KOENIG
step forward

Open-Source Intelligence (OSINT)

Duration: 40hrs

Module 1: Introduction to Open-Source Intelligence (OSINT)

- What is OSINT? Scope and Applications
- OSINT vs. Threat Intelligence vs. Reconnaissance
- Ethical and Legal Considerations in OSINT
- OSINT Methodologies and Frameworks (OSINT Framework, IntelTechniques)

Module 2: Setting Up an OSINT Lab

- Configuring a Secure OSINT Environment
- Using Virtual Machines (Kali Linux, Tails, Whonix)
- Privacy and Anonymity Tools (VPNs, Tor, ProxyChains)
- Essential OSINT Browser Extensions and Plugins

Module 3: Search Engine OSINT & Advanced Google Dorking

- Effective Search Engine Techniques (Google, Bing, Yandex, DuckDuckGo)
- Google Hacking Database (GHDB) for Advanced Queries
- Extracting Data from Cached and Archived Pages (Wayback Machine)
- Searching Hidden and Non-Indexed Content

Module 4: Social Media Intelligence (SOCMINT)

- Investigating Social Media Platforms (Facebook, Twitter, LinkedIn, Instagram)
- Extracting Metadata from Posts and Profiles
- Automated Social Media Data Collection
- Analyzing Social Connections and Network Mapping

Module 5: Email and Username OSINT

- Investigating Email Addresses
- Tracing Username Footprints Across Platforms
- Email Header Analysis for Source Tracking
- Identifying Fake or Disposable Email Addresses

Module 6: Website & Domain Intelligence

- WHOIS Lookups and DNS Reconnaissance

- Investigating Subdomains and Server Infrastructure
- Web Technology Fingerprinting (Wappalyzer, WhatWeb)
- Monitoring Website Changes and Leaks (Wayback Machine, Visualping)

Module 7: Dark Web and Deep Web OSINT

- Understanding the Dark Web and Deep Web
- Accessing .onion Sites Securely Using Tor
- Investigating Dark Web Marketplaces and Forums
- Dark Web Search Engines and Information Gathering

Module 8: Geolocation and Image OSINT

- Reverse Image Search Techniques
- Extracting Metadata from Images
- Geolocation Using OpenStreetMap, Google Earth, and Sentinel Hub
- Satellite and Aerial Imagery for OSINT Investigations

Module 9: Video and Audio Analysis in OSINT

- Extracting Metadata from Videos and Audio Files
- Reverse Searching Video Frames
- Identifying Background Noises and Locations from Audio Sources
- Fact-Checking and Verifying Multimedia Content

Module 10: People and Identity Investigations

- Investigating Public Records and Data Breaches
- Tracking Online Identities and Digital Footprints
- Analyzing Behavioral Patterns and Social Engineering Risks
- Gathering Intelligence on Threat Actors

Module 11: OSINT for Cyber Threat Intelligence (CTI)

- Identifying Cyber Threat Actors and Groups
- Monitoring Data Breaches and Leaks
- Investigating Malware and Cybercrime Activities (VirusTotal)
- OSINT for Incident Response and Threat Hunting

Module 12: Reporting and Operational Security (OPSEC) in OSINT

- Organizing and Documenting OSINT Findings

- Creating Actionable OSINT Reports
- Ensuring Investigator Anonymity and OPSEC
- Automating OSINT Collection