SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

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

GOSI
Open Source Intelligence
giac.org/gosi

6	36	Laptop
Day Program	CPEs	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
- 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
- Collect data from the dark web

GOSI
Open Source Intelligence
giac.org/gosi

GIAC Open Source Intelligence

As the first and only non-vendor specific, industry-wide OSINT certification, the GIAC Open Source Intelligence (GOSI) certification represents a huge milestone in the worlds of open source intelligence and cyber reconnaissance. It creates a marker from which students can be recognized for their achievements and competence in the OSINT field of study. Whether they are performing social media analysis of a target or just "fancy googling," the GOSI certification shows they have a strong foundation in OSINT."
— Micah Hoffman, SEC487 Course Author

- Open Source Intelligence Methodologies and Frameworks
- OSINT Data Collection, Analysis, and Reporting
- Harvesting Data from the Dark Web

This is a foundational course in open-source intelligence (OSINT) gathering and, as such, will move quickly through many areas of the field. While the course is an entry point for people wanting to learn about OSINT, the concepts and tools taught are far from basic. The goal is to provide the OSINT groundwork knowledge 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.

Many people think using their favorite Internet search engine is enough to find the data they need and do not realize that most of the Internet is not indexed by search engines. SEC487 teaches students effective methods of finding these data. You will learn real-world skills and techniques that law enforcement, private investigators, cyber attackers, and defenders use to scour the massive amounts of information found on the Internet. Once you have the information, we'll show you how to ensure that it is corroborated, how to analyze what you've gathered, and how to make sure it is useful in your investigations.

With over 25 real-world exercises using the live Internet and dark web to reinforce the course material, and with quizzes and other activities to test knowledge, the SEC487 course does not just provide you materials but also helps you learn them. The course teaches students how to use specific tools and techniques to accomplish their investigative goals, focusing on processes through flow charts that map out procedures for most of the course techniques.

Course Author Statement

"I have always been intrigued by the types and amount of data that are available on the Internet. From researching the best restaurants in a foreign town to watching people via video cameras, it all fascinates me. As the Internet evolved, more high-quality, real-time resources became available and every day was like a holiday, with new and wondrous tools and sites coming online and freely accessible.

"At a certain point, I was no longer in awe of the great resources on the web and, instead, transitioned to being surprised that people would post images of themselves in illegal or compromising positions or that a user profile contained such explicit, detailed content. My wonder shifted to concern for these people. What I found was that, if you looked in the right places, you could find almost anything about a person, a network, or a company. Piecing together seemingly random pieces of data into meaningful stories became my passion and, ultimately, the reason for this course.

"I recognized that the barrier to performing excellent OSINT was not that there was no free data on the Internet. It was that there was too much data on the Internet. The challenge transitioned from 'how do I find something' to 'how do I find only what I need.' This course was born from this need to help others learn the tools and techniques to effectively gather and analyze OSINT data from the Internet."

—Micah Hoffman

"OSINT is something that I do on a daily basis. All these techniques and considerations will be invaluable."

— Taylor Bowder, **Duke Power**

sans.org/sec487

- **Watch a preview of this course**
- **Discover how to take this course: Online, In-Person**

Section Descriptions

SECTION 1: Foundations of OSINT

The first section of the course seeks to get all students speaking the same language and understanding core concepts. We will introduce the common terms and techniques to be used throughout the course. With such a diverse set of students taking the SEC487 course, establishing this common ground for all students is not only useful for discussions but is imperative to move forward. The concepts covered focus on topics students need to examine and prepare for before they begin collecting OSINT data, including discussions about what OSINT is, setting up an OSINT collection platform, how to document and analyze OSINT data objectively, and the use of research accounts and sock puppets.

