OSINT E REGOLAMENTO DORA

Ogni giorno gli Istituti finanziari – e in particolare le banche – si confrontano con uno scenario caratterizzato da minacce informatiche in costante evoluzione. La crescente digitalizzazione dei servizi bancari e l'interconnessione con fornitori tecnologici espongono quindi il settore a rischi operativi e cyber senza precedenti. Per far fronte a queste sfide, l'Unione Europea ha introdotto il *Digital Operational Resilience Act* (DORA), ovvero il **Regolamento (UE) 2022/2554** sulla resilienza operativa digitale del settore finanziario. Entrato in vigore il 16 gennaio 2023 e applicabile a partire dal 17 gennaio 2025, il DORA definisce un quadro normativo vincolante e armonizzato che impone standard rigorosi per la gestione del rischio ICT, la continuità operativa e la segnalazione degli incidenti nei servizi finanziari. L'obiettivo è assicurare che banche, assicurazioni e altre entità finanziarie europee siano in grado di assorbire e gestire efficacemente anche gravi disruption operative o attacchi cyber, tutelando la stabilità del sistema finanziario e la fiducia di clienti e partner. In parallelo, le autorità di vigilanza europee (**EBA**, **ESMA**, **EIOPA**) e l'Agenzia per la Cybersecurity europea **ENISA** promuovono l'adozione di *best practice* di Cyber Intelligence e cooperazione informativa per potenziare la resilienza del settore*. In questo scenario, l'Open Source Intelligence (OSINT) – inteso come l'insieme di tecniche di raccolta e analisi di informazioni da fonti aperte e pubbliche – emerge come uno strumento strategico imprescindibile.

Come evidenziato dalle analisi condotte da ENISA, nel solo periodo gennaio 2023 – giugno 2024 sono stati osservati in Europa 301 incidenti cyber a danno di banche, pari al 46% del totale degli incidenti nel settore finanziario. Questo dato sottolinea l'elevata esposizione delle banche a minacce quali attacchi ransomware, violazioni di dati, campagne di phishing mirate e disruption operative (ad es. DDoS) che possono avere impatti sistemici. In risposta, il Regolamento DORA richiede agli enti finanziari di adottare una **postura proattiva di resilienza digitale**, **integrando nei propri processi di risk management strumenti avanzati di Cyber Threat Intelligence**. L'OSINT, in quanto componente chiave dell'Intelligence finalizzata all'individuazione e analisi delle minacce, può fornire alle banche informazioni tempestive e pertinenti su vulnerabilità emergenti, attività di attori malevoli e segnali premonitori di incidenti, contribuendo così a prevenire gli attacchi o mitigarne gli impatti. Nei passaggi successivi questo lavoro inquadrerà dapprima il Regolamento DORA e i principali obblighi per le banche, quindi analizzerà il valore strategico dell'OSINT nelle fasi di prevenzione, rilevamento e risposta a incidenti ICT, con esempi concreti di strumenti e metodologie utilizzabili. Verranno inoltre forniti riferimenti normativi (EBA, ESMA, EIOPA, ENISA) e mostrato come l'OSINT può essere integrato nei processi di gestione del rischio, controllo dei fornitori terzi critici, B*usiness Continuity* e *Incident Reporting* previsti da DORA.

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.

**In italia l'Agenzia per la cybersicurezza nazionale (ACN) è l'Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nel campo della cybersicurezza. L'Agenzia ha il compito di tutelare la sicurezza e la resilienza nello spazio cibernetico, incluso il settore finanziario.*

IL REGOLAMENTO DORA E GLI OBBLIGHI PER LE BANCHE

Il Regolamento DORA introduce un quadro organico di requisiti per rafforzare la resilienza digitale di un ampio spettro di entità finanziarie (incluse banche, assicurazioni, imprese di investimento, infrastrutture di mercato nonché fornitori ICT critici). In quanto regolamento UE, le sue disposizioni sono direttamente applicabili in tutti gli Stati membri senza necessità di recepimento nazionale. Di seguito sintetizziamo i pilastri chiave del DORA e gli obblighi pertinenti per gli Istituti bancari:

- **Governance e ICT Risk Management**: le banche devono implementare un robusto **framework di gestione del rischio informatico e operativo**. Ciò implica *policies* e procedure formali per identificare, valutare e mitigare i rischi ICT su base continuativa. Il *Management* bancario ha precisi doveri di *Governance*: il DORA richiede infatti **chiara assegnazione di ruoli e responsabilità**, coinvolgimento del Consiglio di Amministrazione nella supervisione della resilienza digitale, nonché integrazione della gestione del rischio ICT nella strategia aziendale. Le banche devono quindi effettuare periodiche valutazioni dei rischi, mantenere un registro aggiornato delle risorse ICT critiche e delle relative vulnerabilità e adottare controlli di sicurezza adeguati e proporzionati alla loro dimensione e profilo di rischio. EBA, ESMA ed EIOPA (le E*uropean Supervisory Authorities*, ESAs) stanno sviluppando *Regulatory Technical Standards* (RTS) per dettagliare gli elementi del framework di gestione del rischio ICT (ad es. requisiti di ICT *Risk Assessment*, controllo e audit interno). Le linee guida esistenti dell'EBA su ICT e sicurezza inoltre state adeguate per allinearsi a DORA e fornire indicazioni coerenti alle banche.

- **Gestione degli incidenti ICT e incident reporting**: il DORA impone obblighi stringenti di rilevazione e segnalazione degli incidenti informatici. Le banche devono disporre di processi per identificare tempestivamente gli *ICT-related incidents* (in particolare quelli con impatto significativo) e notificare quelli maggiori alle Autorità competenti entro termini prefissati.

