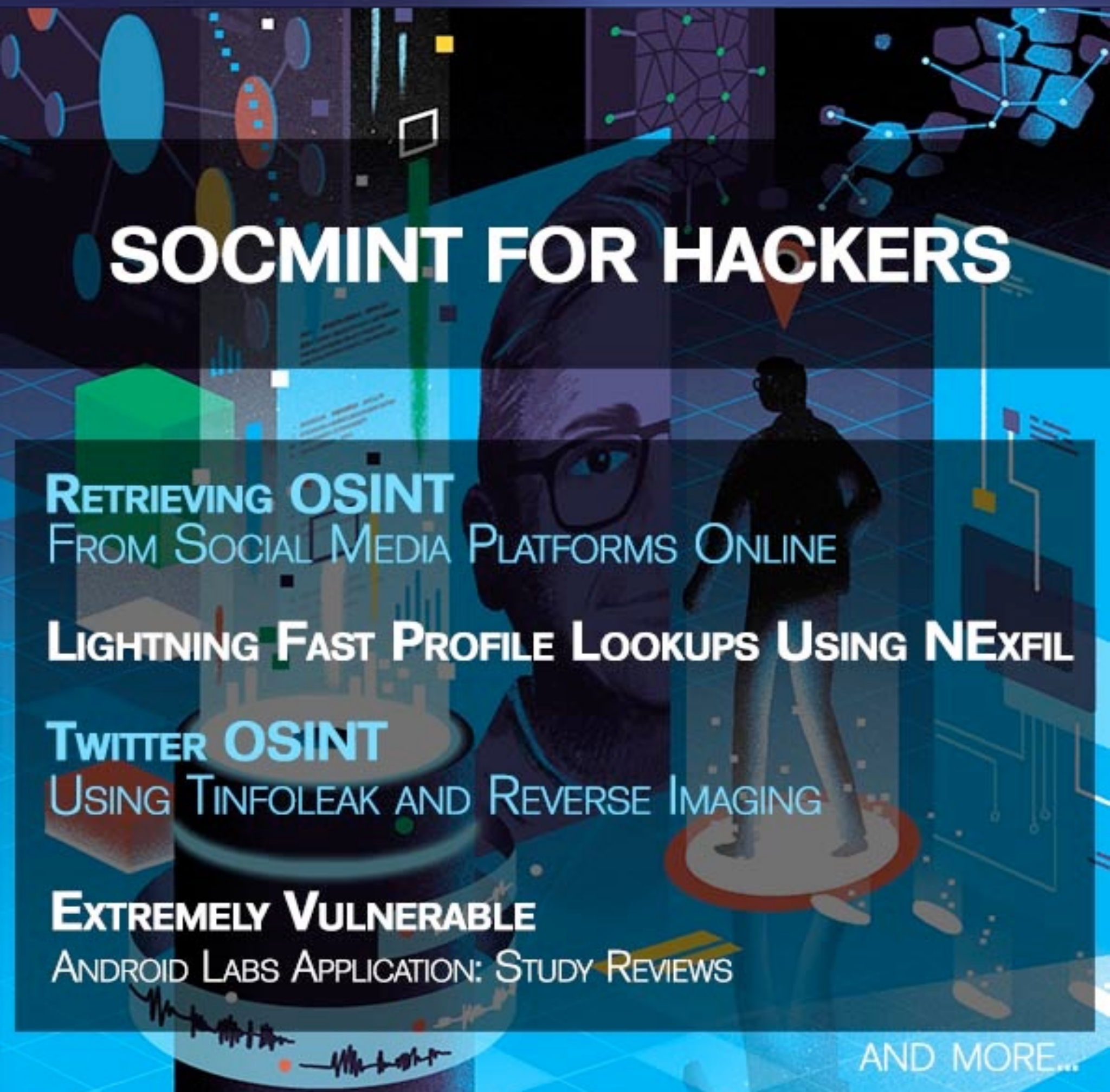
Hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

VOL.16, NO. 05



SOCMINT FOR HACKERS

Retrieving OSINT
From Social Media Platforms Online

Lightning Fast Profile Lookups Using NExfil

Twitter OSINT
Using Tinfoleak and Reverse Imaging

Extremely Vulnerable
Android Labs Application: Study Reviews

AND MORE...

