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

GIAC CERTIFICATIONS

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

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Gather and analyze public data to generate actionable intelligence with advanced OSINT tools and techniques
- Utilize automated systems to streamline the OSINT process, increasing efficiency and accuracy in intelligence gathering
- Identify and mitigate security threats by understanding and applying OSINT to predict and prevent potential vulnerabilities
- Navigate legal and ethical considerations in intelligence gathering to ensure compliance with applicable laws and standards
- Apply OSINT for competitive advantage by monitoring and analyzing market and industry trends to inform business strategy
- Enhance decision-making processes with real-time, data-driven insights from a variety of open and publicly accessible sources
- Implement technological solutions to effectively manage and analyze large datasets from disparate sources, fostering more informed business decisions

Business Takeaways

- Enhance decision-making with actionable insights from public data
- Proactively identify risks using advanced OSINT techniques
- Increase efficiency through automated intelligence gathering
- Stay ahead competitively by monitoring industry and market trends
- Ensure compliance in legal and ethical intelligence collection

> **"This content is the next level for OSINT researchers. It fills in the areas that I have not been using but wanted to learn."**
>
> —Janie Brewer, **Oracle**

Beyond the Basics: Advanced OSINT Techniques

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.

What Is Open-Source Intelligence (OSINT) Automation?

Open-source intelligence automation leverages advanced software tools and algorithms to expedite the collection, analysis, and interpretation of publicly accessible data. By automating the processing of vast amounts of information from sources like social media, news outlets, and databases, it enhances the speed, accuracy, and scalability of intelligence gathering. This technology is crucial for real-time decision-making in fields such as cybersecurity, market analysis, and national security.

Hands-On Advanced OSINT Training

SEC587 offers an immersive experience through practical labs and real-world scenarios, allowing students to master intelligence gathering using publicly available data. This course emphasizes hands-on practice with real-world tools and data, providing guided labs for beginners and more challenging tasks for advanced users, enabling tailored learning at any skill level. Participants will tackle a variety of case studies and simulations that mirror the complex challenges faced by professionals in corporate, security, and governmental fields. The curriculum is designed not only to build a solid foundation in OSINT methodologies but also to instill the ability to ethically and legally apply these skills in professional settings. Students will leave with continued access to course materials and tools, empowering them to further refine their abilities after taking the course.

> **"The course manages to provide both breadth and depth, with practical hands-on practices and tools students can implement right away."**
>
> —Patrick Muprhy, **Palo Alto Networks**

sans.org/sec587

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

Section Descriptions

SECTION 1: Disinformation, Intelligence Analysis and Sensitive Groups

We live in an information age where disinformation is becoming more and more common. In Section 1, students will learn what disinformation is by understanding how disinformation campaigns are set up and deployed. 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 have a section on how to analyze gathered OSINT information using several reliability rating and analytic assessment techniques such as Admiralty code, Analysis of Competing Hypotheses (ACH) and Currency, Relevance, Authority, Accuracy & Purpose (CRAAP) analysis. These techniques will help students to make their overall analysis outcome become more solid. Many of the targets of OSINT work may be individuals who like to identify themselves within a group or as part of a group, so we'll cover how to analyze sensitive groups and individuals who identify with groups online. Students will also learn how to detect and analyze various forms of disinformation using advanced and structured methodologies and reliability rating systems. We'll end the section with an introduction to AI for OSINT.

TOPICS: Detecting and analyzing disinformation and fake news; Understanding reliability rating models for OSINT; Rating the reliability of information; U.S. Army OSINT and the Admiralty/NATO system; CRAAP; Standard intelligence assessment techniques; ACH and other methods; 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; An introduction to AI for OSINT

SECTION 2: Python for OSINT

This content is all new, includes seven new hands-on labs and requires no previous experience! We start off with the building blocks of Python that are most important for OSINT and keep increasing the functionality to perform such tasks as web scraping, all while managing our attribution. We use Python to build an automated intelligence dashboard that updates in real time and can be customized in endless ways. We cover out to utilize third-party APIs including those belonging to AI providers to help us automatically evaluate programs and perform other tasks. Finally, we end the section by covering persistent monitoring of sites like Telegram and Discord, and how we can move our Python code to the cloud using serverless infrastructure like AWS Lamba.

TOPICS: Python fundamentals for OSINT; Web requests and parsing web pages; Managing attribution with Python; Intermediate web scraping; Creating an automated intelligence dashboard; Interacting with APIs, including AI; Persistent Monitoring; Automating your Python code in the cloud

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

SECTION 3: Video and Image Verification, AI for OSINT and Advanced Enumeration

Section 3 starts off with practical and advanced image and video verification techniques utilizing both tools inside the course VM, and cloud based resources. We will then discuss practical ways to incorporate artificial intelligence into their OSINT research as both a means for increasing our efficiency and effectiveness, but also in detecting AI being used by others to generate content. The section ends with advanced enumeration where we cover methods to find domains related to your target, to discover difficult to find infrastructure on websites and in the cloud, and perform 100% passive enumeration on a target website.

TOPICS: Image analysis and reverse image searches; Video analysis; Cloud based video analysis; Prompt Engineering; AI for code review; AI for automating social media accounts; Detecting AI generated content; Automated scans of a website for sensitive files; Discovering cloud based assets; 100% passive enumeration of a website

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 the criminal underground including the initial access marketplaces fed by data stealer logs. Students will learn advanced techniques for finding the true location of servers hosting sites on the dark web as well as automated methods for dark web monitoring. We will close 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); Searching for dark web content; Essential cybercrime underground concepts; Underground marketplaces, shops and forums; Technical methods to de-anonymize dark websites; Understanding cryptocurrency and the blockchain; Investigating cryptocurrency wallets and transactions

SECTION 5: Automated Monitoring, Vehicle Tracking, and Dealing with Password-Protected Files

Section 5 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. We'll cover technical methods to access information in password-protected files encountered online and will also learn how to find, gather, and analyze information that is related to vehicles (cars, boats, planes, etc.) using open-source information. We'll end the day by using automated methods to identify sensitive credentials in various offline and online sources.

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; Methods to access information in password-protected files; Methods to identify sensitive credentials in both offline and online repositories

SECTION 6: Capstone

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.