  La segnalazione deve includere informazioni dettagliate sull'incidente, causa, impatti su servizi critici, misure di contenimento adottate, ecc… L'EBA e le altre autorità stanno armonizzando a livello europeo i template e le soglie per il *major incident reporting* (in coordinamento anche con quanto già previsto dalla PSD2 per gli incidenti gravi nei pagamenti). Inoltre, il DORA incoraggia la **trasparenza e la collaborazione intra-settoriale**: non bisogna solo notificare ai regolatori, ma anche condividere, ove appropriato, informazioni utili su minacce e vulnerabilità con altri attori. L'obiettivo è creare un **ecosistema in cui le banche imparino dagli incidenti reciproci, elevando la postura di difesa collettiva.**

- **Gestione del rischio dei fornitori ICT di terze parti:** riconoscendo l'elevata interdipendenza digitale del settore finanziario, il DORA dedica particolare attenzione alla gestione del rischio ICT derivante da fornitori terzi e partner tecnologici critici. Le banche devono effettuare una rigorosa *due diligence* e un'attività di monitoraggio continuo sui propri fornitori di servizi ICT (es. *cloud provider*, società di *outsourcing* IT, *software vendor*), soprattutto quelli che erogano servizi essenziali o processano dati sensibili. Ciò include la valutazione dei rischi, la verifica dei piani di continuità operativa del fornitore, e l'inclusione nei contratti di specifiche clausole di resilienza (ad es. audit, requisiti minimi di sicurezza, obbligo di informare circa gli incidenti subiti). Il DORA istituisce inoltre un **meccanismo di oversight** diretto sui fornitori ICT critici: se un fornitore esterno viene designato *Critical Third-Party Provider* (CTPP) per il settore finanziario, sarà soggetto alla supervisione congiunta delle ESAs (*Lead Overseer)* in collaborazione con ENISA. In pratica, un *cloud provider* o servizio core designato come "critico" per molte banche UE dovrà sottostare a verifiche di compliance e resilienza da parte delle autorità europee.

Le banche sono poi tenute a mantenere aggiornato l'elenco dei fornitori ICT critici e a notificare alle Autorità eventuali nuove esternalizzazioni di funzioni importanti, in linea con gli RTS emanati (ad es. RTS sull'esternalizzazione ICT di funzioni critiche).

- **Test di resilienza operativa digitale:** il DORA rende obbligatori **programmi di *testing* periodico** delle difese cibernetiche. Tutte le banche devono condurre test di base (*vulnerability assessments, penetration test* tradizionali) almeno annualmente sui propri sistemi e processi ICT. Inoltre, le istituzioni finanziarie più grandi o sistemicamente rilevanti dovranno effettuare test avanzati di tipo *threat-led* almeno ogni tre anni. Questi test avanzati, spesso indicati come TLPT (*Threat-Led Penetration Testing*), consistono in **esercizi di *Red Teaming* etico condotti sulla base di Intelligence sulle minacce reali** (quindi scenario di attacco realistico). Il modello di riferimento europeo per la conduzione di test avanzati di cybersicurezza armonizzati è il TIBER-EU. In Italia, la Banca d'Italia, la Consob e l'IVASS hanno adottato la Guida nazionale TIBER-IT che costituisce quindi il recepimento in ambito nazionale del framework TIBER-EU. Lo scopo è simulare attacchi sofisticati mirati ai sistemi critici della banca, per identificare punti deboli e verificare la capacità di rilevamento e risposta. Il DORA prevede anche criteri uniformi nell'UE per individuare chi deve fare TLPT, come condurli (es. requisiti per i *tester*, scopo minimo, gestione dei risultati) e il mutuo riconoscimento degli esiti tra Stati membri. Per le banche italiane ed europee, ciò rappresenta un **significativo "innalzamento dell'asticella"**: dovranno dotarsi di capacità interne o esterne di *Threat Intelligence* e *Red Teaming* per soddisfare questa richiesta di test basati su scenari di attacco reali.

- **Informazione e cooperazione sulle minacce**: un ulteriore pilastro di DORA riguarda la condivisione di informazioni di *Threat Intelligence*. Il regolamento facilita (pur senza renderlo obbligatorio) l'istituzione di accordi di *condivisione informativa tra entità finanziarie, al fine di scambiare dati su indicatori di compromissione (IOC), tattiche e tecniche di attacco emergenti, vulnerabilità individuate e incidenti gestiti.*
  Lo scopo è elevare la consapevolezza collettiva sulle minacce: ogni banca che partecipa a tali circuiti (ad esempio information sharing platforms settoriali come CERTfin in Italia o l'FS-ISAC a livello globale) contribuisce e al contempo beneficia dell'Intelligence condivisa. Nel rispetto di condizioni antitrust, privacy e riservatezza, il DORA chiarisce quindi che le banche "possono scambiare tra loro informazioni e Intelligence su cyber threat, inclusi IoC, TTP degli attaccanti, ecc…" per migliorare le capacità di difesa.

Questa enfasi sulla collaborazione riflette la consapevolezza "regolamentare" che la cybersicurezza è un problema sistemico: solo attraverso la cooperazione attiva l'ecosistema finanziario può tenere il passo con minacce sempre più sofisticate.

Questi obblighi imposti dal DORA si applicano pienamente alle banche (in quanto *credit institutions* rientranti tra le "*financial entities*" previste) al pari degli altri attori regolati. Le banche, data la loro criticità, dovranno affrontare compiti significativi di compliance, adeguando alle nuove norme: processi interni, sistemi di controllo e contratti con terze parti. In cambio, l'attuazione efficace del Regolamento dovrebbe tradursi in un incremento tangibile della resilienza operativa: minori interruzioni dei servizi finanziari essenziali e capacità di assorbire shock-cyber senza impatti sistemici. Tuttavia, soddisfare tali requisiti richiede anche un cambio di paradigma nella gestione della sicurezza: dalle sole *checklist* di conformità verso un approccio *Intelligence-driven*, in cui strumenti come l'OSINT e la *Threat Intelligence* diventano parte integrante del ciclo di vita del *Risk Management*. Nel capitolo seguente esamineremo proprio come l'OSINT possa apportare valore strategico nella prevenzione, rilevazione e risposta a minacce e incidenti ICT, aiutando le banche a rispettare e dare sostanza ai principi del DORA.

IL VALORE STRATEGICO DELL'OSINT NELLA RESILIENZA DIGITALE BANCARIA

L'OSINT è comunemente definita come l'attività finalizzata a raccogliere e analizzare dati liberamente disponibili al pubblico per ricavarne **Intelligence "actionable".** In ambito finanziario, questo concetto si traduce nell'impiego di informazioni provenienti da fonti aperte – come siti web, blog, forum cyber underground, social media, database pubblici di vulnerabilità, report di ricerca, ecc. – per ottenere indicazioni utili a prevenire o gestire i rischi informatici. A differenza delle fonti classificate o proprietarie, l'OSINT sfrutta materiale informativo di dominio pubblico (open web, deep web accessibile e in alcuni casi dark web) e lo trasforma, attraverso attività di analisi, in conoscenza a supporto dei processi decisioni.

In ottica DORA, l'OSINT rappresenta quindi un "sensore avanzato" sull'ecosistema delle minacce e delle vulnerabilità che circondano la banca. **Integrando le capacità di OSINT nei propri processi, un istituto finanziario può ottenere benefici lungo l'intero ciclo di gestione degli incidenti**: **dalla prevenzione proattiva, all'individuazione tempestiva, fino alla risposta e al recovery**. L'intero processo è descritto in maniera puntuale nel framework sviluppato dal Computer Emergency Response Team della Banca d'Italia (CERTBI) che integra aspetti tassonomici e specifici processi funzionali allo scopo di sviluppare avanzate capacità di CTI. Ma analizziamo ora come l'OSINT contribuisce alle tre fasi.

