Codice Etico e di Condotta Professionale

1. La gestione del sapere: Riservatezza e Fiducia: Nel nostro lavoro, maneggiare dati sensibili e scoprire falle critiche è la norma, non l'eccezione. Per questo, la riservatezza per noi non è un modulo da firmare, ma un impegno nel tempo: quello che impariamo durante un mandato resta protetto anche quando il progetto è concluso o il rapporto di lavoro termina.

• Il principio del minimo indispensabile: Ci limitiamo a guardare solo i dati necessari per l'obiettivo tecnico, rispettando la privacy degli utenti finali come se fosse la nostra.

2. Regole d'ingaggio: l'Integrità operativa: Non esiste hacking etico senza un perimetro chiaro e un'autorizzazione scritta.

• Business First: La nostra priorità è che il cliente continui a lavorare. Se un test rischia di causare un denial of service, ci fermiamo e concordiamo insieme ogni passo successivo.

• Pulizia finale: Quando finiamo un intervento, non lasciamo tracce. Account temporanei, shell o script di analisi vengono rimossi sistematicamente. L'obiettivo è lasciare il sistema più sicuro di come l'abbiamo trovato.

3. Gestione delle vulnerabilità: Se troviamo uno Zero-Day o una falla in prodotti di terzi, ci sentiamo custodi della sicurezza di tutti, non solo del nostro cliente.

• Collaborazione, non protagonismo: Informiamo subito il produttore per risolvere il problema. Non ci interessa il titolo sul giornale se questo mette a rischio gli utenti.

• Trasparenza: Se il cliente è in pericolo immediato, la sua protezione è l'unica priorità. Usiamo i canali più veloci e sicuri per metterlo al riparo.

4. Un parere tecnico che sia davvero "terzo": La nostra consulenza deve essere nuda e cruda, basata sui fatti.

• Niente conflitti d'interesse: Se abbiamo partnership con dei vendor, lo diciamo chiaramente. Non consiglieremo mai un software solo per incassare una provvigione se non è la scelta migliore.

• Etica commerciale: Non usiamo la paura per vendere. Non gonfiamo i rischi per piazzare servizi inutili.

5. Con chi scegliamo di lavorare: Abbiamo il diritto e il dovere di scegliere con chi schierarci.

• Il limite dei Diritti Umani: Ci riserviamo di rifiutare incarichi da chi usa la tecnologia per sorveglianza indiscriminata, repressione o per calpestare le libertà fondamentali. La tecnologia deve proteggere le persone, non controllarle.

• Controllo sull'uso duale: Vigiliamo affinché le nostre analisi o i nostri software non finiscano nelle mani sbagliate o non vengano deviati per scopi offensivi.

6. Parlarsi chiaro per proteggere il lavoro In questa azienda non c'è spazio per i "non sapevo" o per i dubbi tenuti nel cassetto. Se vedi qualcosa che non ti torna, a livello tecnico o etico, dillo. Preferiamo una discussione accesa oggi a un problema legale o reputazionale domani. Chi solleva un dubbio o segnala un'irregolarità troverà sempre ascolto e protezione: la nostra forza sta nel saper ammettere dove finisce la tecnica e dove inizia la responsabilità personale.

Firma
BRUNO DI STEFANO (Founder)