Open Source Intelligence Osint Investigation Training

CHEN EATON

Critical Infrastructure Security and Resilience Jeffrey Frank Jones
The skills and tools for collecting, verifying and correlating information from different types of systems is an essential skill when tracking down hackers. This book explores Open Source Intelligence Gathering (OSINT) inside out from multiple perspectives, including those of hackers and seasoned intelligence experts. OSINT refers to the techniques and tools required to harvest publicly available data concerning a person or an organization. With several years of experience of tracking hackers with OSINT, the author whips up a classical plot-line involving a hunt for a threat actor. While taking the audience through the thrilling investigative drama, the author immerses the audience with in-depth knowledge of state-of-the-art OSINT tools and techniques. Technical users will want a basic understanding of the Linux command line in order to follow the examples. But a person with no Linux or programming experience can still gain a lot from this book through the commentaries. This book's unique digital investigation proposition is a combination of story-telling, tutorials, and case studies. The book explores digital investigation from multiple angles: Through the eyes of the author who has several years of experience in the subject. Through the mind of the hacker who collects massive amounts of data from multiple online sources to identify targets as well as ways to hit the targets. Through the eyes of industry leaders. This book is ideal for: Investigation professionals, forensic analysts, and CISO/CIO and other executives wanting to understand the mindset of a hacker and how seemingly harmless information can be used to target their organization. Security analysts, forensic investigators, and SOC teams looking for new approaches on digital investigations from the perspective of collecting and parsing publicly available information. CISOs and defense teams will find this book useful because it takes the perspective of infiltrating an organization from the mindset of a hacker. The commentary provided by outside experts will also provide them with ideas to further protect their organization's data.
OSINT Ninja John Wiley & Sons
This book presents the latest trends in attacks and protection methods of Critical Infrastructures. It describes original research models and applied solutions for protecting major emerging threats in Critical Infrastructures and their underlying networks. It presents a number of emerging endeavors, from newly adopted technical expertise in industrial security to efficient modeling and implementation of attacks and relevant security measures in industrial control systems; including advancements in hardware and services security, interdependency networks, risk analysis, and control systems security along with their underlying protocols. Novel attacks against Critical Infrastructures (CI) demand novel security solutions. Simply adding more of what is done already (e.g. more thorough risk assessments, more expensive Intrusion Prevention/Detection Systems, more efficient firewalls, etc.) is simply not enough against threats and attacks that seem to have evolved beyond modern analyses and protection methods. The knowledge presented here will help Critical Infrastructure authorities, security officers, Industrial Control Systems (ICS) personnel and relevant researchers to (i)

get acquainted with advancements in the field, (ii) integrate security research into their industrial or research work, (iii) evolve current practices in modeling and analyzing Critical Infrastructures, and (iv) moderate potential crises and emergencies influencing or emerging from Critical Infrastructures.

Open Source Intelligence Investigation Springer

Learn to gather and analyze publicly available data for your intelligence needs In Deep Dive: Exploring the Real-world Value of Open Source Intelligence, veteran open-source intelligence analyst Rae Baker explains how to use publicly available data to advance your investigative OSINT skills and how your adversaries are most likely to use publicly accessible data against you. The author delivers an authoritative introduction to the tradecraft utilized by open-source intelligence gathering specialists while offering real-life cases that highlight and underline the data collection and analysis processes and strategies you can implement immediately while hunting for open-source info. In addition to a wide breadth of essential OSINT subjects, you'll also find detailed discussions on ethics, traditional OSINT topics like subject intelligence, organizational intelligence, image analysis, and more niche topics like maritime and IOT. The book includes: Practical tips for new and intermediate analysts looking for concrete intelligence-gathering strategies Methods for data analysis and collection relevant to today's dynamic intelligence environment Tools for protecting your own data and information against bad actors and potential adversaries An essential resource for new intelligence analysts, Deep Dive: Exploring the Real-world Value of Open Source Intelligence is also a must-read for early-career and intermediate analysts, as well as intelligence teams seeking to improve the skills of their newest team members.

Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise Apress

Introducing "OSINT Tactics and Tools: Maximizing Intelligence in the Digital Age" by Ethan Hughes - a comprehensive guide that equips readers with the essential knowledge and practical skills to excel in the world of Open Source Intelligence (OSINT). In today's digital landscape, where information is abundant and easily accessible, OSINT has emerged as a powerful tool for gathering intelligence from publicly available sources. From law enforcement agencies and intelligence organizations to corporate investigators and individuals concerned about their personal privacy, OSINT is invaluable for maximizing intelligence in diverse domains. With a wealth of experience in the field, Ethan Hughes takes readers on a captivating journey through the world of OSINT, unraveling its intricacies and empowering them to harness its potential. This book serves as an authoritative resource, combining theoretical insights with hands-on techniques and tools that amplify the effectiveness of OSINT investigations. The book begins by laying a solid foundation in Chapter 1, "Introduction to OSINT: Understanding Open Source Intelligence." It elucidates the fundamental concepts of OSINT and establishes its significance in the digital age. From there, readers embark on an enlightening exploration of various topics, each meticulously crafted into comprehensive chapters. Throughout the book, readers gain a deep understanding of ethical considerations in OSINT, legal boundaries, and privacy concerns. They learn to navigate the digital landscape with finesse, employing advanced search techniques, harnessing the power of social media, and extracting valuable data through web scraping and data extraction techniques. The book also delves into the intriguing world of the deep web and dark web, shedding light on their distinctive characteristics, investigations, and the challenges they present. It uncovers the techniques for conducting OSINT investigations on these hidden realms, equipping readers with the skills to uncover hidden information and track illicit activities. Furthermore, the author explores OSINT applications in diverse domains, such as digital forensics, threat intelligence, corporate investigations, and law enforcement operations. Real-world case studies and practical examples bring the concepts to life, enabling readers to grasp their application in different scenarios. An emphasis on critical thinking, analysis, and verification runs as a common thread throughout the book, enabling readers to evaluate the reliability and credibility of sources. They learn to cross-reference and verify OSINT data, ensuring the accuracy of their intelligence findings. The book culminates in Chapter 12, "OSINT for Personal Privacy and Security," where readers gain invaluable insights into protecting personal information in the digital age. They discover strategies to counter OSINT techniques used against individuals and safeguard their digital privacy, empowering them to take control of their personal information. Written in a clear, concise, and accessible manner, "OSINT Tactics and Tools: Maximizing Intelligence in the Digital Age" caters to both beginners and seasoned professionals in the field of OSINT. Its comprehensive coverage, practical insights, and expert guidance make it an indispensable resource for anyone seeking to enhance their intelligence-gathering capabilities. With Ethan Hughes as their trusted guide, readers embark on a transformative journey, mastering the art of OSINT and unlocking its potential to maximize intelligence in the digital age. This book is an essential companion for individuals, professionals, and organizations seeking to thrive in an era where information is power.

Open Source Intelligence in the Twenty-First Century Independently Published

In the information age, it is critical that we understand the implications and exposure of the activities and data documented on the Internet. Improved efficiencies and the added capabilities of instant communication, high-speed connectivity to browsers, search engines, websites, databases, indexing, searching and analytical applications have made

Options for Strengthening All-Source Intelligence Syngress

Over 1,600 total pages ... CONTENTS: AN OPEN SOURCE APPROACH TO SOCIAL MEDIA DATA GATHERING Open Source Intelligence – Doctrine's Neglected Child (Unclassified) Aggregation Techniques to Characterize Social Networks Open Source Intelligence (OSINT): Issues for Congress A BURNING NEED TO KNOW: THE USE OF OPEN SOURCE INTELLIGENCE IN THE FIRE SERVICE Balancing Social Media with Operations Security (OPSEC) in the 21st Century Sailing the Sea of OSINT in the Information Age Social Media: Valuable Tools in Today's Operational Environment ENHANCING A WEB CRAWLER WITH ARABIC SEARCH CAPABILITY UTILIZING SOCIAL MEDIA TO FURTHER THE NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE THE WHO, WHAT AND HOW OF SOCIAL MEDIA EXPLOITATION FOR A COMBATANT COMMANDER Open Source Cybersecurity for the 21st Century UNAUTHORIZED DISCLOSURE: CAN BEHAVIORAL INDICATORS HELP PREDICT WHO WILL COMMIT UNAUTHORIZED DISCLOSURE OF CLASSIFIED NATIONAL SECURITY INFORMATION? ATP 2-22.9 Open-Source Intelligence NTTP 3-13.3M OPERATIONS SECURITY (OPSEC) FM 2-22.3 HUMAN INTELLIGENCE COLLECTOR OPERATIONS

