9:00-9:15 am	*Opening Remarks* **Micah Hoffman @WebBreacher, Summit Chair, SANS Institute**
9:15-10:00 am	*Keynote* **So, You Want to OSINT Full-Time** What does it take to turn OSINT into a career? Kirby Plessas, an Army veteran, trained linguist, and DHS-designated "technical expert," regularly consults with intelligence agencies, law enforcement entities, and corporations, teaching them how to leverage open source research. She'll share her experience and wisdom on building your brand and even your own business as an OSINT specialist. If open source intelligence is your passion, Kirby will introduce you to the world of opportunities. **Kirby Plessas @kirbstr, Founder & CEO, Plessas Experts Network, Inc.**
10:00-10:25 am	**Networking Break**
10:25-10:55 am	**OSINT: Breach Data, Ethics, and OpSec... Oh My!** This talk will examine the use of breach data in OSINT investigations. What do breach data look like? Are breach data ethical? How can they be used? What do breach data teach us about privacy and security awareness? What can we do to protect our own data against a breach? Using real-world examples, we'll discuss these questions and provide resources you can use to leverage breach data in your own investigation. **Josh Huff @baywolf88, OSINT Investigator**
10:55-11:00 am	Q&A
11:00-11:30 am	**Backdoors to the Kingdom: Changing the Way You Think about Organizational Reconnaissance** Most current reconnaissance methodologies – such as Domain Name System enumeration, subnet scanning, reliance on Whois Data, and knowledge of owned Autonomous System Numbers (ASNs) or netblocks – are still targeting wells that are drying up or are no longer relevant. The European Union's General Data Protection Regulation has removed access to most Whois data, and moving to the cloud has reduced organizational presence on owned ASNs. But you can still map out an organization if you know where to look. No matter the objective of your team (red, blue, or purple) it's important to know where the security and/or visibility gaps are. We are only here to find things – we'll leave the resolutions/mitigations/code development

	and go-dead workflows to your architecture and application teams. This talk will highlight truly passive reconnaissance utilizing often-overlooked open-source data – all without ever touching a domain. **David Westcott, Security Principal - Threat Hunting, OSINT & Reconnaissance (THOR), iDefense**
11:30-11:35 am	Q&A
11:35 am – 12:05 pm	**From the Mean Streets to the Information Superhighway: Lessons Learned as a Private Investigator** This talk will offer Insights into investigations from the perspective of a cyber analyst with a background as a private investigator. The presentation will draw on years of experience in the field and in front of a keyboard to make connections between the worlds of physical security, "old-school" OSINT, and field investigations of cyber and Internet OSINT. We'll also provide some thoughts on useful investigative processes, techniques, and "gotchas" that may shift your perspective on how to manage and conduct OSINT investigations. **John TerBush @thegumshoo, Senior Threat Intelligence Researcher, Recorded Future**
12:05-12:10 pm	Q&A
12:10-1:30 pm	**Lunch**
1:30-2:00 pm	**Weaponizing OSINT** We need to explore the malicious side of OSINT. As professionals, we should discuss the action of using data against people, see the attacker side, and review the ease of locating information valuable enough to be used against someone. This includes a truly passive attack with no code being launched at the targets, and even getting at the target through passive means. The material involved doesn't have to include data dumps of paid dating or porn sites. Health records, online groups/forums, and even social media might have an effect on a target's future. Now that more data points are surfacing on many different levels, it is more possible to pattern targets. What if a person was profiled? What about a large corporate target's brand? What about people asking for job material or looking for a new career? What would people pay to not have stuff known? In this presentation, we'll investigate embarrassing ways to make sure that the target notices, and we'll also travel down other attack paths. The point of the talk is: Attack to defend. Every case may be different, but we'll look at some basic steps that targets can take to help their online presence. Only by knowing that there is a problem can we defend against it. **@ginsberg5150**
2:00-2:05 pm	

