# *SC350 OSINT Basics*

**Kurzbeschreibung:**

Im Kurs **SC350 OSINT Basics** vermitteln wir Ihnen die Grundlagen der OSINT-Analyse. In verschiedenen Szenarien erlernen Sie die Methodiken, Arbeitsschemata und benötigten Techniken, um Daten zu identifizieren und in wertvolle Informationen zu transformieren.

Zu den vermittelten Techniken zählen die Einrichtung einer sauberen Arbeitsumgebung, die Bewertung des potenziellen Risikos beim Zugriff auf bestimmte Quellen und der Ableitung von Informationen aus Datenspuren sowie Ihr eigenes System und Datenspuren angemessen gegen die Identifizierung und Analyse durch andere OSINT-Akteure oder Bedrohungsakteure zu schützen.

Dieser Workshop wird von einem Trainer durchgeführt, der über mehrjährige einschlägige OSINT-Erfahrung bei Strafverfolgungsbehörden und LE-Akademien verfügt, insbesondere bei operativen Einheiten, die Cyberkriminalität untersuchen. Er ist führender Experten für die Themen, die er unterrichtet, und hat die OSINT-Tools selbst ausgiebig genutzt sowie Schulungen für Spezialkräfte anderer Cybercrime-Einheiten durchgeführt.

**Zielgruppe:**

Das Training **SC350 OSINT Basics** richtet sich an Einsteiger im Bereich OSINT, Ermittler sowie Mitarbeiter im Bereich der Compliance, Revision, Betrugsermittlung, CTI und Gefahrenabwehr.

**Voraussetzungen:**

Um den Kursinhalten und dem Lerntempo des Trainings **SC350 OSINT Basics** gut folgen zu können, werden keine spezifischen Vorkenntnisse benötigt, jedoch sind grundlegende IT-Kenntnisse hilfreich.

**Sonstiges:**

**Dauer:** 5 Tage

**Preis:** 3450 Euro plus Mwst.

**Ziele:**

Der Workshop vermittelt folgende Kenntnisse und Fähigkeiten:

- systematische und gezielte Beschaffung, Auswertung und Aggregation von Informationen
- Operations Security (OPSEC) zum Schutz der eigenen Identität
- manuelle, toolgestützte und automatisierte Analyse von Daten
- OSINT-Analyse von Metadaten, Nutzernamen, Systemen, Domains, etc.
- Erfahrung in SOCMINT und der Generierung von Sockpuppets

**Inhalte/Agenda:**

- **OPSEC - Einführung in die Operations Security**
  - ◊ Standard Operating Procedures (SOP)
  - ◊ · Overt
    · Covert
    · Clandestine
  - ◊ Browsereinstellungen
  - ◊ Browser-Erweiterungen
  - ◊ VPN-Einrichtung und -Nutzung
  - ◊ Analyse von Verhaltensmustern
  - ◊ Korrelation Fingerprinting

- **Methodik & Arbeitsablauf**
  - ◊ Ermittlungsmethodik
  - ◊ Dokumentation und Berichterstattung
  - ◊ Richtlinien, Ethik

- **VMs Virtuelle Maschinen und ihre Verwendung in OSINT**

- **Suchmaschinen und ihre Verwendung in OSINT**
  - ◊ Übersichten über Suchmaschinen
  - ◊ Suchoperationen und Anpassungen
  - ◊ Bildsuche
  - ◊ Archive und ihr Einsatz in OSINT
  - ◊ Metasuche
  - ◊ FTP-Suchmaschinen
  - ◊ Darknet-Suche

- **Darknet - eine Einführung**
  - ◊ Tor (The Onion Router)
  - ◊ I2P
  - ◊ Web3.0

- **Soziale Netze als Datenquellen**
  - ◊ Facebook
  - ◊ Twitter
  - ◊ Instagram
  - ◊ Online Communities
  - ◊ und andere

- **Datentypen und Analyse**
  - ◊ Bilder
  - ◊ Videos
  - ◊ Benutzernamen
  - ◊ Domänen
  - ◊ IP-Adressen

- **Werkzeuge für die Automatisierung**
  - ◊ Spiderfoot
  - ◊ Maltego
  - ◊ recon-ng
  - ◊ und weitere
  - ◊