Hakin9

TEAM

Editor-in-Chief
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Editors:

Marta Sienicka
sienicka.marta@hakin9.com

Magdalena Jarzębska
magdalena.jarzebska@software.com.pl

Marta Strzelec
marta.strzelec@eforensicsmag.com

Bartek Adach
bartek.adach@pentestmag.com

Michalina Szpyrka
michalina.szpyrka@eforensicsmag.com

Proofreader:
Lee McKenzie

Senior Consultant/Publisher:
Paweł Marciniak

CEO:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Marketing Director:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

DTP
Magdalena Jarzębska
magdalena.jarzebska@software.com.pl

Cover Design
Hiep Nguyen Duc
Joanna Kretowicz

Publisher
Hakin9 Media Sp. z o.o.
02-676 Warszawa
ul. Bielawska 6/19
Phone: 1 917 338 3631

www.hakin9.org

Betatesters & Proofreaders

Lee McKenzie

Hammad Arshed

Avi Benchimol

Amit Chugh

Kevin Goosie

Craig Thornton

Paul Mellen

Tom Updegrove

Bhuna Selvadurai

Girshel Chokhonelidze

Alex Giles

Gilles Lami

Alexandre D'Hondt

Tahir Saleem

Filipi Pires

Shanika B

Jason Ross

Elia Pinto

Clancey

Dear Readers,

Spring is here for good and so is the newest issue of Hakin9 Magazine! This month we prepared for you various guides and introductions dedicated to one of your favourite topics - SOCMINT for Hackers. Let's take a look at what's inside!

If you are just starting your adventure with OSINT, we recommend you take a look at *Beginner's Friendly Guide to OSINT*, in which you will learn the basics of information mining and some of the most useful OSINT tools.

Then we move to a more advanced topic with *Retrieving OSINT from Social Media Platforms Online; a Detailed Guide and Analysis*, and as the title says, the author will guide you through gathering information on social media platforms, such as Facebook, Twitter, and LinkedIn.

Next, we have *OSINT - Social Media. Gathering Data From Large Social Networks* in which the author presents the use of various OSINT tools on selected examples. Then we drift off to *Twitter OSINT Using Tinfoleak and Reverse Imaging*.

Later on we have *Lightning Fast Profile Lookups Using NExfil* - an introduction to NExfil, a new open source profile lookup that will help you quickly fetch accurate results, with low amount of false positives in a short time. This article is written by the tool creator themselves, Lohitya Pushkar. Then we move to *Mining Information with SpiderFoot* - a detailed guide to SpiderFoot, in which the author presents use cases with hands-on examples.

In *OSINT - Challenges* the author discusses challenges related to OSINT, such as information overload, data rejections, conflicting data, mosaic effect, etc. This article may help those of you that have to face those challenges in your everyday life.

We also prepared articles on other interesting topics that will make your work as an ethical hacker a little bit easier. You may want to take a look at *Majestic Meterpreter* - a research paper in which the authors explain ways and techniques of attack using Meterpreter - or at *Bypass Endpoint Protection of Various Vendors Using TrevorC2* - a guide that demonstrates the bypass to Trend Micro, Sophos, and McAfee endpoint security.

And if you liked our Android Hacking issue, we suggest you take a look at *Extremely Vulnerable Android Labs (EVABS) Application: Study Reviews* - an article that will help you understand the basics and fundamentals on how the android vulnerabilities can be analysed and exploited.

As you can see, this month's issue is packed with guides and tools that may come in handy in your everyday work. We hope you'll find something that suits your needs best! We would also like to send gratitude to our contributors, reviewers and proofreaders, who helped us create this issue!

Stay safe and enjoy!