OSINT per la prevenzione di incidenti e minacce

In fase di prevenzione, l'OSINT consente di giocare d'anticipo rispetto ai potenziali attaccanti, fornendo *early warning* su rischi emergenti. Alcuni esempi concreti di valore aggiunto:

- **Individuazione di vulnerabilità e exploit emergenti**: tramite il monitoraggio costante di fonti aperte (portali di sicurezza, *mailing list, repository* di *exploit*, social media di ricercatori, ecc...), una banca può venire a conoscenza tempestivamente di nuove vulnerabilità che impattano sistemi o software da essa utilizzati, ancor prima che gli attaccanti le sfruttino su larga scala. Ad esempio, la divulgazione pubblica di una nuova *Common Vulnerabilities and Exposures* (CVE) critica su un sistema bancario core (come un *software* di *online banking*) può essere captata via OSINT in tempo reale, permettendo alla banca di valutare immediatamente l'applicabilità della *patch* o di implementare misure di mitigazione. Anche le informazioni provenienti dal dark web possono essere rilevanti: nei forum in cui sono attivi gruppi di cybercriminali potrebbero essere messi in vendita *exploit* o *zero-day* contro applicativi finanziari – segnalazioni che, se intercettate per tempo dall'Intelligence bancaria, consentono di attivare contromisure prima che la falla venga sfruttata. In sintesi, un **efficace *vulnerability assessment* basato sull'OSINT aiuta a rinsaldare gli anelli deboli prima che diventino porte d'ingresso per gli attacchi**, supportando così l'obbligo DORA di gestione proattiva del rischio ICT.

- **Threat modeling e anticipazione di nuove tattiche di attacco:** attraverso l'analisi di report pubblici e condivisioni di *Threat Intelligence* (ad esempio

white paper di società di sicurezza, bollettini CSIRT, CERT, analisi tecniche di campagne malevole recenti), i Team di sicurezza bancaria possono aggiornare costantemente i propri modelli di minaccia e gli scenari di rischio. L'OSINT offre un flusso continuo di informazioni sulle TTP (tattiche, tecniche e procedure) adottate dai *Threat Actors*: quali *malware* sono in circolazione, quali nuove tecniche di *social engineering* si stanno diffondendo, quali settori sono nel mirino dei cybercriminali, ecc...

Queste conoscenze consentono di adattare le misure preventive *ex ante* – ad esempio irrobustendo certe difese, alzando soglie di allerta per determinati indicatori o svolgendo sessioni formative specifiche al personale su nuove tipologie di *phishing* osservate. In termini di Regolamento, tutto ciò significa **rinforzare il *framework* di *Risk Management* con un ciclo di apprendimento continuo basato sull'Intelligence**: la norma infatti richiede di aggiornare periodicamente l'analisi dei rischi tenendo conto dell'evoluzione delle minacce. Incorporare l'OSINT nei processi di *Threat Modeling* soddisfa proprio questa esigenza di dinamismo, creando un collegamento tra ciò che accade "fuori" e le strategie difensive interne della banca.

- **Scoperta di esposizioni involontarie di dati e configurazioni vulnerabili:** un aspetto peculiare dell'OSINT è la capacità di far luce su informazioni relative all'Istituzione che sono già pubblicamente disponibili, senza che la banca ne sia consapevole. Ciò include, ad esempio, la presenza di dati sensibili pubblicati accidentalmente (es. documenti interni finiti online), di credenziali o chiavi API trapelate su *repository* di codice pubblici, di *bucket cloud* non protetti contenenti informazioni della banca o di configurazioni errate rilevabili attraverso *scanning* esterno. **Un'attività di OSINT ben strutturata simula l'attività di ricognizione che un attaccante potrebbe svolgere per rilevare il *Digital footprinting* dell'organizzazione da colpire**: utilizzando motori di ricerca specializzati e altre tecniche passive, è possibile mappare l'"ombra digitale" dell'Istituto, identificando asset esposti e possibili falle. Tali scoperte permettono interventi correttivi preventivi (ad es. rimuovere dati pubblicati per errore, chiudere "porte aperte", modificare impostazioni di sicurezza), riducendo la superficie d'attacco. Questo approccio sposa pienamente la filosofia del DORA, che impone alle banche negli aspetti meno visibili. L'OSINT diventa quindi un alleato del IT *Risk Assessment* perché integra la visione interna con la prospettiva esterna dell'attaccante, contribuendo a un'identificazione completa delle criticità.

L'OSINT per il rilevamento tempestivo e l'allerta preventiva

In aggiunta all'ambito della prevenzione, l'OSINT gioca un ruolo cruciale anche nella fase di rilevamento (*detection*) di incidenti e minacce in atto. Molto spesso, i primi segnali di un attacco o di una violazione compiuta emergono su canali esterni prima ancora che l'organizzazione target se ne accorga tramite i propri sistemi interni. Avere sensori OSINT significa poter captare questi segnali deboli e trasformarli in alert attivabili. Vediamo alcuni casi d'uso:

- **Monitoraggio del dark web e forum clandestini:** i gruppi cybercriminali utilizzano il *dark web* (circuiti Tor, marketplace illegali, chat riservate) per scambiare informazioni e vendere dati rubati. Un programma OSINT efficace deve quindi includere anche la funzione di *dark web monitoring*, volta a individuare eventuali riferimenti all'Istituto bancario, ai suoi clienti o asset. Ad esempio, la comparsa su un *forum underground* di un database in vendita contenente i dati dei clienti di una banca rappresenta un chiaro indicatore di *breach*: grazie all'OSINT, la banca può venire a conoscenza della potenziale violazione anche se gli attaccanti non l'hanno comunicata pubblicamente.

  Sul *dark web* compaiono anche spesso credenziali rubate (username/password) appartenenti a utenti di servizi finanziari: intercettare liste di account della propria banca permette di avviare subito azioni di mitigazione (forzare reset password, avvisare i clienti coinvolti) prima che gli attaccanti utilizzino quelle credenziali per successive frodi. In generale, come evidenziato da analisti di *Cyber Intelligence*, attraverso OSINT su fonti *darknet* si possono scoprire *leak* di informazioni sensibili, dati su campagne di attacco in preparazione e perfino segnalazioni di falle *zero-day* quindi sconosciute. Tutti elementi che, se raccolti e validati rapidamente, consentono di riconoscere un possibile incidente nelle sue fasi iniziali (o addirittura prevenirlo) e attivare le contromisure del caso.

