SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Create an OSINT process
- Conduct OSINT investigations in support of a wide range of customers
- Understand the data collection life cycle
- Create a secure platform for data collection
- Analyze customer collection requirements
- Capture and record data
- Create sock puppet accounts
- Create your own OSINT process
- Harvest web data
- Perform searches for people
- Access social media data
- Assess a remote location using online cameras and maps
- Examine geolocated social media
- Research businesses
- Use government-provided data
- Collect data from the dark web
- Leverage international sites and tools

Course Preview
available at: **sans.org/demo**

Immeasurable amounts of personal, potentially incriminating data are currently stored in the websites, apps, and social media platforms that people access and update via their devices daily. Those data can become evidence for citizens, governments, and businesses to use in solving real financial, employment, and criminal issues with the help of a professional information gatherer.

SEC487 teaches students legitimate and effective ways to find, gather, and analyze these data from the Internet. You'll learn about reliable places to harvest data using manual and automated methods and tools. Once you have the data, we'll show you how to ensure that those data are analyzed, sound, and useful to your investigations.

This is a foundational course in open-source intelligence (OSINT) gathering and, as such, will move quickly through many areas of the field. The course will teach you current, real-world skills, techniques, and tools that law enforcement, private investigators, cyber attackers, and defenders use to scour the massive amount of information across the Internet, analyze the results, and pivot on interesting pieces of data to find other areas for investigation. Our goal is to provide the OSINT knowledge base for students to be successful in their fields whether they are cyber defenders, threat intelligence analysts, private investigators, insurance claims investigators, intelligence analysts, law enforcement personnel, or just someone curious about OSINT.

Throughout the course week, students will participate in numerous hands-on labs using the tools and techniques that are the basis for gathering free data from the Internet. The 20 labs in this course use the live Internet and dark web to help students gain real-world confidence. You'll leave the course knowing not just how to use search features on a website, but all of the scenario-based requirements and OSINT techniques needed to gather truly important OSINT data.

> **"Fantastic introduction to a wide spectrum of OSINT techniques and practices, with great interactive labs and lots of deep dives!"**
>
> — Dave Huffman, **Rockwell Automation**

> **"OSINT is something that I do on a daily basis. All these techniques and considerations will be invaluable."**
>
> — Taylor Bowder, **Duke Power**

Available Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Private Training
sans.org/private-training

Online Training

OnDemand
sans.org/ondemand

Simulcast
sans.org/simulcast

Section Descriptions

SECTION 1: Foundations of OSINT

We begin with the basics and answer the questions "what is OSINT" and "how do people use it." This first section is about level-setting and ensuring that all students understand the background behind what we do in the OSINT field. We also establish the foundation for the rest of the course by learning how to document findings and set up an OSINT platform. The information taught in this section is a key component for the success of an OSINT analyst because without these concepts and processes in place, researchers can get themselves into serious trouble during assessments by inadvertently alerting their targets or improperly collecting data.

TOPICS: Course Introduction; Understanding OSINT; Goals of OSINT Collection; Diving into Collecting; Taking Excellent Notes; Determining Your Threat Profile; Setting up an OSINT Platform; Effective Habits and Process; Leveraging Search Engines

SECTION 2: Gathering, Searching, and Analyzing OSINT

OSINT data collection begins in section two after we get a glimpse of some of the fallacies that could influence our conclusions and recommendations. From this point in the class forward, we examine distinct categories of data and think about what they could mean for our investigations. Retrieving data from the Internet could mean using a web browser to view a page or, as we learn in this section, using command line tools, scripts, and helper applications.

TOPICS: Data Analysis Challenges; Harvesting Web Data; File Metadata Analysis; OSINT Frameworks; Basic Data: Addresses and Phone Numbers; Basic Data: Email Addresses; User Names; Avatars and Reverse Image Searches; Additional Public Data; Creating Sock Puppets

SECTION 3: Social Media, Geolocation, and Imagery

Section three kicks off by examining free and paid choices in people search engines and understanding how to use the data we receive from them. Some of these engines provide social media content in their results. This makes a terrific transition for us to move into social media data, geolocation, and eventually mapping and imagery.

TOPICS: People Search Engines; Exercise in People Searching; Facebook Analysis; LinkedIn Data; Instagram; Twitter Data; Geolocation; Imagery and Maps

SECTION 4: Networks, Government, and Business

Section four focuses on many different but related OSINT issues. This is our blue team day, as we dive into OSINT for IP addresses, domain names, DNS, and Whois. We then move into how to use wireless network information for OSINT. We end the section with two huge modules on searching international government websites for OSINT data and supporting business processes with OSINT.

TOPICS: Whois; IP Addresses; DNS; Finding Online Devices; Wireless Networks; Recon Tool Suites and Frameworks; Government Data; Researching Companies

SECTION 5: The Dark Web and International Issues

The entire morning of section five focuses on understanding and using three of the most popular dark web networks for OSINT purposes. Students will learn why people use Freenet, I2P, and Tor. The first module in the afternoon examines how blue teamers (cyber defenders) can use monitoring to receive alerts when data of interest appear on the Internet. We then shift our focus to data found on "paste" sites. Considering that a big barrier to using non-English websites can be the language, students learn how to use techniques to translate content and search locally for relevant information in our international OSINT section. We leave some time at the end of the section for a massive lab, the "Solo Capture-the-Flag" event, which helps students put together all that they have learned in a semi-guided walk-through that touches on many of the concepts taught throughout the week.

TOPICS: The Surface, Deep, and Dark Webs; The Dark Web; Freenet; I2P - Invisible Internet Project; Tor; Monitoring and Alerting; International Issues; Vehicle Searches; Solo CTF Challenge

SECTION 1: Capstone: Capture (and Present) the Flag

The capstone for the course is a group event that brings together everything that students learned throughout the week. This is not a "canned" Capture-the-Flag event where specific flags are planted and your team must find them. It is a competition where each team will collect specific OSINT data about a certain group of people. The output from this work will be turned in as a "deliverable" to the "client" (the instructor), and then the three teams with the most-complete work will present their research to the class for voting. This multi-hour, hands-on event will reinforce what the students practiced in the Solo CTF the day before and add the complexity of performing OSINT assessments under pressure and in a group.

TOPICS: Capstone Capture-the-Flag Event

Who Should Attend

- Cyber incident responders
- Digital Forensics and Incident Response (DFIR) analysts
- Penetration testers
- Social engineers
- Law enforcement personnel
- Intelligence personnel
- Recruiters
- Private investigators
- Insurance investigators
- Human resources personnel
- Researchers

> **"This course sets up the student with a whole range of OSINT tools that are essential for investigation!"**
>
> — Selvi Krishnan, **Blue Voyant**

> **"Lots of real world tools that will help improve my job."**
>
> — Sean McCormack, **Bridgewater Associates**