OSINT Essentials Taylor & Francis

Are you ready to take your Open Source Intelligence (OSINT) skills to the next level and become an OSINT Ninja? In this comprehensive guide, renowned OSINT expert Elias Chaput equips you with the knowledge and tools needed to excel in the world of intelligence gathering using open sources. As technology evolves, so do the methods of information collection. OSINT has emerged as a critical discipline in various fields, including cybersecurity, law enforcement, journalism, and business intelligence. This book serves as your ultimate resource to harness the power of OSINT and gain a competitive edge in your field. Unleashing Advanced Techniques: Discover advanced OSINT techniques that go beyond basic searches and explore the vast world of open-source information. From deep web mining to geospatial OSINT and social media intelligence, this book covers it all. Learn how to leverage powerful tools and APIs, master search operators, and employ automation for more effective and efficient intelligence gathering. Protecting Privacy and Security: In the digital age, safeguarding privacy and maintaining security are paramount. OSINT Ninja not only empowers you to extract valuable information but also educates you on ethical practices and privacy considerations. Learn how to handle sensitive data responsibly, minimize personal digital footprints, and protect yourself during investigations. Real-World Applications: OSINT Ninja is not just a theoretical guide; it delves into real-world case studies and applications. Gain insights into how OSINT is used in law enforcement to identify suspects, track missing persons, and investigate cybercrimes. Explore how journalists leverage OSINT for fact-checking, source verification, and in-depth investigative reporting. Understand how businesses use OSINT for competitor analysis, market research, and brand monitoring. Tackling Challenges and Limitations: Every intelligence gathering endeavor comes with challenges and limitations. OSINT Ninja equips you with the strategies to navigate these obstacles and overcome the limitations of open-source information. Learn to identify and combat misinformation, detect fake accounts and disinformation campaigns, and handle information exposure and doxing incidents. Your Journey as an OSINT Ninja: This book is designed to be your comprehensive guide, catering to all levels of expertise. Whether you are a beginner looking to build a solid foundation or an experienced OSINT practitioner seeking advanced techniques, OSINT Ninja has something to offer. Why Choose OSINT Ninja? Detailed coverage of advanced OSINT techniques and tools for a holistic understanding. Emphasis on ethical practices, privacy protection, and responsible data handling. Real-world case studies and applications across various domains. Insightful guidance to tackle challenges and limitations in OSINT investigations. Written by a leading expert in the field, Elias Chaput, with years of practical experience. Unlock the potential of OSINT and become a master intelligence gatherer with OSINT Ninja. Elevate your skills, enhance your investigations, and contribute to a safer, more informed world. Whether you are a cybersecurity professional, a journalist, a business analyst, or a law enforcement officer, this book is your gateway to becoming an OSINT Ninja. Are you ready to embark on this thrilling journey?