- **Social media monitoring e analisi open source:** le piattaforme social e il web accessibile spesso fungono da "allarme" in caso di problemi di sicurezza. Clienti che segnalano su Twitter anomalie nell'accesso ai servizi *online banking*, post su forum di tecnologia che discutono di un possibile disservizio di una banca, o ancora rivendicazioni di attacco da parte di cyber criminali su canali social – tutti questi eventi rappresentano indicazioni rilevanti.

Un team di sicurezza che monitora attivamente parole chiave e menzioni relative al proprio brand bancario sui *social network* può identificare tempestivamente segnali di *phishing* in corso (es. segnalazioni di clienti che ricevono messaggi sospetti a nome della banca) o capire che un certo disservizio IT potrebbe in realtà celare un attacco (es. numerosi clienti twittano di non riuscire ad accedere all'*home banking* – potrebbe essere in atto un DDoS). L'OSINT dunque funge da "radar esterno" integrativo rispetto ai sistemi di monitoraggio interni (SIEM, IDS, etc...): mentre questi ultimi rilevano indicatori tecnici sulla rete aziendale, l'OSINT coglie l'elemento umano e informativo esterno, completando il quadro situazionale. Per una banca, questo può fare la differenza tra venire a conoscenza di un attacco *ex post*, oppure intercettare subito l'allarme lanciato dalla comunità online e reagire in tempo reale. Il DORA richiede peraltro alle entità finanziarie capacità di monitoraggio continuo e *detection* efficace degli incidenti: incorporare flussi OSINT nelle attività di security monitoring contribuisce a soddisfare tale requisito, ampliando il raggio d'azione del Security Operations Center (SOC) anche oltre i confini aziendali.

- **Indicatori di compromissione (IoC) e Threat Intelligence pubblica:** un altro contributo fondamentale dell'OSINT al rilevamento delle minacce, consiste nell'apporto di indicatori di compromissione noti, raccolti da fonti aperte. Ad esempio, molte organizzazioni (CSIRT, CERT, aziende di sicurezza, comunità open source) condividono pubblicamente indicatori di compromissione relativi a campagne malevole: indirizzi IP di *Command-and-Control*, *hash* di file *malware*, domini di *phishing*, ecc... Questi IoC, reperibili tramite OSINT in feed pubblici o report tecnici, possono essere integrati nei sistemi di difesa della banca (firewall, IDS, anti-virus, SIEM) per innalzare subito barriere contro minacce note. Se una nuova botnet prende di mira il settore finanziario e pubblicamente vengono diffusi gli IP da bloccare, una banca dotata di capacità OSINT potrà acquisire rapidamente tali dati e caricarli nei propri controlli di sicurezza, innalzando lo stato di allerta prima ancora di subire l'attacco. Allo stesso modo, l'OSINT può fornire informazioni di contesto relative agli eventi rilevati dai sistemi interni: ad esempio, se il SOC nota traffico verso un certo dominio sospetto, un'analisi OSINT potrebbe rivelare che quel dominio compare in una *blacklist* pubblica associata a un gruppo APT noto – informazione vitale per qualificare l'evento come grave e avviare le attività di *Incident Response*. In questo senso il DORA enfatizza l'importanza di *Threat Intelligence* nel migliorare *detection* e *situational awareness*; l'OSINT ne è un pilastro naturale, poiché gran parte della Threat Intelligence (soprattutto a livello tattico) deriva da dati open source condivisi tra le comunità che si occupano di sicurezza.

In sintesi, l'OSINT potenzia il rilevamento trasformando le informazioni in *alert*. Ciò aumenta il *lead time* a disposizione della banca per reagire e consente di migliorare la capacità di *Incident Response,* attraverso una risposta più "pronta e rapida". A livello operativo, molte banche stanno integrando flussi OSINT nei loro strumenti SIEM/SOAR, automatizzando in parte la correlazione tra eventi interni e informazioni esterne: ad esempio, collegando feed OSINT (feed IoC, social media stream) e generando alerts combinati. Questo approccio multi-sorgente rappresenta oggi lo stato dell'arte nel rilevamento cyber.

L'OSINT per la risposta e la gestione degli incidenti

Durante e dopo un incidente ICT conclamato, l'OSINT continua a fornire valore aggiunto supportando la fase di risposta (*Response*) e le successive attività di Recovery & *Remediation*. Una risposta efficace agli incidenti, come richiesto dal DORA, deve essere informata e tempestiva e l'Intelligence da fonti aperte contribuisce a supportarla in diversi modi:

- **Contestualizzazione della minaccia e attribuzione.** Nel momento in cui una banca subisce un attacco (es. malware diffuso nella rete, un *defacement* al sito, un furto di dati), una priorità per orientare la risposta è comprendere chi potrebbe essere responsabile e come sta operando. L'OSINT consente di attingere a informazioni pubbliche su campagne malevole: ad esempio, se la banca identifica un certo *ransomware* nei suoi sistemi, tramite OSINT può raccogliere dai report pubblici tutto ciò che è noto su quella specifica minaccia (tecniche di propagazione, eventuali *killswitch*, indicatori, modalità di recupero dei dati, affiliati noti). Ciò consente di assumere decisioni informate (es. isolare subito certe parti di rete, cercare indicatori specifici). Allo stesso modo, se un attaccante rivendica l'attacco sui social o su un sito di *leak*, l'OSINT fornisce all'*Incident Response Team* possibili elementi di *attribution* (chi sono, quali altri attacchi hanno compiuto, che scopo hanno). Sapere che dietro un attacco DDoS c'è, ad esempio, un collettivo noto per azioni brevi e dimostrative orienterà la risposta e la comunicazione in modo diverso rispetto a trovarsi di fronte a un'operazione APT di spionaggio protratta nel tempo. Ottenere queste informazioni attraverso l'Intelligence open source, mentre l'incidente è ancora in corso, migliora la situational awareness e consente di coinvolgere le autorità o attivare piani di crisi appropriati al tipo di avversario.