	Q&A
2:05-2:35 pm	**Hunting Down Malicious Sites Using Certstream Data and Available Web Services** A number of automated tools now provide for analytics of new SSL certificate registration to watch for sites that may be spoofing the brands of a company or organization in order to create phishing domains that bypass DMARC, camouflage command and control infrastructure, or undertake other nefarious purposes. In this presentation we will walk through one of these tools – StreamingPhish by Wes Connell – and look at a number of other web-based services that can be used to hunt down possible malicious look-alike sites. **Sean Gallagher @thepacketrat, IT Editor/National Security Editor, ArsTechnica**
2:35-2:40	Q&A
2:40-3:00 pm	**Networking Break**
3:00-3:30 pm	**Getting Started with OSINT Data Collection** Analysts who use open-source Intelligence are usually confined to the tools and websites that have been created by others, without having ways to expand or enrich those data. However, with some knowledge of Python you can build your own tools, or integrate those data with other tools such as Maltego. In this talk, we'll be going over how to scrape websites for data using Python. We'll show you how easy it is to build your own tools and to write scripts that can be used in Maltego to enrich our data. **Brian Warehime @brian_warehime, Manager – Security, Nuna Inc.**
3:30-3:35 pm	Q&A
3:35-4:05 pm	**Beginner's Business and Legal Research** If you were asked to look at a company's 8-K or to find a Writ of Certiorari, would you know what to do? Harness the power of OSINT in this session to learn the basics of finding business and legal information. Get an understanding of the resources available, key terms, and in some cases, what you can actually do with the information you find. Gain insight into research from a former law firm librarian to feel more at ease with these often confusing industries. Users will leave this session with a foundation of where to find business and legal information, terminology, and applications of the knowledge gained. **Tracy Z. Maleeff, Cyber Analyst**
4:05-4:10 pm	Q&A

4:10-4:50 pm	**Using OSINT to Improve Critical Business Decision-Making** Thorough due diligence is a game changer for any organization considering an acquisition, merger, or c-suite hire. It can also be the critical difference between getting a hefty return on an investment versus writing off a loss. In this presentation, we will discuss how organizations should leverage open-source intelligence (OSINT) to identify risks, threats, and opportunities – thereby facilitating well-informed decisions that affect the future of an organization. **Tazz @GRCNinja, Threat Intelligence Advisor, Divine Intel, LLC**
4:50-4:55 pm	Q&A
4:55-5:00 pm	*Closing Remarks*
5:00-6:30 pm	*Networking Reception*

Speaker Biographies

Sean Gallagher @thepacketrat, IT Editor/National Security Editor, ArsTechnica
Sean Gallagher is the IT editor and national security editor at Ars Technica. A University of Wisconsin grad, he wrote his first program in high school on a DEC PDP-10, and his first database app on a dual-floppy Apple II. Sean's first paid writing gig was producing "supplemental content" for Microprose's Gunship 2000 and F-117 Stealth Fighter 2.0 game manuals. A former naval officer, Sean served aboard the USS Iowa (BB-61) and at a river patrol boat squadron— where discovery of his computer skills landed him the assignments of network administrator and computer security officer. Aside from a few dark years as a systems integrator and a stint as Ziff Davis Enterprise's director of IT strategy, Sean has been either in the review lab or on a tech beat for most of the last two decades.

Micah Hoffman @WebBreacher, Summit Chair, SANS Institute
Micah Hoffman has been working in the information technology field since 1998 supporting federal government, commercial, and internal customers in their searches to discover and quantify information security weaknesses within their organizations. He leverages years of hands-on, real-world OSINT, penetration testing, and incident response experience to provide excellent solutions to his customers. Micah is the author of SEC487: Open-Source Intelligence Gathering and Analysis, is a SANS Certified Instructor, and holds GIAC's GMON, GAWN, GWAPT, and GPEN certifications as well as the CISSP. Micah is a highly active member in the cyber security and OSINT communities. When not working, teaching, or learning, Micah can be found hiking on Appalachian Trail or the many park trails in Maryland.

Josh Huff, OSINT Investigator
Josh Huff is an OSINT Analyst in the Finance industry. With a prior background in digital forensics and private investigation he'ss been able to use open source intelligence in a variety of professional applications. Josh blogs his OSINT research at https://www.learnallthethings.net/ and he can be found on Twitter @baywolf88.

