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

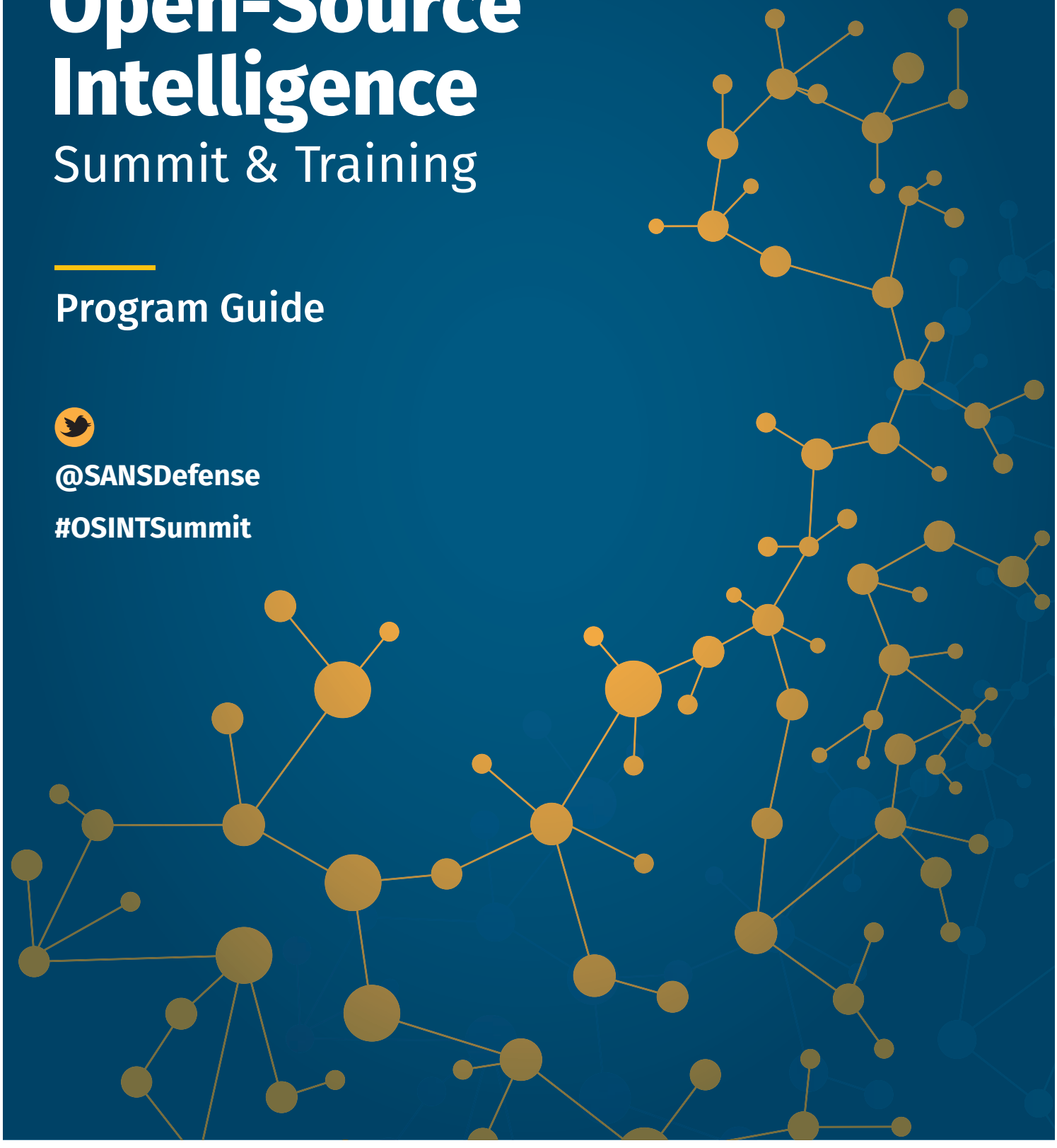
Open-Source Intelligence

Summit & Training

Program Guide

@SANSDefense

#OSINTSummit



Agenda

All Summit Sessions will be held in the The Grand Ballroom (unless noted otherwise).
All approved presentations will be available online following the Summit at ***sans.org/summit-archives***

