SC350 Open Source Intelligence (OSINT) Basics

Kurzbeschreibung:

Teilnehmende erhalten eine praxisnahe Einführung in Open Source Intelligence (OSINT). Vermittelt werden Methodiken, Arbeitsschemata und Techniken zur Identifikation von Daten und deren Umwandlung in Informationen. Behandelt werden Einrichtung einer sicheren Arbeitsumgebung, Risikobewertung beim Zugriff auf Quellen sowie Schutz eigener Systeme und Datenspuren vor Analyse durch Bedrohungsakteure.

Zielgruppe:

Das Training **SC350 Open Source Intelligence (OSINT) Basics** richtet sich an:

- Einsteiger im Bereich OSINT
- Ermittler sowie Mitarbeiter im Bereich der Compliance
- Revision
- Betrugsermittlung
- CTI
- Gefahrenabwehr
- Journalisten
- Behörden
- Mitarbeiter in der IT-Security

Voraussetzungen:

Um den Kursinhalten und dem Lerntempo des Trainings **SC350 Open Source Intelligence (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
- Risiken von öffentlichen Daten erkennen
- Datenlecks identifizieren
- digitale Fußabdrücke für Personen und Unternehmen erstellen
- Awareness von Mitarbeitern

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
    - ♦ ◊