Hacking Web Intelligence Springer

Open source intelligence (OSINT) and web reconnaissance are rich topics for infosec professionals looking for the best ways to sift through the abundance of information widely available online. In many cases, the first stage of any security assessment—that is, reconnaissance—is not given enough attention by security professionals, hackers, and penetration testers. Often, the information openly present is as critical as the confidential data. Hacking Web Intelligence shows you how to dig into the Web and uncover the information many don't even know exists. The book takes a holistic approach that is not only about using tools to find information online but also how to link all the information and transform it into presentable and actionable intelligence. You will also learn how to secure your information online to prevent it being discovered by these reconnaissance methods. Hacking Web Intelligence is an in-depth technical reference covering the methods and techniques you need to unearth open source information from the Internet and utilize it for the purpose of targeted attack during a security assessment. This book will introduce you to many new and leading-edge reconnaissance, information gathering, and open source intelligence methods and techniques, including metadata extraction tools, advanced search engines, advanced browsers, power searching methods, online anonymity tools such as TOR and i2p, OSINT tools such as Maltego, Shodan, Creepy, SearchDiggity, Recon-ng, Social Network Analysis (SNA), Darkweb/Deepweb, data visualization, and much more. Provides a holistic approach to OSINT and Web recon, showing you how to fit all the data together into actionable intelligence Focuses on hands-on tools such as TOR, i2p, Maltego, Shodan, Creepy, SearchDiggity, Recon-ng, FOCA, EXIF, Metagoofil, MAT, and many more Covers key technical topics such as metadata searching, advanced browsers and power searching, online anonymity, Darkweb / Deepweb, Social Network Analysis (SNA), and how to manage, analyze, and visualize the data you gather Includes hands-on technical examples and case studies, as well as a Python chapter that shows you how to create your own information-gathering tools and modify existing APIs

The Tao of Open Source Intelligence BoD – Books on Demand

NOWHERE TO HIDE: Open Source Intelligence Gathering provides practical insight into the investigative tools and open source intelligence gathering (commonly known as "OSINT") used by law enforcement, the media, and the general public to identify individuals involved in the events of January 6, 2021, at the U.S. Capitol Building in Washington, DC. NOWHERE TO HIDE retraces the FBI's investigative techniques - some using cutting-edge technology and others using old fashioned, knocking-on-doors detective work - used to pursue the hundreds of thousands of leads received from the general public. NOWHERE TO HIDE is filled with real world case studies, specific resources and practical "how to" guides to equip both beginner and seasoned OSINT investigators with the right tools for their OSINT toolboxes. This insightful volume includes 36 case studies that follow the FBI's investigations of individual persons of interest, including the tactics, techniques, and procedures used by law enforcement, the media, and public sleuths to track down, identify, and - most importantly - verify the identities of suspected rioters. Learn how the FBI sifted through hundreds of thousands of leads, false positives, dead ends, as well as numerous unexpected leads to perform their investigations. NOWHERE TO HIDE provides vivid context around the events of January 6, 2021, at the U.S. Capitol Building in Washington, DC, which left five people - one police officer and four protestors - dead by the end of the assault. Effective OSINT research requires a combination of technical knowledge to find the Who, What, When, Where, and How threads of data and information as well as taking into account our unpredictable human nature that sometimes leads us to do the things we do (the Why). OSINT is both science and art. NOWEHERE TO HIDE provides practical, actionable information to help both novice and expert investigators, researchers, advocates, and journalists navigate and penetrate OSINT resources to find the information and evidence they seek. Daniel Farber Huang is author of "Practical Cyber Security for Extremely Busy People" and a consultant to a wide range of organizations on cyber and strategy issues. He has worked closely with numerous federal, state, and local law enforcement agencies across the U.S. on providing solutions to their mobile technology requirements. He has focused on providing hardware and software solutions to federal field agents, investigators, the police,

and other authorities to support them in performing their duties. He is a strategic consultant helping a wide range of companies in different industries reduce risks at all levels of their organizations, including their cyber security. Daniel is also a documentary photographer and freelance journalist.

Hunting Cyber Criminals CRC Press

"Prepared for the Office of the Secretary of Defense."

Open Source Intelligence Techniques Syngress Publishing

One of the most important aspects for a successful police operation is the ability for the police to obtain timely, reliable and actionable intelligence related to the investigation or incident at hand. Open Source Intelligence (OSINT) provides an invaluable avenue to access and collect such information in addition to traditional investigative techniques and information sources. This book offers an authoritative and accessible guide on how to conduct Open Source Intelligence investigations from data collection to analysis to the design and vetting of OSINT tools. In its pages the reader will find a comprehensive view into the newest methods for OSINT analytics and visualizations in combination with real-life case studies to showcase the application as well as the challenges of OSINT investigations across domains. Examples of OSINT range from information posted on social media as one of the most openly available means of accessing and gathering Open Source Intelligence to location data, OSINT obtained from the darkweb to combinations of OSINT with real-time analytical capabilities and closed sources. In addition it provides guidance on legal and ethical considerations making it relevant reading for practitioners as well as academics and students with a view to obtain thorough, first-hand knowledge from serving experts in the field.

