SEC497: **Practical Open-Source Intelligence (OSINT)**

GOSI
Open Source Intelligence
giac.org/gosi

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Perform a variety of OSINT investigations while practicing good OPSEC
- Create sock puppet accounts
- Locate information on the internet, including some hard-to-find and deleted information
- Locate individuals online and examine their online presence
- Understand and effectively search the dark web
- Create an accurate report of the online infrastructure for cyber defense, merger and acquisition analysis, pen testing, and other critical areas for an organization.
- Use methods that can often reveal who owns a website as well as the other websites that they own or operate
- Understand the different types of breach data available and how they can be used for offensive and defensive purposes
- Effectively gather and utilize social media data
- Understand and use facial recognition and facial comparison engines
- Quickly and easily triage large datasets to learn what they contain
- Identify malicious documents and documents designed to give away your location

Business Takeaways

- Improve the effectiveness, efficiency, and success of OSINT investigations
- Build an OSINT team that can perform a variety of OSINT investigations while practicing good OPSEC
- Create accurate reporting of your organization's online infrastructure
- Understand how breach data can be used for offensive and defensive purposes

SEC497 is a comprehensive training course on Open-Source Intelligence (OSINT) written by an industry professional with over two decades of experience. The course is designed to teach you the most important skills, tools, and methods needed to launch or further refine your investigation skills. SEC497 will provide actionable information to students throughout the OSINT world, including intelligence analysts, law enforcement officials, cyber threat intelligence and cyber defenders, pen testers, investigators, and anyone else who wants to improve their OSINT skills. There is something for everyone, from newcomers to experienced practitioners.

SEC497 focuses on practical techniques that are useful day in and day out. This course is constructed to be accessible for those new to OSINT while providing experienced practitioners with tried-and-true tools that they can add to their arsenal to solve real-world problems. The course has a strong focus on understanding how systems work to facilitate informed decisions, and includes hands-on exercises based on actual scenarios from the government and private sectors. We will discuss cutting-edge research and outlier techniques and not only talk about what is possible, we will practice doing it! Dive into the course syllabus below for a detailed breakdown of the topics covered.

Course Author Statement

"When I started the first open-source intelligence (OSINT) unit for my organization over a decade ago, I was told we had no budget for tools, equipment, or training. I used to joke that one nice thing about not having a budget was that it made many of my decisions very easy. If there was something I needed, I either built it myself or did without.

"Coming from that background forces you to understand how things work and what truly matters. In addition to performing countless OSINT investigations, I've traveled across the world for over a decade teaching operational security (OPSEC) and OSINT to various government agencies and consulted with numerous private companies, ranging from small start-ups to Fortune 100 enterprises. I have helped hunt down international fugitives, identified online infrastructure for a merger and acquisitions due diligence report, and handled numerous tasks in between. This course allows me me share my experience with what works, what does not work, and how we can achieve our goals with minimal effort and cost."

—Matt Edmondson

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

"The module on dealing with large data sets was very helpful. Getting a deep understanding on the challenges large data sets pose and how to work around them is very helpful and practical."

—Jamal Gumbs

Section Descriptions

SECTION 1: OSINT and OPSEC Fundamentals

Before diving into tools and techniques to find, gather, and process information, the course starts with a discussion of how to undertake these activities as safely and effectively as possible. This section begins with an overview of the OSINT process and tips on avoiding analytical pitfalls. We then move into Operational Security or OPSEC. A big part of OSINT is going to new sites and downloading files and information. Creating fictitious accounts (aka sock puppets) has gotten tougher over the past few years, with many sites requiring criteria like a real phone number, facial image, etc. We'll discuss the issues and cover current methods for creating these accounts. The course section wraps up by examining two tools that can improve your organization and efficiency. Hunchly is a fantastic tool for cataloging online research, and Obsidian is an effective open-source tool for note-taking and various other uses. We'll also cover report writing. Many OSINT students have improving Linux skills on their to-do list, so at the end of the section there is an optional lab for Linux command line practice. This gives students who would like to work on these skills the opportunity to do so in a controlled environment.

TOPICS: The OSINT Process; Avoiding Analytical Pitfalls; OPSEC; Dealing with Potential Malware; Canary Tokens; Creating Accounts; Hunchly; Effective Note Taking; Report Writing; Introduction to Linux

SECTION 2: Essential OSINT Skills

Section 2 presents a range of fundamental skills that all OSINT practitioners should have, regardless of the industry they work in. We 'll start with a brief overview of curated lists of OSINT resources and quickly move into understanding the fundamentals of how the web works and utilizing search engines effectively. We'll cover methods to find other sites owned and operated by the same individuals, how to see content that the site owners may not want you to see, and, as always, the OPSEC implications and how to do undertake these tasks safely. We'll also cover the why and how of setting up persistent monitoring alerts. Multiple methods will be presented to archive content from websites, view historical content from websites, and get other sites to visit websites on your behalf. We'll talk about collecting and preserving Internet data and how to convert raw data into useable formats for processing and analysis. We'll discuss how to gather useful intelligence from metadata, even if the data initially appear insignificant or do not appear at all, and look at useful sites for mapping, imagery, and analysis. The course section will then turn to image analysis, with a discussion of methodology, tools that can help us, and some real-world examples. From there, we'll move into facial recognition and real-world examples and resources we can use to find people online. We'll conclude with a discussion about translation resources. At the end of the section there will be an optional capstone. Participants will start off with raw chat logs from a Russian ransomware group and go through the process of converting the logs into a usable format for analysis.

