SEC587: Advanced Open-Source Intelligence (OSINT) Gathering and Analysis

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Take a dive more in-depth into finding, collecting, and analyzing information found on the internet
- Debug, understand, alter, and create your own OSINT-focused Python scripts
- Move and pivot around safely on the Dark Web
- Perform financial OSINT investigations

> **"This would be a valuable course for any cybersecurity professional. The subjects and tools in this class are invaluable. I have not seen navigating the Dark Web being taught anywhere else."**
>
> —Mark Styron

SANS SEC587 is an advanced Open-Source Intelligence (OSINT) course for those who already know the foundations of OSINT. The goal is to provide students with more in-depth and technical OSINT knowledge. Students will learn OSINT skills and techniques that law enforcement, intelligence analysts, private investigators, journalists, penetration testers and network defenders use in their investigations.

Open-source intelligence collection and analysis techniques are increasingly useful in a world where more and more information is added to the internet every day. With billions of internet users sharing information on themselves, their organizations, and people and events they have knowledge of, the internet is a resource-rich environment for intelligence collection. SEC587 is designed to teach you how to efficiently utilize this wealth of information for your own investigations.

SEC587 will take your OSINT collection and analysis abilities to the next level, whether you are involved in intelligence analysis, criminal and fraud investigations, or just curious about how to find out more about anything! SEC587 is replete with hands-on exercises, real-world scenarios, and interaction with live internet and dark web data sources.

This course is also blended with all the fundamentals an OSINT analyst will need to learn and understand and apply basic coding in languages such as Python, JSON, and shell utilities as well as interacting with APIs for automating your OSINT processes.

SEC587 students will learn effective OSINT methods and techniques including:

- Structured intelligence analysis
- Rating the reliability of information and its sources
- Researching sensitive and secretive groups
- Practical and Advanced Image and video analysis and verification
- Dark web and criminal underground investigations.
- Operational Security (OPSEC) for OSINT
- Fact-checking and analysis of disinformation and misinformation
- Knowing cryptocurrency fundamentals and tracking
- Using basic coding to facilitate information collection and analysis
- Interacting with APIs for data collection and filtering
- Conducting internet monitoring
- Automation techniques to support OSINT processes

> **"Having a broad coverage over multiple areas of OSINT is really helpful to reinforce the fundamentals and understand the diverse applications of an open source investigator's skills."**
>
> —Dan Black

Section Descriptions

SECTION 1: Disinformation and Coding for OSINT Efficiency

We live in an information age where disinformation is becoming more and more common. In the first section of day 1 students will learn what disinformation is by understanding how disinformation campaigns are set up and deployed. The rest of day one serves as an introduction to coding automation techniques for OSINT and teaches students how to efficiently collect and analyze large quantities of information. The basics of simple scripts are covered, along with simple techniques for manipulating data that has been collected. JavaScript Object Notation (JSON) data is commonly encountered by OSINT analysts and must be appropriately collected, filtered, manipulated, and searched to be leveraged in an investigation.

TOPICS: Detecting and Analyzing Disinformation and Fake News; Using Shell utilities for OSINT Data Collection and Analysis; Determining File and Data Types; Working with Structured and Unstructured Data; Normalization of Data for Analysis; Analyzing Large Sets of Data; Searching and Extracting Specific Data from a Dataset; Understanding and Parsing JavaScript Object Notation Data; Introduction to Application Programming Interfaces (APIs)Stages; Goals of OSINT Collection; Setting Up an OSINT Platform; Documentation; Sock Puppets; Data Analysis

SECTION 3: Sensitive Group Investigations and Video and Image Verification

The beginning of day three is about how to analyze sensitive groups and individuals who identify with groups online. This is becoming increasingly important because many of the targets of OSINT work may be individuals who like to identify themselves within a group or are part of a group. Students will also learn practical and advanced image and video verification techniques.