Hakin9 Editorial Team

Contents

OSINT – CHALLENGES

SYED PEER

The author is a seasoned 20-year IT professional having worked in Fortune 400 companies across diverse verticals from Social Media to Banking to Cyber Security with experience managing Software Development, Engineering and Cyber Security teams.

"Give every man thine ear, but few thy voice:
Take each man's censure, but reserve thy judgment (1.3.74–75)"

– *Hamlet* by William Shakespeare

Introduction

While billions of users across the globe merrily navigate from shopping site to music site to blog post to news app, they leave an indelible trace across the web – an invisible path of breadcrumbs that advertise their associations, comments, likes and dislikes, all of which make their travels all the more transparent and visible to externally interested parties. In fact, a whole industry has evolved (online marketing) for appeasing their appetite for fancy goods and cheap food and everything in between.

This albeit public information trail now forms the basis of a whole new science for discovery: "Open Source Intelligence" or "OSINT" for short. This technology trend uses publicly available and "open" sources of information rather than having to depend on any covert operations to exfiltrate data. No teams of hackers or Trojan horse malware is required.

Relying solely on the internet, never before in our storied history has so much valuable information been made available willingly online by government agencies, corporations, nonprofits and common users. One now has the means to easily tap into this information vault for perusal or profits.

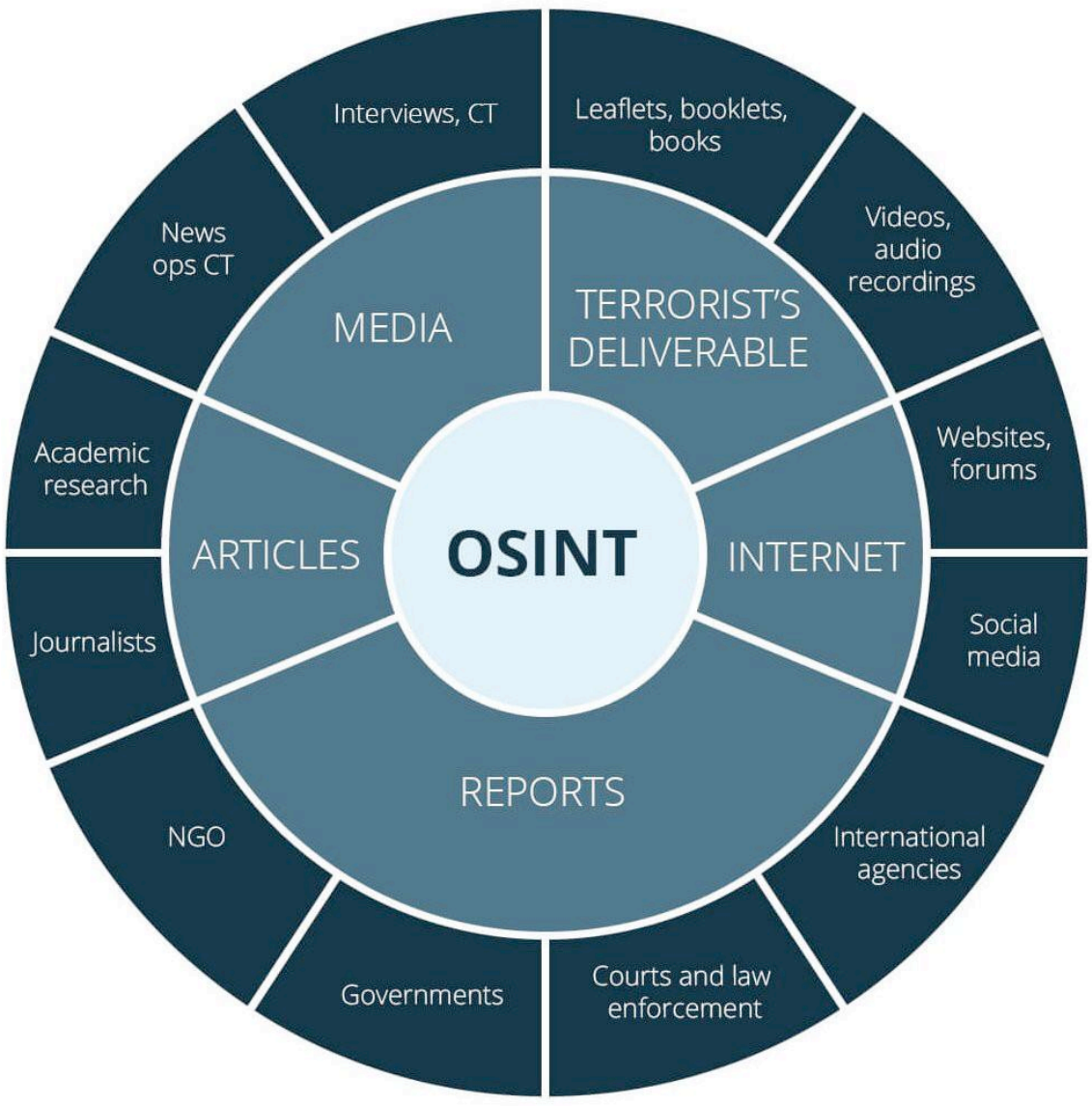
Open Source Intelligence Definition

As defined by Wikipedia:

"Open-source intelligence (OSINT) is a multi-factor (qualitative, quantitative) methodology for collecting, analyzing and making decisions about data accessible in publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources."

OSINT Sources

Although methods used for gathering information have a history of hundreds of years, and especially so for military campaigns, the recent digital revolution and searchable web have made OSINT the "go to" trend for easy and quick results. OSINT relies heavily on a range of different information sources as shown in the figure below.



Courtesy DataDriverInvestor

Easy information accessibility brings with it the monumental effort involved in aggregating all this data and trying to make sense of what it all means to the data scientist or cyber security analyst. No simple feat by any means.

Publicly Available Information

As OSINT relies so heavily on information that is publicly available, it may be helpful for readers to understand what all constitutes the same.

The Department of Defense Manual 5240.01 (August 2016) defines publicly available information as the following:

☑ Is published or broadcast for public consumption