Open Source Intelligence Techniques Rob Botwright

Do you want to learn more about OSINT or Open Source Intelligence or are interested in online investigations? If your answer is yes, this is the Cyber Secrets issue for you. Inside, you will learn how to manually get evidence from some online sources along with several tools that can help automate some of the processes. Most of the tools are prepackaged into CSI Linux, a forensic investigation platform, while not required for the vast majority of the OSINT material. HANDS-ON WALKTHROUGHS!!! Yes, we cover both theory and hands-on content from some great authors that have helped put this issue together.

Deep Dive Syngress

Algorithms for Automating Open Source Intelligence (OSINT) presents information on the gathering of information and extraction of actionable intelligence from openly available sources, including news broadcasts, public repositories, and more recently, social media. As OSINT has applications in crime fighting, state-based intelligence, and social research, this book provides recent advances in text mining, web crawling, and other algorithms that have led to advances in methods that can largely automate this process. The book is beneficial to both practitioners and academic researchers, with discussions of the latest advances in applications, a coherent set of methods and processes for automating OSINT, and interdisciplinary perspectives on the key problems identified within each discipline. Drawing upon years of practical experience and using numerous examples, editors Robert Layton, Paul Watters, and a distinguished list of contributors discuss Evidence Accumulation Strategies for OSINT, Named Entity Resolution in Social Media, Analyzing Social Media Campaigns for Group Size Estimation, Surveys and qualitative techniques in OSINT, and Geospatial reasoning of open data. Presents a coherent set of methods and processes for automating OSINT Focuses on algorithms and applications allowing the practitioner to get up and running quickly Includes fully developed case studies on the digital underground and predicting crime through OSINT Discusses the ethical considerations when using publicly available online data

Web Intelligence: Research and Development Independently Published

Unlock the Power of Advanced OSINT Strategies Welcome to the "Advanced OSINT Strategies" book bundle – your ultimate guide to mastering Online Investigations and Intelligence Gathering. This comprehensive collection spans four volumes, each tailored to take you from a beginner's foundation to expert-level proficiency in the exciting world of open-source intelligence. BOOK 1 - Foundations of OSINT Mastery: A Beginner's Guide Discover the essentials of OSINT as you embark on this enlightening journey. Explore digital landscapes, decode digital footprints, and harness the vast range of open-source information. This volume equips you with internet search techniques, social media investigation skills, and the ability to analyze websites and extract valuable data. Ethics and privacy considerations are also emphasized to ensure responsible and ethical OSINT practices. BOOK 2 - Navigating the Digital Shadows: Intermediate OSINT Techniques Take your skills to the next level with advanced search queries, deep web and dark web investigations, and geospatial intelligence mastery. Dive deep into social media analysis, email tracing, and open-source analysis tools. This volume also guides you towards automating your OSINT workflows and becoming proficient in cyber threat intelligence. BOOK 3 - Advanced OSINT Arsenal: Expert-Level Intelligence Gathering Elevate your expertise with this advanced volume. Analyze cryptocurrencies and blockchain, exploit IoT devices for intelligence, and employ advanced data scraping and automation techniques. Real-world intelligence operations and the synergy of ethical hacking with OSINT are explored in depth, making you an expert in the field. BOOK 4 - Mastering OSINT Investigations: Cutting-Edge Strategies and Tools In the final volume, delve into cutting-edge strategies and tools that give you an edge in OSINT investigations. Explore the potential of big data, artificial intelligence, and quantum computing in OSINT. Navigate hidden markets and forums, track cryptocurrencies on the dark web, and master advanced geospatial analysis techniques. Complete your journey with IoT vulnerability assessment and data collection and analysis, equipping you with the latest tools and strategies. Why Choose "Advanced OSINT Strategies"? · Comprehensive Learning: Master the entire spectrum of OSINT, from beginner to expert. · Real-World Skills: Gain practical knowledge and hands-on experience. · Ethical and Legal Focus: Understand the ethical and legal considerations in OSINT. · Cutting-Edge Insights: Stay updated with the latest tools and techniques. · Authoritative Content: Written by experts in the field. With "Advanced OSINT Strategies," you'll become a formidable force in the world of online investigations and intelligence gathering. Unlock the power of information, uncover hidden truths, and make informed decisions. Begin your journey to OSINT mastery today! Get the entire bundle now and take your OSINT skills to the next level. Don't miss out on this opportunity to become an expert in Online Investigations and Intelligence Gathering.

