Checklist Operativa per Analisti CTI - Accesso al Dark Web

1. Preparazione Tecnica

- ☐ Utilizzare una macchina virtuale (es. Kali Linux, Tails) dedicata all'accesso.
- ☐ Connettersi tramite VPN aziendale con crittografia avanzata.
- ☐ Installare e aggiornare il browser Tor da fonti ufficiali.
- ☐ Verificare che antivirus e firewall siano attivi e aggiornati.
- ☐ Disattivare JavaScript nel browser Tor per maggiore sicurezza.

2. Strumenti da Utilizzare

- ☐ Sistema operativo live (es. Tails) per anonimato totale.
- ☐ VPN no-log e affidabile.
- ☐ Browser Tor aggiornato.
- ☐ Email anonime (es. ProtonMail, TutaMail).
- ☐ Strumenti di logging e monitoraggio (SIEM, audit trail).

3. Comportamenti da Evitare

- ☐ Non fornire dati personali o aziendali.
- ☐ Non accedere da dispositivi personali.
- ☐ Non scaricare file o cliccare link non verificati.
- ☐ Non effettuare transazioni o comunicazioni non autorizzate.
- ☐ Non interagire con contenuti illegali o ambigui.

4. Obiettivi di Intelligence

- ☐ Monitorare forum underground e marketplace .onion.
- ☐ Analizzare blog di gruppi ransomware (es. BlackBasta).
- ☐ Raccogliere informazioni su credenziali rubate e accessi venduti.
- ☐ Identificare nuove minacce e tecniche di attacco.
- ☐ Documentare fughe di dati e documenti compromessi.

5. Misure di Sicurezza

- ☐ Registrare ogni sessione di accesso (log, durata, obiettivi).
- ☐ Monitorare le attività tramite strumenti di auditing.
- ☐ Analizzare periodicamente i log per rilevare anomalie.
- ☐ Limitare l'accesso solo a personale autorizzato.
- ☐ Formare il personale sui rischi e sulle tecniche di protezione.

Sezione 6: Preparazione Documentale

- ☐ Definire gli obiettivi dell’accesso prima di iniziare la sessione.
- ☐ Preparare un piano di raccolta dati (target, fonti, tipo di informazioni).
- ☐ Verificare le policy aziendali e normative prima di ogni accesso.
- ☐ Tenere traccia delle fonti consultate per eventuali report o analisi.

Sezione 7: Analisi e Reporting

- ☐ Redigere un report post-sessione con evidenze raccolte.
- ☐ Classificare le informazioni secondo livello di rischio o criticità.
- ☐ Condividere i risultati solo con personale autorizzato.
- ☐ Archiviare i report in repository sicuri e cifrati.

Sezione 8: Comportamento Psicologico ed Etico

- ☐ Mantenere un atteggiamento analitico e distaccato.
- ☐ Evitare coinvolgimenti emotivi o personali.
- ☐ Non interagire con utenti o contenuti provocatori.
- ☐ Rispettare i limiti etici e legali imposti dal ruolo aziendale.

Sezione 9: Revisione e Miglioramento

- ☐ Valutare l'efficacia della sessione e degli strumenti usati.
- ☐ Aggiornare la checklist in base a nuove minacce o tecnologie.
- ☐ Partecipare a sessioni di aggiornamento e simulazioni.
- ☐ Contribuire al miglioramento delle policy aziendali.

N.B. la Checklist è orientativa e non esaustiva