TOPICS: Overview of OSINT; The Intelligence Process; Creating and Understanding the OSINT Process Stages; Goals of OSINT Collection; Setting Up an OSINT Platform; Documentation; Sock Puppets; Data Analysis

SECTION 2: Core OSINT Skills

In most of their assessments, OSINT investigators perform certain techniques such as querying search engines, analyzing images, and examining files for metadata. These core OSINT skills are the focus for this course section, which flows from finding data to downloading it, analyzing what it means, and then moving back to the Internet to discover other places where it can be found online. Search engines play a large role in the indexing of data on the Internet, and for that reason Section 2 starts with a detailed look at how search engines work and how to use them. Following that, students will learn techniques to retrieve files and web data rapidly and safely through command-line and web-based tools. With a firm understanding of how to gather files and data, students will learn how to analyze image content and extract metadata from those files. This naturally leads the conversation to imagery and mapping sites students can use to examine remote locations, discover video footage that can be used in their work, and geolocation techniques.

TOPICS: Leveraging Search Engines; Harvesting Web Data; File Metadata Analysis; Reverse Image Searching; Image Analysis; Imagery and Maps; Language Translation

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

SECTION 3: People Investigations

Humans generate online data. They post, share photos and videos at certain locations, and discuss topics that may be important in your OSINT investigations. Many investigators focus their entire assessment on what people do and where they do it. For others, human activity may be a smaller portion of their work. Regardless of how often your work focuses on OSINT data about people, Section 3 teaches students the core people investigation skills they need. The flow of Section 3 starts with data about people, such as email addresses and usernames, and turns to how to use those data points to discover user activities. Since these activities are usually discovered in social media platforms, a large portion of Section 3 is devoted to examining social media data.

TOPICS: Email Addresses; Usernames; Avatars and Image Searching; Addresses and Phone Numbers; People Search Engines; Introduction to Social Media; Facebook; Twitter; Geolocation

SECTION 4: Website, Domain, and IP Investigations

Section 4 explores more computer-focused sources of OSINT data and gives investigators the skills to research Internet domains, IP addresses, and websites. This course section reveals new techniques to investigators that mainly focus on human activities and social media. For students with strong skills in information technology and cybersecurity, Section 4 reveals new tools and techniques that will enhance their investigative approaches to domain and website investigations. Since websites are prime targets for OSINT investigators to research, the section begins with an examination of how to research these locations, progresses to discovering data on websites, and finishes by teaching students how to analyze the servers that run the sites. Many websites are tied to domains, so the courseware shifts to techniques to discover the owners of domains and where those domains are registered. Since domains are usually tied to IP addresses, students learn how to research and understand where IP addresses are and how to use them to find online data. Continuing to follow the connected information, IP addresses are tied to computer infrastructure that may be hosting non-website data. Students will learn techniques to research all aspects of a website, from what is displayed on it down to the systems it is hosted on.

TOPICS: Website Investigations; WHOIS; DNS; IP Addresses; Computer Infrastructure; Wireless OSINT

SECTION 5: Business and Dark Web OSINT

The two main topics for Section 5 are business OSINT and the dark web. Students will learn how to take a business name and discover, through official and unofficial sources, who runs the business, where the company does its work, and what people think about that company s brand and reputation. The course section then turns to the dark web. Students will learn how several dark webs work, why people use them, and how to access them in their OSINT investigations. Students will also learn how the Tor dark web network works, what software to use to reach Tor onion services, and how to research data inside Tor. Section 5 continues by showing students how to harvest and interact with online data efficiently using automated websites and tools, then reveals how breach data can be used in OSINT investigations. The end of this section features a massive exercise called the Solo Capture-the-Flag (CTF). This challenge helps students practice the tools and skills they learned in the course in a fun, challenging exercise. Through a semi-guided walkthrough that touches on many of the concepts taught throughout the course, students will work through CTF challenge questions at their own speed. Setting aside time to work through the OSINT processes discussed in class in an organized manner reinforces key concepts and allows students to practice executing OSINT processes, procedures, and techniques.

TOPICS: Business OSINT; Surface, Deep, and Dark Webs; Overview of Several Dark Webs; Tor; OSINT Automation; Breach Data

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

The capstone for SEC487 is a group event that brings together everything that students have learned throughout the course. This is not a canned Capture-the-Flag event where specific flags are planted and teams must find them. It is a competition where each team will collect specific OSINT data about certain live, online targets. The output from this work will be turned in as a deliverable to the client (the instructor and fellow classmates). This multi-hour, hands-on event reinforces what the students practiced in the Solo CTF and adds the complexity of performing OSINT assessments under pressure and in a group.

> **"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**