FORNITURA DI UN SERVIZIO THREAT INTELLIGENCE BASATO SULLA SOLUZIONE ZEROFOX

1. OGGETTO DELLA FORNITURA

Il presente documento tecnico ha per oggetto la fornitura di un servizio al fine di eseguire attività di raccolta informazioni, incluse quelle provenienti dal deep web, dal dark web e dai social media, in merito a possibili attacchi in grado di mettere a rischio la sicurezza informatica della ASL Roma 2. Inoltre il servizio dovrà dare evidenza degli account aziendali di posta compromessi per i quali sono state rubate le password di accesso al fine di intraprendere contromisure mirate (reset della password di posta/di dominio).
Il servizio di Threat Intelligence basato sulla soluzione ZeroFox è un servizio di sicurezza informatica focalizzato sulla protezione della superficie di attacco esterna (External Attack Surface) e sulla gestione dei rischi digitali (Digital Risk Protection).

2. Funzionalità Chiave del Servizio

- **Dark Web Monitoring:** Tracciamento dei cyber-attivisti, rilevamento di database compromessi, vendita di credenziali aziendali e mercati di Initial Access Brokers.
- **Brand & Domain Protection:** Identificazione e rimozione automatica di siti di phishing che imitano il brand aziendale, profili social fake, applicazioni mobili malevole o campagne di disinformazione.
- **Breach & Extortion Response:** Supporto operativo specializzato e intelligence guidata da agenti infiltrati (DarkOps) in caso di violazioni di dati o tentativi di estorsione.
- **Executive Protection:** Monitoraggio delle minacce digitali rivolte specificamente ai dirigenti VIP (es. furto d'identità, doxxing o minacce alla sicurezza fisica).
- **Global Disruption Network:** Capacità di effettuare "take-down" (rimozioni) automatizzati o gestiti da analisti per abbattere infrastrutture malevole e contenuti abusivi in tempi rapidissimi.

3. QUANTITÀ E DESCRIZIONE DEI SERVIZI

La fornitura dovrà comprendere:
- nr 2 Brand Protection – Foundation
- nr 10 Domain Protection – Foundation
- nr 5 Takedowns - Foundation
- nr 1 OnWatch Alert - Foundation
- Platform API Connector - Foundation
- nr 1 servizio di Intelligence Search
- nr 8 servizi On-Demand Investigations (ODI)

4. DURATA E DECORRENZA DEL SERVIZIO

- Durata contrattuale: 12 mesi
- Modalità di erogazione del servizio: as a service

5. MODALITÀ DI CONSEGNA E COLLAUDO

La consegna si intenderà formalmente eseguita con l'attivazione del servizio.
L' ASL ROMA 2 si riserva un periodo di 5 (cinque) giorni lavorativi dalla data di prima di procedere al verbale di regolare esecuzione.