e-REAL®
by LOGOSNET

Cybersecurity



Riservatezza e decisioni sotto attacco

Prevenzione e affiancamento sul campo per studi legali, uffici legali e team compliance

www.e-real.net

Riservatezza e decisioni sotto attacco

Prevenzione e affiancamento sul campo per studi legali, uffici legali e team compliance

Affianchiamo studi legali, uffici legali interni e team compliance esposti ad attacchi informatici, sottrazione di informazioni dei clienti, ricatti e pressioni su chi custodisce dati riservati e decide cosa comunicare. Aiutiamo a mantenere lucidità, proteggere clienti, segreto professionale e reputazione e coordinare la risposta con specialisti tecnici, assicuratori e autorità mentre la situazione evolve.

Prevenire

Affiancamento pratico per verificare istruzioni sospette, proteggere fascicoli e coordinate di pagamento, usare i canali corretti e preparare la risposta.

Affrontare la crisi

Affiancamento sul campo e consulenza in tempo reale per le scelte immediate: cosa dire a clienti, tribunali e autorità, e quando. Disponibili anche per interventi rapidi e d'urgenza, con attivazione all'occorrenza senza preavviso.

Apprendere agendo

Simulazioni realistiche e lavoro sui casi reali per allenare le decisioni su comunicazione, notifica e disclosure sotto pressione.

Far funzionare le protezioni attraverso le persone

Conosciamo il funzionamento dei sistemi di sicurezza e i vincoli che impongono a uno studio o a una direzione legale: gestione documentale, piattaforme di e-discovery, portali clienti, procedure di pagamento. Non li progettiamo: aiutiamo avvocati, praticanti, paralegal e compliance officer a comprenderli, interpretarne le segnalazioni e tradurre le procedure in comportamenti efficaci, anche sotto pressione. Lavoriamo insieme agli specialisti tecnici dello studio o dell'azienda per collegare strumenti, persone e responsabilità.

Le competenze che portiamo sul campo

Un team con esperti di psicologia e comportamento organizzativo, esperti civili e militari di PSYOPS, tra cui ufficiali in congedo delle Forze Armate italiane, avvocati penalisti, criminologi ed esperti ICT.

Formazione e intervento prima e durante la crisi.

CASISTICA

Quando l'attacco interrompe l'attività

Ransomware, fascicoli sottratti, frodi nei pagamenti e minacce di diffusione.



01 Ransomware e fascicoli bloccati

Gestione documentale, posta elettronica e fatturazione diventano indisponibili alla vigilia di una scadenza processuale o di un closing. Clienti, tribunali e controparti chiedono risposte e tempi che il team ancora non possiede.

Il nostro lavoro: definire le priorità, comunicare l'incertezza a clienti e tribunali, distribuire le responsabilità e contenere conflitti e sovraccarico.

02 Dati dei clienti sottratti e ricatto

Una richiesta di denaro si accompagna alla minaccia di pubblicare documenti coperti da segreto professionale e informazioni dei clienti. Paura, urgenza e dovere di riservatezza spingono in direzioni diverse.

Il nostro lavoro: riconoscere la pressione psicologica, verificare i messaggi e sostenere un confronto strutturato tra soci, general counsel, compliance e specialisti ICT, anche su cosa dire ai clienti e quando.

Nelle simulazioni e nei casi reali seguiamo l'evoluzione degli eventi e adattiamo l'affiancamento alle decisioni da prendere.

CASISTICA

Quando il bersaglio è la persona

Impersonificazione, dirottamento dei pagamenti, intimidazione e disinformazione.



03 Una falsa istruzione da un socio o da un cliente

Un'email, una telefonata o una voce contraffatta chiedono di cambiare le coordinate bancarie di una transazione o di un deposito fiduciario, o di consegnare documenti riservati prima di una scadenza.

Il nostro lavoro: riconoscere l'uso di autorità e urgenza, verificare attraverso canali affidabili e gestire il timore di contraddire un socio o un cliente importante.

04 Minacce e attacco alla reputazione

Un socio, un general counsel o un compliance officer riceve intimidazioni mentre circolano documenti manipolati e accuse. Un cliente o un giornalista fa domande. Il gruppo si divide su come reagire.

Il nostro lavoro: valutare le informazioni disponibili, gestire paura e rabbia, concordare messaggi e responsabilità e sostenere la coesione del team.

Le competenze di PSYOPS aiutano a comprendere i meccanismi di influenza e manipolazione e a costruire risposte consapevoli.

DURANTE LA CRISI

Affiancamento mentre gli eventi accadono

Un supporto concreto alle persone che devono decidere e agire.



05 Notifica e comunicazione sotto pressione

Una violazione tocca dati personali e segreti dei clienti. Corrono i termini di GDPR, normative di settore, contratti con i clienti e polizze assicurative, mentre i fatti sono ancora incompleti e legale, compliance e direzione non concordano su cosa dire.

Il nostro lavoro: rendere esplicite priorità e ruoli, ordinare i fatti, sostenere le decisioni su notifiche e comunicazioni a clienti, autorità e assicuratori e curare comunicazioni e passaggi di consegne.

Intervenire e prevenire in modo pratico

Durante la crisi aiutiamo a ordinare le informazioni, chiarire i ruoli e gestire le interazioni difficili. Prima che si verifichi, lavoriamo sulle attività quotidiane: verifica delle istruzioni, protezione dei fascicoli, canali di segnalazione, decisioni da condividere e comportamenti da provare. La formazione-intervento collega apprendimento e azione sul caso concreto.