☑ Is available on request to the public

☑ Is accessible online or otherwise to the public

☑ Is available to the public by subscription or purchase

☑ Is made available at a meeting open to the public

☑ Is obtained by visiting any place or attending any event that is open to the public

☑ Is any information that could be seen or heard by any casual observer

In short, if an individual can access a piece of information without doing anything illegal, it may be reasonably classified as "publicly available".

OSINT Challenges

Every organization needs to look before they leap into OSINT; though it has many advantages, there are some challenges that need to be addressed. Choosing to ignore these challenges will make the OSINT effort harder, longer, costlier and potentially less productive.

The following outline of OSINT challenges may be helpful:

1. **Data Sources:** As OSINT is reliant on publicly available websites, both the selection of sources and the intent behind those choices can add potential bias to the final results. This will mean that data samples extracted and analysis done on that basis may be both misleading and troublesome to defend at a later stage. The results may smack of "curve fitting" simply to arrive at a foregone conclusion. Much will hang on the burden of proof in such cases and publicly available data can be easily refuted by taking (and sourcing) from other locations on the web with contrary opinion based on data alone. This battle rages on but the problem is real.

2. **Information Overload & Filtering**: The availability of readily accessible information means that there is a danger of "*information overload*" to put it mildly. The sheer volume of data extracted and the quality required of it requires that a strict regime needs to be enforced to filter data appropriately, otherwise any number of *false positives* may be drawn out of the bag.

Any content filters applied need to be reviewed judiciously and regularly to ensure that the highest quality data is being primed. This may require additional staff hiring or training for team members for identifying the right data elements and approach. That may entail some additional costs to the organization for the process to be successful.

Successful OSINT requires good data sources, being primed by skilled data science/cyber analysts, and employing the correct filters and approach.

3. **Data Rejections**: In the search for quality information from disparate sources (websites) and voluminous inventories, content filtering will inevitably create additional volumes of "*rejections*" from invalid data. Consequently, the manual efforts required for aggregating, processing and delivering pertinent results by "separating out the chaff from the wheat" will also increase and may put a considerable strain on staffing levels for smaller teams of analysts. All this needs to be factored in at the beginning before building out OSINT teams.