- **Individuazione di dati sottratti e gestione delle notifiche:** in caso di *data breach* (esfiltrazione di dati riservati), l'OSINT diventa fondamentale per scoprire se e cosa dei dati rubati viene pubblicato o venduto. Molti attaccanti, specialmente nei *ransomware double extortion*, rendono noti estratti dei dati rubati sui propri siti nel *dark web* per fare pressione sulle vittime. Monitorando tali siti o canali Telegram affiliati, la banca può verificare l'entità dei dati compromessi. Questa conoscenza è fondamentale sia per predisporre comunicazioni chiare ai clienti coinvolti, sia per assolvere ad obblighi normativi di notifica (ad esempio verso il Garante per la Privacy per violazione di dati personali). Il DORA stesso prevede che, nella reportistica post-incidente, l'ente finanziario fornisca alle autorità aggiornamenti sull'evoluzione dell'incidente e sulle misure correttive intraprese. Poter riferire se i dati sono apparsi online (o confermare che non risultano diffusi pubblicamente) è parte di queste informazioni.

  L'OSINT post-incidente aiuta anche a scoprire eventuali indicatori residui: ad esempio, cercando in database open di *malware* (come VirusTotal) eventuali campioni correlati all'attacco subito, per assicurarsi di rimuovere tutte le componenti maligne. In definitiva, integrare l'OSINT nelle attività di *Incident Response* migliora sia la completezza "forense" (capire cosa è successo con evidenze anche esterne) sia la capacità comunicativa verso *stakeholder* interni, regolatori e clienti, basata su fatti oggettivi raccolti da fonti aperte.

- **Lezioni apprese e miglioramento continuo**: dopo la gestione immediata dell'incidente, l'OSINT contribuisce anche alla fase di *post-incident review* e successivo *hardening*. Analizzando tramite l'OSINT le modalità con cui altre organizzazioni hanno affrontato incidenti simili (case study pubblici, blog post tecnici) si possono infatti identificare le azioni di miglioramento da adottare. Inoltre, continuare a monitorare nel medio termine, le fonti OSINT relative all'incidente, consente di sapere se, ad esempio, emergono nuove varianti della minaccia iniziale o ancora se la vulnerabilità sfruttata viene discussa e potrebbe causare attacchi secondari. In questo senso, il DORA richiede alle banche di aggiornare i propri processi e controlli sulla base degli incidenti occorsi (**principio di apprendimento continuo**): l'OSINT funge quindi anche da fulcro della conoscenza esterna a cui attingere per non sprecare le lezioni apprese sia internamente che dalle comunità informative di riferimento. Ad esempio, se l'incidente ha rivelato una lacuna, l'OSINT può suggerire quali soluzioni hanno implementato le altre banche (emerse ad esempio attraverso conferenze o pubblicazioni di settore).

Riassumendo, l'OSINT permea tutte le fasi dell'*Incident Management*, fornendo Intelligence tempestiva e contestuale che può consentire l'assunzione di decisioni migliori. Ciò è perfettamente allineato alla filosofia del DORA: il Regolamento infatti, pur essendo *compliance-oriented*, incoraggia un approccio *risk-based* e quindi informato ai rischi cyber. Le linee guida EBA evidenziano la necessità per le banche di adottare capacità di *situational awareness* e monitoraggio continuo di minacce e vulnerabilità e l'OSINT è uno dei mezzi più efficaci per soddisfare tale aspettativa.

STRUMENTI E METODOLOGIE OSINT APPLICABILI IN AMBITO DORA

Dopo aver esaminato cosa può offrire l'OSINT, passiamo al come: quali strumenti e approcci pratici le banche possono utilizzare per integrare l'OSINT nelle loro attività di resilienza digitale in ottica DORA. È importante sottolineare che l'OSINT non si riduce all'utilizzo un singolo tool, ma è un insieme di metodologie supportate da differenti fonti e tecnologie. Una strategia OSINT completa attinge da fonti eterogenee – dal web superficiale fino al dark web – e richiede competenze analitiche per trasformare i dati grezzi in insight utili.

Vediamo ora, a titolo esemplificativo, alcune categorie di esempi concreti di utilizzo dell'OSINT nel contesto bancario:

- **Monitoraggio di fonti aperte e news:** piattaforme di news monitoring e web crawling permettono di aggregare in tempo reale notizie, blog e aggiornamenti relativi a cybersecurity e attacchi. Ad esempio, utilizzare feed RSS di siti specializzati, Google alerts e similari con parole chiave o piattaforme OSINT che scandagliano continuamente il web alla ricerca di menzioni. Così facendo, i Team di sicurezza e *compliance* possono ricevere allarmi immediati su eventi nel settore e reagire valutando l'esposizione della propria organizzazione. Questo monitoraggio riguarda anche possibili notizie reputazionali (es. *leak* di dati) spesso diffuse prima dai media.

- **Threat Intelligence pubblica e database di indicatori:** esistono molte fonti open di cyber *Threat Intelligence* che le banche possono sfruttare. Tra queste: database di vulnerabilità come NVD e CVE database (utili per tracciare CVE e *exploit* noti), piattaforme di condivisione IoC come VirusTotal, MalwareBazaar, Abuse.ch, ecc... (dove reperire *hash* di *malware*, URL malevoli, IP di botnet), report tecnici di vendor di sicurezza che spesso pubblicano dettagli di campagne APT o nuove famiglie di malware. Strumenti OSINT possono automatizzare la raccolta da queste fonti: ad esempio *script* che ogni giorno estraggono da piattaforme specializzate le CVE nuove con *score* alto relative a *software* finanziari, oppure integrazione API a servizi come VirusTotal per allertare se compaiono file sospetti col nome della banca.

- **Ricognizione della propria "impronta digitale"**: rientrano qui strumenti e tecniche OSINT volti a scandagliare ciò che di pubblico esiste sull'organizzazione. Si va da semplici query mirate (utilizzo avanzato di motori di ricerca – Google dorking – per trovare documenti o pagine riferite alla banca) a strumenti specializzati: ad es. Shodan per individuare dispositivi e sistemi della banca esposti su Internet, SecurityTrails o DNSdumpster per mappare i sottodomini noti e l'infrastruttura DNS, HaveIBeenPwned per controllare se email di dipendenti compaiono in

archivi pubblici di account violati. Anche i social network professionali come LinkedIn possono essere fonti OSINT: analizzando i profili pubblici dei dipendenti di una banca, un attaccante può dedurre informazioni organizzative utili a phishing mirati – quindi anche la banca può svolgere questa analisi per rendersi conto di quali informazioni sensibili (ruoli, tecnologie usate menzionate nei CV, ecc...) stia più o meno consapevolmente esponendo.

- **Analisi del dark web e data leak detection:** come già evidenziato, esistono tool dedicati alla navigazione e ricerca nel dark web. Piattaforme commerciali di Dark Web Monitoring consentono di cercare in modo relativamente sicuro informazioni specifiche all'interno di marketplace, forum e canali Telegram utilizzati da criminali. In alternativa, analisti OSINT addestrati possono utilizzare browser Tor e motori di ricerca specializzati per individuare risorse nascoste. Spesso si impiegano anche strumenti di crawling automatico che analizzano interi forum per potervi effettuare ricerche di parole chiave.