Advanced OSINT Strategies Createspace Independent Publishing Platform

This edited book provides an insight into the new approaches, challenges and opportunities that characterise open source intelligence (OSINT) at the beginning of the twenty-first century. It does so by considering the impacts of OSINT on three important contemporary security issues: nuclear proliferation, humanitarian crises and terrorism.

Cybersecurity Threats with New Perspectives Bloomsbury Publishing USA

Unlock the power of Open Source Intelligence (OSINT) with "OSINT Essentials: Your Comprehensive Guide to Open Source Intelligence" by Samuel Bonheur. This expertly crafted guide is your gateway to mastering the art of gathering, analyzing, and interpreting publicly available information from the vast expanse of the digital realm. Dive into a wealth of knowledge that empowers you to harness the potential of OSINT for a multitude of purposes, from cybersecurity to investigative journalism, threat intelligence to business intelligence. Unveil Hidden Insights: Explore the world of OSINT like never before. This comprehensive guide takes you on a journey through the intricacies of online information gathering. Discover how to leverage the vast resources of the internet to uncover hidden insights, unmask concealed connections, and extract meaningful data to fuel your endeavors. Comprehensive Coverage: From fundamental concepts to advanced techniques, "OSINT Essentials" covers it all. Delve into chapters that encompass a wide spectrum of OSINT domains, including search engine mastery, social media investigations, geolocation and mapping, digital forensics, and much more. This book serves as your one-stop reference, guiding you through every step of the OSINT process. Real-World Applications: Experience the real-world impact of OSINT through captivating case studies and success stories. Witness how OSINT has played a pivotal role in solving complex mysteries, thwarting cyber threats, and unearthing critical information. Gain insights into the practical applications of OSINT across diverse industries and scenarios. Ethical Excellence: Ethics and responsibility are at the forefront of "OSINT Essentials." Understand the ethical considerations that underpin effective OSINT practices. Navigate the complex terrain of privacy concerns, data protection, and legal boundaries with confidence, ensuring that your OSINT activities are both impactful and morally sound. Best Practices and Tools: Equip yourself with a diverse toolkit of OSINT techniques and tools. Master advanced search strategies, refine your web scraping skills, analyze images and videos with precision, and unravel the secrets of the deep web and dark web. "OSINT Essentials" provides you with the guidance needed to excel in each facet of OSINT. Structured Learning: Structured for both beginners and seasoned practitioners, this book provides a logical and easy-to-follow progression. Each chapter presents a deep dive into a specific OSINT domain, complete with sub-chapters that explore essential concepts, tools, methodologies, and practical examples. Empower Your Endeavors: Whether you're a cybersecurity enthusiast, a journalist unearthing groundbreaking stories, an investigator seeking truth, or a professional enhancing business strategies, "OSINT Essentials" empowers you to harness the power of publicly available information to make informed decisions and achieve remarkable outcomes. Embark on a transformative journey through the realm of Open Source Intelligence. "OSINT Essentials: Your Comprehensive Guide to Open Source Intelligence" by Samuel Bonheur is more than a book - it's your indispensable companion in unlocking the endless possibilities of OSINT. Dive in and elevate your understanding, skills, and impact in the world of information discovery.

