S.No	Problem Statement ID	Problem Statement Name	Domain
22	CT-OSINT - 04	Dark Web / DarkNet / CDR Analysis Tool	OSINT / Threat Intelligence

Description:

The **Dark Web and CDR Analysis Tool** is designed to help investigators uncover links between activities on the Dark Web and call-related data from Call Detail Records (CDRs). The tool leverages OSINT (Open-Source Intelligence) and advanced data analytics to identify connections between suspicious communications, Dark Web transactions, and illegal activities.

By combining insights from the Dark Web with CDR data, investigators can identify patterns, trace networks, and gather actionable intelligence to combat cybercrime, fraud, trafficking, and other illicit activities.

Objectives:

1. **Dark Web Activity Analysis:**
    - Identify and monitor suspicious websites, forums, and transactions on the Dark Web.
2. **CDR Data Correlation:**
    - Analyze call records to find communication patterns, frequency, and geolocation data related to suspicious activities.
3. **Link Analysis:**
    - Connect Dark Web activities with CDR data to uncover hidden networks and individuals involved in illegal operations.
4. **Visual Mapping:**
    - Generate visual maps that show relationships between entities (e.g., phone numbers, IP addresses, and transactions).
5. **Support Investigations:**
    - Provide actionable insights to law enforcement agencies (LEAs) to help solve complex cases involving both digital and physical crimes.

Expectations:

For Hackathon Participants:

1. **Build a Unified Platform:**
    - Create a system that integrates Dark Web monitoring and CDR analysis into a single tool.
2. **Enable Automation:**
    - Automate data collection from the Dark Web and processing of CDRs to save time and enhance efficiency.
3. **Focus on Visualization:**
    - Include features like spider maps, timeline graphs, and relationship diagrams for better data interpretation.
4. **Ensure Data Security:**
    - Handle sensitive data (e.g., CDRs and Dark Web records) securely to prevent misuse.
5. **Develop Search Capabilities:**
    - Include search functionality to trace specific numbers, IP addresses, or keywords across both datasets.

For Law Enforcement Agencies (LEAs):

1. **Enhanced Investigative Capability:**
    - Trace communication patterns and Dark Web transactions linked to crimes like drug trafficking, cyber fraud, or human trafficking.
2. **Real-Time Alerts:**
    - Identify suspicious activities and generate alerts for timely action.
3. **Simplified Analysis:**
    - Correlate large datasets (Dark Web and CDR) efficiently to identify suspects and their networks.
4. **Evidence Generation:**
    - Provide detailed reports for legal proceedings, including visual maps and timeline analyses.
5. **Customizable Reports:**
    - Generate reports tailored to specific cases or investigative needs.

Expected Results:

1. **Uncover Hidden Connections:**
    - Identify links between suspicious phone numbers, IP addresses, and Dark Web activities.
2. **Detect Illegal Activities:**
    - Highlight patterns indicating crimes such as smuggling, cyber fraud, or ransomware payments.
3. **Actionable Insights:**
    - Provide investigators with clear leads to trace and apprehend suspects.
4. **Comprehensive Reporting:**
    - Generate detailed, easy-to-read reports that summarize findings for legal and operational purposes.
5. **Improved Collaboration:**
    - Foster collaboration between different law enforcement units by providing a centralized tool for intelligence analysis.