Dopo la fase critica ricostruiamo quanto accaduto e trasformiamo l'esperienza in pratiche utili per le crisi successive.

IL NOSTRO CONTRIBUTO

Comprendere la minaccia e sostenere chi la affronta

Competenze diverse lavorano sullo stesso caso.

Il team

Esperti di psicologia e comportamento organizzativo

Stress, emozioni, dinamiche di gruppo, conflitti e decisioni nell'incertezza: lavoriamo su ciò che può aiutare o ostacolare la risposta di soci, avvocati e addetti alla compliance.

Esperti civili e militari di PSYOPS

Nel team sono presenti ufficiali in congedo delle Forze Armate italiane. Le competenze nelle operazioni psicologiche aiutano a comprendere influenza, intimidazione, inganno e pressione e a riconoscerne gli effetti.

Avvocati penalisti e criminologi

Contribuiscono alla lettura delle condotte, delle responsabilità e dei doveri professionali, alle scelte di comunicazione e alla comprensione dei rapporti tra vittime, autori delle minacce e altri interlocutori.

Esperti ICT

Conoscono strumenti, sistemi e vincoli operativi. Collegano lo scenario informatico alle decisioni delle persone e collaborano con gli specialisti dello studio o dell'azienda.

Dalla comprensione all'uso efficace dei sistemi

Aiutiamo a capire gli avvisi, usare i canali corretti, applicare le procedure e segnalare le anomalie. È qui che la conoscenza tecnica diventa comportamento e rafforza l'efficacia delle protezioni.

e-REAL by LOGOSNET

OSSERVARE PER MIGLIORARE

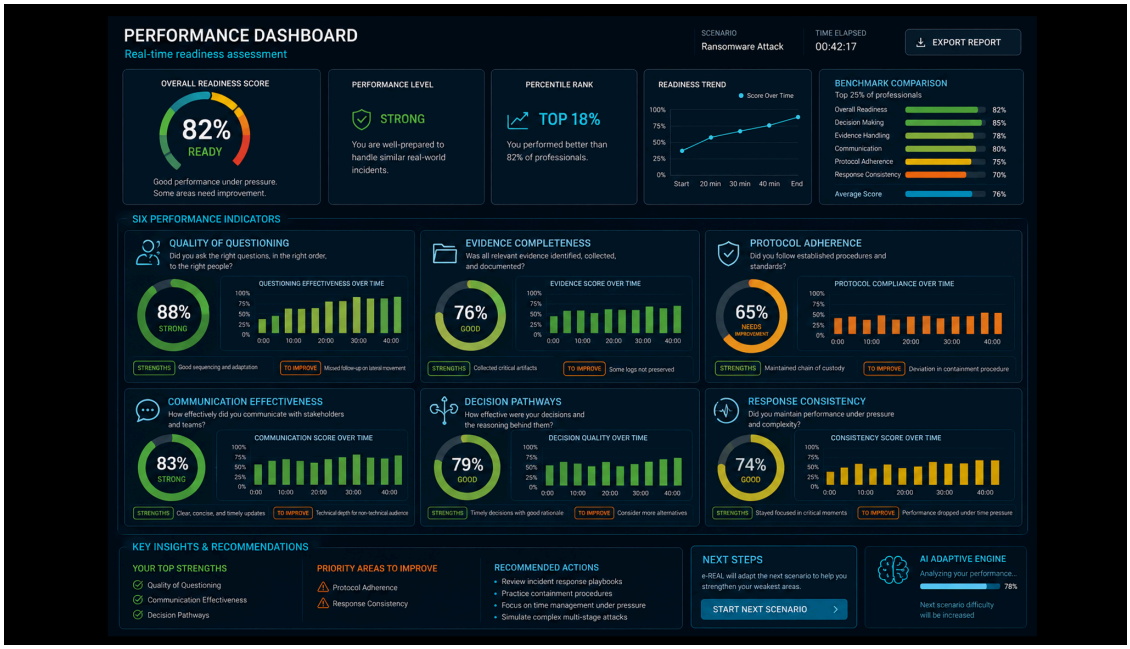
Rendere visibili le capacità e le priorità di sviluppo

Il feedback collega i comportamenti agli episodi della simulazione.

Simulare. Riflettere. Riprovare.

I partecipanti affrontano scenari individuali o di gruppo, interagiscono con avatar conversazionali di IA nei panni di clienti, controparti, autorità e colleghi e ricevono nuovi eventi durante l'esercitazione. Feedback e debriefing aiutano a riconoscere i comportamenti osservati, capire le scelte e sperimentare risposte più efficaci.

Esempio di restituzione dopo la simulazione



Domande, decisioni e comunicazione

Il cruscotto collega gli episodi della simulazione alle aree di prestazione: qualità delle domande, verifica delle informazioni, uso delle procedure, comunicazione con clienti e autorità e coerenza della risposta sotto pressione.

Feedback che aiuta a scegliere il passo successivo

Confrontiamo dialoghi, verifiche e decisioni con gli obiettivi dell'esercitazione. Il debriefing fa emergere punti di forza e priorità concrete per il lavoro quotidiano e per le simulazioni successive.