- **Social media Intelligence (SOCMINT)**: Oltre al monitoraggio generico dei social citato prima, esistono strumenti OSINT specifici per analizzare contenuti da social network. Ad esempio, *tool* in grado di estrarre e aggregare *tweet* e post pubblici in base a geolocalizzazione o *hashtag* (per cogliere *trend*, *sentiment* o concentrazione anomala di discussioni su un certo tema legato alla banca). Nel caso di crisi, questi strumenti aiutano a avere il polso della situazione in tempo reale. L'OSINT consente inoltre l'identificazione di profili falsi che si spacciano per la banca o per dirigenti (minaccia al brand e possibili frodi).

- **Framework e piattaforme integrate:** in commercio e nella comunità open source esistono piattaforme che raccolgono molte di queste funzionalità OSINT in un unico ambiente. Alcuni esempi: strumenti di *link analysis*, che permettono di incrociare varie fonti OSINT (DNS, social, leak, etc.) per mappare relazioni; oppure OSINT *Framework* ovvero *repository* di risorse OSINT categorizzati, utili per costruire la propria *toolbox*; o ancora soluzioni di *Threat Intelligence Platform* (TIP) che integrano dati *open* con fonti proprietarie e permettono analisi collaborative. Le banche più grandi spesso adottano piattaforme di *Threat Intelligence* che includono moduli OSINT e automazione (ad es. MISP – *Malware Information Sharing Platform* – per condividere indicatori, o Soluzioni SIEM/SOAR con connettori a fonti OSINT).

È importante notare che l'OSINT, pur fornendo tantissimi dati, richiede sempre una valutazione critica da parte degli analisti: non tutte le informazioni reperite saranno infatti affidabili o rilevanti. Pertanto, le banche devono sviluppare anche processi di validazione e filtraggio dell'Intelligence grezza (ad es. verificare le fonti, correlare con dati interni, scartare false positive). Inoltre, l'utilizzo di strumenti OSINT deve sempre rispettare le normative (privacy, legalità delle attività di raccolta). In questo senso, è opportuno privilegiare informazioni già pubbliche ed evitare sempre pratiche al confine con l'hacking non etico. Con queste accortezze, le metodologie OSINT possono essere integrate in modo sicuro ed efficace nel security toolkit di una banca.

Tabella 1: Sintesi di fonti e strumenti OSINT applicabili e relativo contributo alla resilienza operativa secondo il DORA.

Categoria OSINT	Esempi di fonti e strumenti	Utilizzo per resilienza DORA
Open Web e News	Siti news cyber, blog, RSS, Google Alerts.	Allerta su nuovi attacchi/vulnerabilità nel settore; contesto sulle minacce emergenti.
Database Threat Intelligence	CVE/NVD, feed IoC open (es. liste IP/URL malevoli), CERT pubblici.	Aggiornamento continuo su vulnerabilità note e indicatori di attacco da bloccare preventivamente.
Footprinting & Asset discovery	Motori di ricerca avanzati (Google dork), Shodan, Lookup DNS, leak credenziali (HaveIBeenPwned).	Identificazione di esposizioni accidentali, asset non noti, credenziali compromesse collegate alla banca.
Dark Web Monitoring	Forum cyber underground, marketplace Tor, siti leak ransomware, Telegram gruppi criminali.	Rilevamento di dati rubati messi in vendita, discussioni su attacchi pianificati alla banca, exploit in vendita che minacciano la banca.
Social Media Monitoring (SOCMINT)	Twitter, Facebook, LinkedIn, forum utenti, strumenti sentiment analysis.	Intercettazione di segnali d'allarme (clienti che segnalano problemi, phishing in corso, account falsi), gestione crisi comunicativa.
Threat Intelligence Platform / Tools integrati	MISP, TIP commerciali, OSINT framework con raccolte di risorse.	Correlazione di informazioni da diverse fonti, condivisione Intelligence interna ed esterna (es. CERTfin), automazione di raccolta e alerting.

INTEGRAZIONE DELL'OSINT NEI PROCESSI DI GESTIONE DEL RISCHIO E RESILIENZA (DORA)

Alla luce di quanto esposto, risulta evidente che **l'OSINT non è una funzione a sé stante, ma rappresenta una disciplina che va integrata trasversalmente nei processi aziendali disciplinati dal Regolamento DORA**. In questa sezione discutiamo come l'OSINT si inserisce nei principali ambiti previsti dal Regolamento – ICT Risk Management, gestione fornitori terzi critici, business continuity, incident reporting – evidenziando principali sinergie e benefici.

- **Risk management & Governance**: il *framework* di gestione del rischio ICT richiesto da DORA deve essere *Intelligence-led*, ovvero guidato dalle informazioni sui rischi reali. L'OSINT può essere formalmente inserita come fase del processo di *Risk Management*: per esempio, durante le periodiche valutazioni dei rischi ICT, gli analisti potrebbero includere un report OSINT sulle nuove minacce rilevanti per la banca e sulle vulnerabilità emerse su fonti aperte dall'ultimo *assessment*. Ciò garantisce che la *Risk analysis* tenga conto non solo di scenari ipotetici, ma anche di ciò che sta concretamente accadendo nel panorama delle minacce. Inoltre, l'OSINT può supportare la prioritizzazione dei rischi: se tramite l'OSINT si scopre che un certo tipo di attacco sta aumentando la propria frequenza (es. attacchi *supply-chain* a *software* gestionali), la banca può elevare il *ranking* di rischio associato e destinare più risorse a controlli mitiganti in quell'area. Dal punto di vista della *Governance*, i risultati dell'attività OSINT dovrebbero essere regolarmente presentati al M*anagement* (es. nei KPI/KRI di rischio ICT): ciò sensibilizza i decisori sul contesto esterno e li aiuta a giustificare eventuali investimenti. In sostanza, l'OSINT diventa un "radar strategico" inserito nel ciclo di gestione rischio, in linea con la spinta di DORA verso un ruolo attivo del board nella *Cyber Resilience*.
- **Monitoraggio fornitori terzi critici:** il DORA enfatizza l'importanza di controllare il rischio derivante da fornitori ICT esterni. In quest'ambito, l'OSINT offre alle banche occhi e orecchie aggiuntive per vigilare sui propri *vendor*.

