO

Countering Foreign Intelligence Threats & Economic Espionage - USDA NIFA
https://www.nifa.usda.gov/sites/default/files/2023-12/Counterintelligence%20and%20Insider%20Threat%20Awareness.pdf

IP Risk Management – How to deal with it (part 1) - Intellectual Property Expert Group
https://www.ipeg.com/ip-risk-management-how-to-deal-with-it-part-1/

IP Risk Management: Infringement Risks, Mitigation Strategies - Counsel Stack Learn
https://blog.counselstack.com/ip-risk-management-infringement-risks-mitigation-strategies/

Counterintelligence - Wikipedia
https://en.wikipedia.org/wiki/Counterintelligence

A Guide to Counterintelligence - Grey Dynamics
https://greydynamics.com/a-guide-to-counterintelligence/

The 10 Commandments of Counterintelligenc
https://www.dni.gov/files/NCSC/documents/archives/10CommandmentsofCI_cind-2002-01-05.pdf

Implementing the -To-Know principle Redlings
https://www.redlings.com/en/guide/-to-know

LINK DI APPROFONDIMENTO

Security: The -to-know principle | Microsoft Community Hub
https://techcommunity.microsoft.com/blog/azuresqlblog/security-the-need-to-know-principle/2112393
IP Risk Management: Infringement Risks, Mitigation Strategies - Counsel Stack Learn
https://blog.counselstack.com/ip-risk-management-infringement-risks-mitigation-strategies/
Counterintelligence - Wikipedia
https://en.wikipedia.org/wiki/Counterintelligence
A Guide to Counterintelligence - Grey Dynamics
https://greydynamics.com/a-guide-to-counterintelligence/
The 10 Commandments of Counterintelligence
https://www.dni.gov/files/NCSC/documents/archives/10CommandmentsofCI_cind-2002-01-05.pdf
Implementing the Need-To-Know principle Redlings
https://www.redlings.com/en/guide/need-to-know

LINK DI APPROFONDIMENTO

Enterprise Security Solutions - ASIS International
https://www.asisonline.org/professional-development/enterprise-security-solutions/
Key Business Principles: A Comprehensive Guide
https://online.mason.wm.edu/blog/what-are-business-principles
Principles of data security | DataGuard
https://www.dataguard.com/blog/principles-of-data-security/
Intellectual Property Risk & How to Manage It | Fortra's Digital Guardian
https://www.digitalguardian.com/blog/intellectual-property-risk-how-manage-it
Corporate Security Is Curious about AI, But Is It Useful Yet? - ASIS International
https://www.asisonline.org/security-management-magazine/articles/2025/02/asis-research-security-trends/curious-about-ai/