Open Source Intelligence in a Networked World Independently Published

Fifth Edition Sheds New Light on Open Source Intelligence Collection and Analysis.Author Michael Bazzell has been well known and respected in government circles for his ability to locate personal information about any target through Open Source Intelligence (OSINT). In this book, he shares his methods in great detail. Each step of his process is explained throughout sixteen chapters of specialized websites, application programming interfaces, and software solutions. Based on his live and online video training at IntelTechniques.com, over 250 resources are identified with narrative tutorials and screen captures. This book will serve as a reference guide for anyone that is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The search techniques offered will inspire analysts to "think outside the box" when scouring the internet for personal information. Much of the content of this book has never been discussed in any publication. Always thinking like a hacker, the author has identified new ways to use various technologies for an unintended purpose. This book will improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network ContentCell Phone Subscriber InformationDeleted Websites & PostsMissing Facebook Profile DataFull Twitter Account DataAlias Social Network ProfilesFree Investigative SoftwareUseful Browser ExtensionsAlternative Search Engine ResultsWebsite Owner InformationPhoto GPS & MetadataLive Streaming Social ContentSocial Content by LocationIP Addresses of UsersAdditional User AccountsSensitive Documents & PhotosPrivate Email AddressesDuplicate Video PostsMobile App Network DataUnlisted Addresses & #sPublic Government RecordsDocument MetadataRental Vehicle ContractsOnline Criminal ActivityPersonal Radio CommunicationsCompromised Email InformationWireless Routers by LocationHidden Mapping ApplicationsDark Web Content (Tor)Restricted YouTube ContentHidden Website DetailsVehicle Registration Details

Espionage Black Book Four Createspace Independent Publishing Platform

Completely Rewritten Sixth Edition Sheds New Light on Open Source Intelligence Collection and Analysis Author Michael Bazzell has been well known in government circles for his ability to locate personal information about any target through Open Source Intelligence (OSINT). In this book, he shares his methods in great detail. Each step of his process is explained throughout twenty-five chapters of specialized websites, software solutions, and creative search techniques. Over 250 resources are identified with narrative tutorials and screen captures. This book will serve as a reference guide for anyone that is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The search techniques offered will inspire analysts to "think outside the box" when scouring the internet for personal information. Much of the content of this book has never been discussed in any publication. Always thinking like a hacker, the author has identified new ways to use various technologies for an unintended purpose. This book will greatly improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network Content Cell Phone Subscriber Information Deleted Websites & Posts Missing Facebook Profile Data Full Twitter Account Data Alias Social Network Profiles Free Investigative Software Useful Browser Extensions Alternative Search Engine Results Website Owner Information Photo GPS & Metadata Live Streaming Social Content Social Content by Location IP Addresses of Users Additional User Accounts Sensitive Documents & Photos Private Email Addresses Duplicate Video Posts Mobile App Network Data Unlisted Addresses &#s Public Government Records Document Metadata Rental Vehicle Contracts Online Criminal Activity Personal Radio Communications Compromised Email Information Automated Collection Solutions Linux Investigative Programs Dark Web Content (Tor) Restricted YouTube Content Hidden Website Details Vehicle Registration

Details

Open Source Intelligence Methods and Tools IT Governance Ltd

Interdisciplinary and multidisciplinary research is slowly yet steadily revolutionizing traditional education. However, multidisciplinary research can and will also improve the extent to which a country can protect its critical and vital assets. Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism is an essential scholarly publication that provides personnel directly working in the fields of intelligence, law enforcement, and science with the opportunity to understand the multidisciplinary nature of intelligence and science in order to improve current intelligence activities and contribute to the protection of the nation. Each chapter of the book discusses various components of science that should be applied to the intelligence arena. Featuring coverage on a range of topics including cybersecurity, economics, and political strategy, this book is ideal for law enforcement, intelligence and security practitioners, students, educators, and researchers.

Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism Rob Botwright

OSINT is a rapidly evolving approach to intelligence collection, and its wide application makes it a useful methodology for numerous practices, including within the criminal investigation community.The Tao of Open Source Intelligence is your guide to the cutting edge of this information collection capability.