Ad esempio, la banca può impostare un monitoraggio OSINT sul nome dei suoi fornitori critici: se un fornitore *cloud* subisce un incidente (anche fuori dai servizi resi alla banca) o un *data breach*, probabilmente la notizia circolerà pubblicamente – saperlo immediatamente consente alla banca di valutare impatti sul proprio business e pretendere chiarimenti dal fornitore (anticipando la comunicazione ufficiale che potrebbe tardare). Analogamente, se nel *dark web* compaiono credenziali o accessi VPN in vendita afferenti a un fornitore terzo della banca, questa informazione OSINT è di enorme valore: permette di allertare il fornitore e temporaneamente sospendere integrazioni in attesa di verifica, prevenendo un possibile attacco *supply-chain*. L'OSINT consente anche di monitorare aspetti reputazionali o di solidità dei partner (es. notizie su difficoltà finanziarie di un service provider IT, che potrebbero preludere a disservizi). Tutti questi *input* dovrebbero confluire nel processo di *Third-Party Risk Management*: per esempio, come parte del *Risk Assessment* periodico sui fornitori, la banca può includere un *Open Source Intelligence check,* riportando se negli ultimi mesi sono emerse criticità pubbliche su quel *provider*. Ciò aumenterà la capacità di risposta rapida richiesta da DORA in caso di problemi su terze parti critiche. Infine, a livello di settore, anche le autorità (ESAs), tramite ENISA, condurranno analisi OSINT sul panorama dei fornitori critici – le banche possono quindi contribuire segnalando tempestivamente problemi che hanno rilevato via OSINT, alimentando un circolo virtuoso di informazione.

- **Business continuity e resilienza operativa:** il DORA impone alle banche di disporre di piani di continuità operativa ICT efficaci, per reagire rapidamente ad attività di *disruption*. L'OSINT può migliorare sia la preparazione dei piani, sia la gestione concreta delle crisi. In fase di pianificazione (*Business Continuity Planning*), l'Intelligence da fonti aperte aiuta a condurre *Business Impact Analysis* e scenari basati su eventi reali: ad esempio, studiando attraverso l'OSINT come un attacco *ransomware* in un'altra banca abbia impattato i servizi, si possono modellare scenari di interruzione più realistici e predisporre soluzioni di resilienza (siti secondari, backup offline, ecc.) tarati su minacce concrete. Inoltre, l'attività OSINT orientata agli attacchi fisici (es. manifestazioni di attivisti che minacciano sedi di data center) o ai rischi ambientali (meteo estremo, blackout) può integrare gli aspetti ICT e operativi tradizionali per una continuità caratterizzata da un concreto approccio olistico. Durante una crisi attiva, poi, l'attività di *monitoring* OSINT è un complemento fondamentale alla *Situational Awareness*: se un attacco impatta i servizi online, la banca può controllare social e news per comprendere la percezione pubblica e intercettare eventuali voci false, guidando la comunicazione durante la crisi. In pratica l'OSINT, nell'ambito della continuità operativa, assicura che i piani non restino teorici ma si alimentino di *real-world Intelligence* e che, nel corso dell'emergenza, si abbia una visuale più ampia possibile dell'evento.
- **Incident reporting e comunicazioni regolamentari:** un aspetto chiave del Regolamento è la segnalazione formale degli incidenti maggiori alle Autorità in tempi stretti. L'OSINT può agevolare la produzione di report più completi e accurati. Come? Durante la fase di notifica, la banca può includere informazioni raccolte via OSINT che diano evidenze aggiuntive dell'incidente. Ciò fornisce ai *supervisor* un quadro chiaro e documentato, supportandone le successive valutazioni. Inoltre, poiché il DORA richiede aggiornamenti successivi sulla gestione dell'incidente, l'OSINT continua a essere utile anche in questo caso: se emergono nuove informazioni pubbliche (es. l'attaccante rilascia ulteriori dati una settimana dopo), queste possono essere tempestivamente riportate. Un altro ambito è la comunicazione ai clienti, spesso parallela al *reporting* regolamentare, attraverso la quale le banche devono informare gli utenti colpiti. Anche in questo caso, sfruttare l'OSINT (per sapere esattamente quali dati sono finiti online e quali no) consente di comunicare con precisione e trasparenza, riducendo il panico e mantenendo la fiducia della propria clientela. Infine, un ulteriore aspetto: il DORA incoraggia lo *sharing* volontario di informazioni tra entità finanziarie e le informazioni OSINT possono essere un importante contributo da condividere (es. la banca che ha subito l'attacco passa agli altri IoC e dettagli individuati via OSINT), alimentando quella collaborazione settoriale virtuosa che, come già evidenziato, è auspicata dal Regolamento.

Tabella 2: Modalità in cui l'OSINT si integra nei principali processi e requisiti DORA per le banche, con relativi benefici.

Processo DORA	Obblighi chiave	Integrazione e beneficio OSINT
ICT Risk Management	Identificare, valutare e mitigare rischi ICT continuativamente; coinvolgimento board e aggiornamento strategie.	L'OSINT fornisce input su minacce emergenti e vulnerabilità zero-day, migliorando l'identificazione dei rischi. Consente valutazioni dinamiche basate su Intelligence attuale e supporta il board con KPI su minacce reali.
Incident Detection & Response	Monitoraggio continuo e rilevazione tempestiva; piani di risposta rapida e contenimento impatti.	L'OSINT estende il monitoraggio oltre il perimetro interno (dark web, social). Rileva segnali iniziali di incidenti. Durante la risposta, offre contesto (IOC, attributi attaccante) e aiuta a delimitare il perimetro della violazione (dati diffusi online).
Incident Reporting	Notifica entro tempi stringenti degli incidenti maggiori alle Autorità con dettagli e successive relazioni.	L'OSINT arricchisce i report con evidenze esterne (es. dati pubblicati) dando completezza. Aiuta a mantenere aggiornate le Autorità su evoluzioni post-attacco rilevate su fonti aperte. Migliora anche la comunicazione verso clienti/terzi grazie a informazioni verificabili.
Third-Party Risk Management	Due diligence e monitoraggio su fornitori ICT critici; obbligo di conoscere e gestire i rischi di terze parti.	L'OSINT monitora news e forum su fornitori: avvisa se un vendor subisce incidenti o ha falle note. Permette di reagire prontamente (es. attivare piani alternativi) e di dialogare con il fornitore su basi fattuali. In due diligence, rivela eventuali red flag pubbliche su sicurezza o reputazione del candidato.
Digital Operational Resilience Testing	Programma di test periodici (annuali base, triennali avanzati TLPT) sui sistemi critici.	L'OSINT fornisce scenari e Threat Intelligence reali da usare come base nei test "threat-led". Ad esempio, i red team utilizzano informazioni OSINT sull'organizzazione per simulare attacchi realistici (phishing con dati pubblici dei dipendenti, exploit di sistemi individuati via OSINT). Ciò garantisce che i test riflettano vettori d'attacco plausibili e attuali.
Business Continuity Management	Piani di continuità e di disaster recovery per ripristinare rapidamente funzioni critiche; BIA e test regolari.	L'OSINT contribuisce alla BIA identificando minacce ambientali o sistemiche (es. campagne globali) da considerare. Durante le crisi, funge da canale informativo parallelo (feedback utenza, contesto esterno) per prendere decisioni migliori. Nel post-incidente, supporta il miglioramento dei piani apprendendo da incidenti pubblici.
Information Sharing	Facoltà di scambiare Cyber Intelligence (IoC, tattiche, best practice) tra entità finanziarie, nel rispetto normative	L'OSINT è sia oggetto che strumento di condivisione: molte informazioni da condividere derivano da fonti aperte raccolte da una banca. Inoltre, le informazioni ricevute dagli altri possono essere validate e arricchite tramite l'OSINT. Favorisce una conoscenza comune delle minacce, diminuendo asimmetrie informative tra banche.