Kirby Plessas @kirbstr, Founder & CEO, Plessas Experts Network, Inc.
Kirby Plessas is founder and CEO of Plessas Experts Network, Inc. (PEN), an Open Source Intelligence (OSINT) internet technology and information extraction company specializing in training, researching, and consulting to meet the unique needs of diverse law enforcement, government, and private-sector organizations.
Kirby established herself as one of the foremost tradecraft experts in OSINT through a successful career as a member of the U.S. Military and as a Government Contractor prior to founding PEN in 2008. A service-disabled veteran, Kirby began her career in Military Intelligence as an Arabic linguist supporting the Department of Defense. Upon completion of her Army service, Ms. Plessas applied her Military Intelligence expertise through the use of her OSINT experience at the Defense Intelligence Agency, supporting the warfighter and other Intelligence Community activities. Acknowledged as an expert in her field, in 2007 she was selected to participate and instrumental in the creation and institution of an innovation center for conducting Open Source Intelligence (OSINT). In great tribute to her long list of personal and corporate accomplishments in her field, the Department of Homeland Security declared Kirby Plessas an OSINT Technical Expert (2010).
Through her work at PEN, Kirby shares her love of innovative technology and OSINT expert skill by delivering hands-on training courses throughout the United States and internationally. Presenting at conferences, corporate workshops, and consulting, over the last decade Ms. Plessas has taught social media and Dark Web classes for more than 12,000 members of law enforcement. Supporting several agencies within the U.S. Department of Justice, a major credit card company and other private industry investigator groups with OSINT training, Kirby demonstrates her adaptability and expertise by presenting training workshops that rely heavily upon the live internet instead of a slide deck. Kirby has presented workshops and served as a panel expert at conferences including SXSW Interactive, the Dutch Cyber Crime Conference, the High Technology Crime Investigation Association, National Association for Medicaid Program Integrity, Association of Certified Fraud Examiners, and the International Conference on Transnational Organized Crime.

John TerBush @MagnifOsint, Senior Cyber Threat Analyst, Booz Allen
John TerBush currently works as a senior cyber threat intelligence (CTI) analyst and subject matter expert with consulting firm Booz Allen, serving multi-national enterprises in a variety of industries including finance, manufacturing, retail and energy. In this role he conducts open-source and dark web investigations, malware and traffic analysis, tracking of threat actors and their tactics, techniques and procedures, and many other tasks in order to provide analytical and technical support to clients and other Booz Allen teams. Previous to his role as a CTI analyst, he worked as a security operations center

(SOC) analyst with a large managed security service organization handling response for numerous Fortune 500 companies. While working through a sea of alerts and research, he developed a focus on creating network detections and tracking attacks. His first role in cyber security consisted of conducting vulnerability and security assessments for small- and medium-sized businesses.
Prior to entering the information security field, John worked for over two decades in legal research and private investigations, providing open-source research, surveillance, court testimony, undercover operations and other investigatory work of all types. John acted as the director of investigations and lead investigator for two well-known regional investigation companies for over a decade, before starting his own investigations firm.
John's background as both a private investigator and cyber threat intelligence analyst make him uniquely suited to share a well-rounded perspective on open-source investigations and other forms of research.
John assisted with the development of the SEC487: Open-Source Intelligence Gathering and Analysis course.
He is a member of both the SANS GIAC Advisory Board and the SANS Open Source Intelligence Summit Advisory Board, and holds the GIAC GCIA and GREM certifications as well as the Certified Information Systems Security Professional (CISSP). John is also active within the information security and investigative communities.
John is an avid outdoorsman and when not at work, teaching, or helping out in the community he may be found camping, mountain biking, kayaking or doing other such activities as far from civilization as possible.

Tazz @GRCNinja, Threat Intelligence Advisor, Divine Intel, LLC
Tazz is a security veteran whose technology interests began with Atari and she was amazed when a word processor had enough memory to hold multiple lines. She's been involved with technology since 1997 starting her career in communications, after which she completed her degree. She's had various IT roles and responsibilities over the years to include Field Software (Breaker/Fixer) Engineer, System Administrator of Chaos, IA Hoodlum, Compliance Sorceress, Information Security Cat Herder, Security Architect and is currently a Security Squirrel. She enjoys fitness, horseback riding, weather above 70F, and anything full of laughs and weird people.

Brian Warehime @brian_warehime, Manager – Security, Nuna Inc.
Brian got his start in security during his time in the US Air Force working in the Intelligence Community. After that, he moved on to the commercial side working with various companies doing threat intelligence, security operations, incident response and building tools. Now he is managing a team of security engineers covering all aspects of security for a healthcare company based out of San Francisco. Brian loves building new tools for research when he finds time, and automating OSINT collection through custom scripts and tools, as well as utilizing Maltego.

David Westcott, Security Principal - Threat Hunting, OSINT & Reconnaissance (THOR), iDefense
I find things on the internet.