TOPICS: OSINT Link and Bookmark Collections; Web Fundamentals and Search Engines; Web Archives and Proxy Sites; Collecting and Processing Web Data; Metadata; Mapping; Image Analysis and Reverse Image Searches; Facial Recognition; Translations

Who Should Attend

- OSINT investigators
- Cyber threat intelligence analysts
- Intelligence personnel
- Law enforcement
- Penetration testers/Red Team members
- Cyber defenders
- Recruiters
- Journalists
- Investigators
- Digital forensics practitioners
- Human resources personnel

NICE Framework Work Roles

- Data Analyst (OPM 422)
- Threat/Warning Analyst (OPM 141)
- All-Source Analyst (OPM 111)
- Target Network Analyst (OPM 132)
- All Source-Collection Manager (OPM 311)
- All Source-Collection Requirements Manager (OPM 312)
- Cyber Intel Planner (OPM 331)
- Cyber Ops Planner (OPM 332)

SECTION 3: Investigating People

Section 3 of the course focuses on investigating individuals or groups. We'll start by discussing privacy and then get into techniques to research usernames and email addresses across popular sites to discover an individual's accounts. The section then covers how to determine if email addresses are potentially tied to fraud and the places where the individual(s) connected to the email addresses may have been. Many OSINT investigations start with a selector such as a phone number or address and require that the researcher tie that selector to an individual or group. We'll cover numerous resources and techniques you can use to do this, including some that can help identify the owner of a prepaid phone number. The remainder of the section will focus on social media sites, including advanced Facebook searches and ways to see deleted Twitter data and analyze Twitter bots. We'll also cover methods to view content on social media sites when you don't have an account on that site; searching and analyzing alternative social media sites; geolocation of social media data; and trends, sentiment, and reputation.

TOPICS: Privacy; Usernames; Email Addresses; Addresses and Phone Numbers; Introduction to Social Media; Facebook; Twitter; Other Social Media Sites; Geolocation; Trends, Sentiment, and Bots

SECTION 4: Investigating Websites and Infrastructure

Section 4 covers investigating websites, IP addresses, and other infrastructure, including the cloud. For students who don't consider themselves tech savvy, we'll take the time to explain what the elements are and how they work, and we'll provide numerous real-world examples of how these elements have helped in investigations. This course section is critical even for analysts who don't focus on technical topics because understanding how these technical elements work reduces the likelihood of falling down rabbit holes during their research. For students who focus more on technology topics, such as those who work in Cyber Threat Intelligence, we'll cover a variety of tools and resources to learn as much as we can about such topics. This course section is a mix of understanding how things work, studying real-world examples and case studies, looking at some cutting-edge research, and using tools in creative ways to achieve things most people did not know were possible.

TOPICS: IP Addresses; Common Ports; WHOIS; DNS; Certificate Transparency; Email Headers; Subdomains; Technology-Focused Search Engines; Cyber Threat Intelligence; Cloud

SECTION 5: Automation, the Dark Web, and Large Data Sets

Section 5 is a fun mix of topics ranging from researching businesses and transitions to covering wireless for OSINT, including using Wi-Fi names to enrich digital forensics data and research locations. We'll also explore different types of breach data and how it can be used for various OSINT and cyber defender purposes. If you work in OSINT long enough, a giant pile of data will eventually be placed in front of you, and someone will ask you what s in it. Depending on your job, this may already be a regular occurrence. This section will cover how to triage and search large datasets effectively and quickly using free or cheap resources. We'll also take a deep dive into the dark web, covering how it works, how we can find things, and what we can expect to find. We'll examine a case study of breach data hitting the dark web and tricks we can use to speed up dark web downloads. We'll also have a short section on cryptocurrency that mainly focuses on a resource that allows us to track cryptocurrency transactions with a focus on web 3.0 and NFTs. As the course section winds down, we'll talk about different automation options that require no programming. The final portion of the section is called "path forward" and covers a variety of resources that can help you continue your OSINT learning journey.

TOPICS: Researching Businesses; Wireless; Breach Data; Dealing with Large Datasets; Dark Web; Cryptocurrency; Automation; Path Forward

SECTION 6: Capstone: Capture the Flag

The capstone for the SEC497 course is a multi-hour capture the flag event which allows students to work together in small groups to create a threat assessment for a fictional client. Preparing this assessment will require that students use the skills learned throughout the course on a variety of real-world sites. The assessment will be delivered to the client (the instructor), who will provide feedback to each group.

"Business intelligence is a topic near and dear to me and Matt did a fantastic job covering not just the how-tos of collecting and analyzing company data, but also providing the real-world context."

—Sammy Shin