Tuesday, February 18

7:00-9:00 am	**Registration & Coffee** (LOCATION: GRAND BALLROOM FOYER)
9:00-9:15 am	***Welcome & Opening Remarks*** ***Micah Hoffman*** *@WebBreacher, Summit Chair, SANS Institute*
9:15-10:00 am	***Keynote: The News is OSINT*** The past decade has seen a rise in publicly reported cyber threat activity occurring alongside geopolitical events. By analyzing cyber attacks within the context of current events, we can reveal the potential motives and catalysts that shape the tools and techniques used by state-sponsored, criminal, and hacktivist threat actors. This presentation will first examine how to collect and analyze stories from foreign and domestic news services. Next, we'll cover how to inject news and politics into threat intelligence reporting for a more holistic view of the threat landscape. Finally, we'll present a timeline of some major foreign relations, legal, and political news stories that have coincided with offensive cyber activity by major threat actors. ***Ashley Holtz****, Cyber Threat Intelligence, NBCUniversal*
10:00-10:25 am	**Networking Break** (LOCATION: GRAND BALLROOM FOYER)
10:25-11:00 am	***Connecting the Dots: Using Engagement Metrics on Social Media to Identify Associates*** This presentation will demonstrate how to conduct social network link analysis using engagement metrics such as likes and comments and drawing on two primary techniques on Facebook and Instagram. The first is to look at how to use on-the-fly web-scrapers and simple Excel formulas to build a "true friends list" link diagram for Facebook friends to extract confirmed associates. The second is to look at how to access publicly available Instagram API endpoints and the subsequent JSON data in order to analyze comments of a public user's last 50 posts and calculate "engagement clusters" for those who routinely engage with the user without having to authenticate to Instagram. The takeaways for attendees will include the ability to use a repeatable process and data points to create true link diagrams of confirmed associates or social touch points using both manual techniques and free tools (for efficiencies and reporting). ***Chris Poulter*** *@osintcombine, Director, OSINT Combine*
11:00-11:35 am	***OSINT for Counter Diversion and Brand Protection Investigations*** Reputation, brand integrity and intellectual property are often among the most valuable assets within an organization. This presentation will show how OSINT can and should be used as part of an organization's comprehensive brand protection program. Actual case studies will be used to demonstrate how open-source intelligence can be used to combat diversion and counterfeiting. The presentation will include proactive and reactive strategies for brand protection. Tips for Investigating and managing incidents that impact brand integrity and reputation will also be discussed. ***Heather Honey*** *@H2Osint, President, Haystack Investigations*

Tuesday, February 18

11:35 am – 12:10 pm	***Think Outside the App: An Investigator's Guide to Mobile App OSINT*** Many investigators focus on open-source intelligence from websites and social media accounts but do not fully comprehend the vast amount of such intelligence that can be obtained from mobile apps. This presentation will show how to obtain real-time intelligence from mobile apps that could potentially provide critical evidence for investigators. Attendees will learn how to perform a static and dynamic analysis on mobile apps, understand the evidence available from third parties, capture geolocation information, and pull down social media account information through deep-linking. Of particular interest are mobile apps that are rarely examined, including Uber, Lyft, Grindr, and Tinder. We will also discuss mobile apps associated with counter-terrorism, organized crime, and counter-intelligence. Attendees will learn how to reverse-engineer mobile applications and be provided with an explanation of the underlying code. They'll also learn about important tools that perform a dynamic analysis of mobile apps and their DNS connections, PCAP analysis, and third-party analytics. ***Dr. Darren R. Hayes*** *@CyberOSINT, Associate Professor, Pace University*
12:10-1:30 pm	**Networking Lunch** (LOCATION: GRAND BALLROOM FOYER)
12:10-1:30 pm	SKOPENOW LUNCH & LEARN: ***Using Skopenow to Automate OSINT Practices*** (LOCATION: JEFFERSON) SKOPENOW Join the CEO of Skopenow, Robert Douglas, as he reviews the backend analytics that go into conducting an automated OSINT search. He will also discuss how to build comprehensive digital records anonymously. ***Robert Douglas****, CEO, Skopenow*
1:30-2:05 pm	***Judging by the Cover: Profiling Through Social Media*** While to the rest of the world social media are friendly communication and sharing platforms, for OSINT analysts, social engineers, and attackers, social media are targeting and information harvesting platforms. Even though social media do not always demonstrate our true personalities, they do demonstrate the way we want to be perceived and treated by others. They also "leak" behavioral tendencies and characteristics. This can provide significant intelligence for OSINT practitioners, intelligence analysts, and penetration testers. This talk will cover information-gathering through social media (a sub-discipline of OSINT known as social media intelligence, or SOCMINT) and explain how even seemingly innocent information can be used to manipulate and victimize targets. The presentation will feature a two-part demonstration on how an attacker's mind works when harvesting information on social media. The first part includes real examples of posts that expose vulnerabilities, attract attackers, and ultimately lead to security breaches. The second demonstrates how the information found on a social media profile (from pictures to the words used by the individual) are gathered, categorized into a profiling matrix, and then analyzed, bringing to the surface a highly accurate personality profile. The target's profile can then provide actionable intelligence that enhances the possibility of successful attacks or attack simulations. ***Christina Lekati*** *@ChristinaLekati, Social Engineering Consultant & Trainer, Cyber Risk GmbH*
2:05-2:40 pm	***Real-Time OSINT: Investigating Events as They Happen*** In this presentation, Josh Huff will share his techniques and resources for conducting open-source intelligence analysis on current events as they unfold. OSINT analysis of weather emergencies, missing persons, fugitives, and active shooter events is the type of fast-paced practice that makes you step out of your normal investigative routines. Real-time OSINT will make you a better investigator and may just help you keep your loved ones safe. ***Josh Huff*** *@baywolf88, OSINT Analyst, Learn All the Things*