TOPICS: Use of Unique Identifying Labels (UILs); Identifying Sensitive Groups using UIL Techniques; Investigate and Link Individuals using UILs; Discovering the Nexus of Hate Groups and Victims; Practical and Advanced Image and Video Verification Techniques

SECTION 5: Automated Monitoring and Vehicle Tracking

Day five will start with tools and techniques that will aid OSINT analysts in using and building their own monitoring and online searching tools. This section will teach students how to utilize third-party web-based monitoring tools as well as how to monitor various topics of interest. Students will also learn how to find, gather, and analyze everything that is related to vehicles (cars, boats, planes, trains etc.) using open-source information.

TOPICS: Practical OSINT Monitoring Using Web Services; Automated Internet Monitoring Using Third-Party Tools; Visualization of Data Sets to Support Network Analysis; Collection and Analysis of Open-Source Vehicle Tracking Information

SECTION 2: Intelligence Analysis and Data Analysis with Python

Standard intelligence information analysis techniques and processes for assessing the reliability of information are a key element of intelligence, and application of these techniques to OSINT are discussed. We close off day one with an advanced section on how to analyze gathered OSINT information using several reliability rating and analytic assessment techniques such as Admiralty code, Analysis of Competing Hypothesis and CRAAP analysis. These techniques will help students to make their overall analysis outcome become more solid. Students will also learn how to detect and analyze various forms of disinformation using advanced and structured methodologies and reliability rating systems. Day two will also show students what APIs are and how to access them using various coding languages. We close off day two with an advanced section on how to perform data analysis using Python and Pandas coding.

TOPICS: Understanding Reliability Rating Models for OSINT; Rating the Reliability of Information; U.S. Army OSINT and the Admiralty/NATO System; Currency, Relevance, Authority, Accuracy and Purpose (CRAAP); Standard Intelligence Assessment Techniques; Analysis of Competing Hypotheses (ACH) and Other Methods; Sharing and Organizing Data on GitHub; Fundamentals of the Python Programming Language; Data Collection via API using Python; Data Analysis with Python and Pandas

SECTION 4: Sock Puppets, OPSEC, Dark Web and Cryptocurrency

This day starts off with instruction on useful concepts for creating and maintaining fictitious identities (sock puppets), particularly those used to interact with others, and how to maintain Operations Security (OPSEC). Within SEC587 students will get a more advanced understanding of how OSINT techniques can be applied on the Dark Web by learning about dark web networks. Students will learn techniques for collecting information on the dark web from private groups and underground forums or marketplaces. We will close of this day with an examination of the fundamentals of cryptocurrency, and techniques for tracking public cryptocurrency transactions.

TOPICS: Creating and Maintaining False Personas; Communicating with Targets and Other Sources of Information; Operational Security (OPSEC); Dark Web Basics; Decentralized DNS Systems; Searching for Dark Web Content; Essential Cybercrime Underground Concepts; Underground Marketplaces, Shops and Forums; Creating and Maintaining False Personas; Communicating with Targets and Other Sources of Information; Understanding Cryptocurrency and the Blockchain; Investigating Cryptocurrency Wallets and Transactions

SECTION 6: Capstone: Capture (and Present) the Flags

This will be the capstone for SEC587 that brings together everything that students have learned throughout the course. This will be a team effort where groups compete against each other by collecting OSINT data about live online subjects. The output from this capstone event will be turned in as a deliverable to the client (the instructor and fellow classmates). This hands-on event reinforces what students have practiced during labs and adds the complexity of performing OSINT using Python code and various advanced OSINT techniques under time pressure as a group.

Who Should Attend

- Open-source intelligence and all-source analysts
- Law enforcement investigators
- Military investigators
- Private investigators
- Insurance claims investigators
- Intelligence analysts
- Geopolitical analysts
- Journalists
- Researchers
- Social engineers
- Political and information campaign researchers
- Incident responders
- Digital forensics (DFIR) analysts
- Cyber threat intelligence specialists

> **"I work in CTI and this course is directly related to my and my team's work. Very practical and useful."**
>
> —Stephanie Metka