4. **Data Unclassified but Detrimental**: The fact that so much information is drawn from different sources, "unclassified" data is available in its "*raw*" form. This means that drawing results out of the same may in some cases potentially be harmful to individuals or groups under investigation. The inability to reconnoiter with the sources makes it doubly difficult at times to take information at face value as so much can be misinterpreted and lead to false accusations. In OSINT efforts to identify the "critical" data of relevance, there may be legal consequences of drawing out the wrong conclusions.

5. **Conflicting or Overlapping Data:** OSINT will often lead to a process of aggregating and processing numerous disparate intelligence sources. These may be Geo-Spatial Intelligence (GEOINT), Measurement and Signature Intelligence (MASINT), Human Intelligence (HUMINT), and Signal Intelligence (SIGINT).

Information garnered from social media outlets would fall under Human Intelligence (HUMINT) but aircraft and vessel travel plans and itineraries abroad to hostile nations may come under Geo-Spatial (GEOINT) whilst unauthorized communications with foreign bad actors should fall squarely in Signal Intelligence (SIGINT). Having a means to see the "big picture" and to consolidate all the different intelligence sources into meaningful traction and results for the investigation is a key skill that a Cyber Security Manager needs to exercise from the get go.

6. **Automation / AI & Machine Learning**: With the volumes of data to be trawled and processed, the use of automation tools such as Artificial Intelligence (AI) and Machine Learning (ML) are obvious use case candidates.

Artificial Intelligence (AI) has made huge strides into the cyber defense arena, often taking the world by storm in its many use cases and efficiency in processing huge amounts of data discreetly, accurately and cleanly. All monitoring measures implemented within any organization generate a huge number of extracted data logs, and the endless stream of transactional time stamped data can be the last straw on the camel's back (figuratively) for OSINT Security teams. Although the data trawled can be voluminous, AI and Machine Learning enabled systems can help to filter out much of the signal noise and identify the subject behavior as per initial requirements. This can help to reduce the number of serious data errors and *false positives*.

Even though we all recognize the benefits that AI and ML brings to table it is still very important that skilled cyber analysts review the resulting data to ask the detrimental questions that may still invalidate the data results.

7. **Mosaic Effect**: During OSINT research one dataset may get delisted as irrelevant but then get re-enlisted with another dataset to draw an assumption or conclusion. The more datasets combined in this way leads to potential abuse in identify-

ing individuals or groups under scrutiny. This is widely known as the "mosaic effect" and one needs to be extra cautious in using these types of connections before releasing potentially damaging information against individuals or groups.

Conclusion

As we entered into a new 21st century over two decades ago, we were unknowingly at the cusp of a digital tsunami headed our way that would redefine our understanding of *War and Peace* and *Friend or Foe*. New "*virtual threats*" arose more dangerous than the physical ones that we were ill prepared for, having practiced for generations to rebuff physical brute force attacks with military, navy and air defenses. To face the modern threats, we have had to re-engineer and re-invent our intelligence services themselves by taking advantage of open sources of data and information.

With the plethora of OSINT recon and intel gathering tools available currently for the security analyst, OSINT provides a treasure trove of information without unnecessary surveillance and targeted attack vectors being used. AI and ML can help to an extent but not entirely. With so much information to review we must be judicious both in information handling and publishing our results. When researching individuals and groups we must always remember that we are all so much more than the sum of our parts. We all encapsulate the desires of our generation, the history of our lineage and ancestry and bias of our convictions and politics.

With OSINT, the aggregated information does not necessarily define us, but assumptions and conclusions drawn from it, correct or otherwise, often do.

References:

1. Wikipedia Definition: https://en.wikipedia.org/wiki/Open-source_intelligence

2. Top 5 OSINT Challenges: https://www.knowledgenile.com/blogs/osint-challenges/

3. Responsible Data: https://responsibledata.io/2016/11/14/responsible-data-open-source-intelligence/