Tuesday, February 18

2:45-3:15 pm	***Welcome to the (Sock) Jungle*** Sock puppets are essential to every OSINT practitioner who wants to do a deep dive investigation through target engagement or simply just stay off the radar. Creating successful puppets is an art, and the knowledge of creating them is not widely covered as everyone has their own tradecraft for it. This talk will walk you through research-based recommendation for creating sock puppets that can operate effectively over various platforms like forums, chat applications, and markets, with a special focus on social media like FB. ***Zhuang Weiliang*** *@egomy_cs, Lead Consultant, Ensign Info Security*
3:15-3:45 pm	***Networking Break*** (LOCATION: GRAND BALLROOM FOYER)
3:45-4:20 pm	***Using the OSINT Mind-State for Better Online Investigations*** In recent years, public interest in open-source intelligence gathering and analysis has increased exponentially. As this interest has grown, more and more OSINT investigations have been relying on tools and automation, leaving the analysis process behind. In this talk, Nico will show why you should consider OSINT a thought process. The "OSINT state of mind" is key for keeping track of your investigative steps, picking the right tools and sources, analyzing the data, and reporting to generate actionable intelligence. ***Nico Dekens*** *@dutch_osintguy, OSINT Specialist*
4:25-5:00 pm	***Weaponizing the Deep Web*** There's a lot of talk about data breaches but not much is discussed about where the data ends up and how it can be used for good. In this low-key talk, we'll discuss where breach data ends up, how you can find copies of it, and most importantly, how you can use it to further your security goals. We'll discuss how it can benefit blue teams/threat intel shops, pen testers, OSINT researchers and even DFIR practitioners. ***Matt Edmondson*** *@matt0177, Certified Instructor, SANS Institute*
5:00-5:45 pm	***Panel: The OSINTCurio.us Project*** Just over a year ago, several members of the OSINT community created an online learning site focused on solid, actionable OSINT tips, tricks, events, and techniques. This is a diverse group of experts from Cyber Threat Intelligence (CTI) to Private Investigation (PI), cyber penetration testing to cyber defenders who make available regular webcasts/podcasts focused on OSINT, a Google calendar with OSINT events and trainings, and blog about a variety of topics that matter to OSINT investigators and enthusiasts alike. Find out what we've learned from each other since the project's inception, and how you can get involved. Come with questions or ask on Twitter with the #osintcurious hashtag. MODERATOR: ***Micah Hoffman*** *@WebBreacher, Summit Chair, SANS Institute* PANELISTS: ***Nico Dekens*** *@dutch_osintguy, OSINT Specialist* ***Michael James*** *@ginsberg5150* ***Kirby Plessas*** *@kirbstr, Founder & CEO, Plessas Experts Network*
5:45-7:00 pm	**Networking Reception** (LOCATION: GRAND BALLROOM FOYER)

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.