Come si evince, l'OSINT funge da collante informativo attraverso tutti questi domini: porta evidenze esterne nel *Risk Management*; estende la visibilità delle attività di *Security Monitoring* e *Incident Response*; salvaguarda dalle minacce provenienti dalla supply chain; sostiene la pianificazione di continuità con dati reali; e alimenta la condivisione collaborativa di conoscenza. In breve, **l'OSINT rende i processi previsti dal DORA più proattivi, *Intelligence-driven* e collaborativi, anziché puramente reattivi o burocratici.**

PROSPETTIVE

Il *Digital Operational Resilience Act* inaugura per le banche europee una nuova era di disciplina della resilienza informatica, richiedendo un cambio di passo nella gestione dei rischi ICT e nella risposta agli incidenti. Per soddisfare pienamente lo spirito del DORA – che punta non solo alla conformità, ma alla creazione di un ecosistema finanziario effettivamente resiliente e preparato – gli Istituti devono abbracciare strumenti avanzati di *Cyber Threat Intelligence*. In questo contesto, **l'OSINT emerge come un alleato imprescindibile: la sua capacità di sfruttare la ricchezza informativa delle fonti aperte consente di anticipare le mosse degli attaccanti, sorvegliare l'orizzonte delle minacce e reagire con cognizione di causa agli eventi avversi.**

Abbiamo fin qui cercato di comprendere come l'OSINT possa supportare le attività previste dal Regolamento DORA. In questo senso, emerge chiaramente come l'OSINT sia essenziale per:

- **prevenire gli incidenti** grazie all'individuazione preventiva di vulnerabilità e schemi di attacco;
- **potenziare il rilevamento** attraverso il monitoraggio del dark web, dei social e di indicatori tecnici pubblici;
- **migliorare la risposta** agli incidenti con Intelligence su attaccanti e dati compromessi.

I riferimenti normativi e di settore citati (linee guida EBA, relazioni ENISA, ecc…) confermano la rilevanza di un approccio *Intelligence-driven*. Del resto sono gli stessi legislatori a riconoscere che una *Situational Awareness* basata su informazioni aggiornate è fondamentale per contrastare minacce in rapida evoluzione.

Per i professionisti finanziari e i *Compliance Officer*, integrare l'OSINT nei processi aziendali significa dotarsi di uno strumento versatile per ottemperare in maniera sostanziale a molti obblighi del DORA: ad esempio, poter dimostrare di aver attivato un monitoraggio continuo delle minacce (a supporto del *Risk Management*), o di aver condiviso con il settore indicatori relativi a un incidente (facoltà prevista dal DORA) o ancora di aver valutato i propri fornitori tenendo conto di segnalazioni pubbliche. Dal punto di vista del *business*, l'OSINT aiuta a proteggere la continuità operativa e la reputazione dell'istituto, mitigando i rischi di sorprese provenienti dall'esterno.

Per gli analisti di Intelligence e Cybersecurity, l'OSINT in ambito bancario offre quindi l'opportunità di **elevare la funzione di Cyber Threat Intelligence a pilastro strategico dell'organizzazione**, in sinergia con gli obiettivi di conformità. Gli analisti possono tradurre i dati OSINT in *insight* fruibili dal *Management*, legandoli agli scenari di rischio: in tal modo, l'Intelligence diventa parte integrante del processo decisionale aziendale e non un elemento ancillare.

L'OSINT rappresenta il *trait d'union* tra l'adempimento normativo e la security Intelligence proattiva. Sfruttato appieno, permette alle banche non solo di essere conformi al DORA sulla carta, ma di elevare il proprio livello di difesa e resilienza operativa nella pratica quotidiana. In un contesto in cui gli attacchi possono provenire da qualsiasi angolo del web e diffondersi a macchia d'olio, attingere alla conoscenza collettiva disponibile attraverso le fonti aperte è fondamentale per cercare di essere un passo avanti agli attaccanti. **Come ci ricorda Miguel de Cervantes: "forewarned is forearmed" – essere preavvisati significa essere preparati: il che riassume bene il valore dell'OSINT per il settore bancario e non solo.**

Fonti: Questo white paper ha citato riferimenti chiave tra cui il testo del Regolamento (UE) 2022/2554 (DORA) (Regulation - 2022/2554 - EN - DORA - EUR-Lex) (Regulation - 2022/2554 - EN - DORA - EUR-Lex), documenti ufficiali delle Autorità di vigilanza (ad es. EBA, Regulations and level three documents recently published under the Digital Operational Resilience Act - Lexology), analisi e report dell'ENISA (ENISA Threat landscape: Finance sector) (ENISA Threat landscape: Finance sector), A service architecture for an enhanced Cyber Threat Intelligence capability and its value for the cyber resilience of Financial Market Infrastructures, Guida nazionale TIBER-IT Threat Intelligence Based Ethical Red-Teaming – Italia, nonché contributi da enti indipendenti e aziende di cybersecurity (Beyond Compliance: Achieving Cyber Resilience in the Financial Sector with DORA and TIBER-EU | SANS Institute) (What is OSINT Open Source Intelligence? | CrowdStrike), al fine di garantire accuratezza e aderenza sia al dettato normativo sia alle best practice operative riconosciute. L'auspicio è che i contenuti presentati possano fungere da guida pratica per implementare programmi OSINT efficaci, capaci di contribuire concretamente alla resilienza digitale delle banche in conformità al DORA.