

Open source intelligence (OSINT)

Type de contenu : Texte

Type de médiation : sans médiation

Type de support : Volume

Titre(s) : Open source intelligence (OSINT) : a practical introduction : a field manual / Varin Khera,..., Anand R. Prasad,..., Suksit Kwanoran,...

Auteur(s) : Khera, Varin (19..-....)

Autre(s) auteur(s) : Prasad, Anand Raghawa Kwanoran, Suksit (19..-....)

Publication : Gistrup, Denmark : River publishers

Date de copyright : C 2024

Description matérielle : 1 volume (XII-115 pages) : illustrations en couleurs, couverture illustrée en couleurs ; 24 cm

Collection : River rapids

ISBN : 978-8-7700-4717-3
87-7004-717-0

EAN : 9788770047173

Appartient à la collection : River rapids

Classification décimale Dewey : 364.168 2

Note sur la responsabilité : Dr. Khera is a distinguished cybersecurity executive with more than 20 years of experience, currently serving as the CEO of CloudSec Asia (CSA) based in Thailand. Throughout his career, he has been at the forefront of developing and implementing cutting-edge cybersecurity solutions. Dr. Khera's expertise spans a wide array of fields within cybersecurity, including threat intelligence, cloud security, and the application of artificial intelligence in enhancing cyber defenses. Under his leadership, CloudSec Asia has emerged as a leader in the cybersecurity industry, known for its innovative approaches to protecting organizations against evolving threats. Dr. Khera's profound knowledge and strategic insights in architecting security operations centers (SOCs) have been instrumental in mitigating cyber risks for high-profile global clients. Prior to founding CSA, Dr. Khera held a key role as head of cybersecurity presales at Nokia, where he collaborated extensively with major telecom providers and

government entities across the Asia Pacific region. He holds a Doctor of Information Technology (DIT) from Murdoch University, a Postgraduate Certificate in Network Computing from Monash University, and a Certificate of Executive Leadership from E-Cornell University. Dr. Khera's contributions to the cybersecurity field have been widely recognized, including his receipt of the prestigious Asia Pacific Information Security Leadership Awards (ISLA) for excellence in IT Security Practitioner leadership. His commitment to advancing cybersecurity practices continues to shape the industry landscape globally. Dr. Anand R. Prasad is a Partner at Deloitte Tohmatsu Cyber. He has also served as Board of Director at Digital Nasional Berhad. Prior to that, among other things, he was Founder & CEO of wenovator, acquired by DTCY, advisor to NTT DOCOMO and CISO, board member of Rakuten Mobile. Anand led the standardization of 5G security as Chairman of 3GPP SA3. He is advisor to several organizations, an innovator with 50+ patents, a recognized keynote speaker and a prolific writer with 6 books and 50+ publications. He is a Fellow of IET & IETE, Editor of Cyber Security Magazine and Editor-in-Chief Journal of ICT Standardization by River Publishers. Suksit Kwanoran is a seasoned expert in the field of cybersecurity and cloud computing, with over 17 years of extensive experience. He currently serves as the Managing Director of SecStrike Co., Ltd., where he leads the development of innovative security solutions and manages a high-performance team providing comprehensive security services. Additionally, he holds the position of Chief Technology Officer (CTO) at CloudSec Asia Co., Ltd., where he has significantly contributed to the company's rapid growth by integrating various technologies and expanding its range of services. Suksit has a strong educational background, holding a Master's degree in Network Engineering and a Bachelor's degree in Electrical Engineering from Mahanakorn University of Technology. His career includes significant roles such as Senior Instructor at Network Training Center and IT Manager at Amata Corporation PCL. He is also a certified professional with numerous credentials including CompTIA CASP, CySA+, Pentest+, Security+, Cisco Certified System Instructor, CEH, ISO 27001 Lead Auditor, CCNA, and AWS Certified Solution Architect

Note sur les bibliographies et les index : Bibliographie en fin de chapitres. Index

Note sur le contenu : Preface ix About the Authors xi 1 Introduction to Threat 1 1.1 Defining Intelligence 1 1.2 Threat Intelligence 3 1.3 Threat Intelligence Life Cycle 3 1.4 TI Types and Purpose 6 1.5 Key Threat Intelligence Terminology 8 1.6 Challenges and Limitations Associated with Threat Intelligence 10 1.7 Realistic Approach to Implementing TI 11 1.8 Open Source Intelligence (OSINT) 12 1.9 Book Overview 13 2 Introduction to Open Source Intelligence (OSINT) 15 2.1 OSINT Definition 16 2.2 OSINT Types 16 2.3 OSINT Users 17 2.4 OSINT Challenges 20 2.5 Chapter Summary 20 3 Online Tracking and Behavioral Profiling 23 3.1 IP Address 24 3.2 Cookies 25 3.3 ETag 27 3.4 Browser Fingerprinting 28 3.5 Chapter Summary 30 4 Hiding Your Traces When Conducting Online Investigations 33 4.1 Protect your Operating System 34 4.2 Secure Online Browsing 36 4.3 Countermeasures Against Online Tracking Techniques 37 4.4 Chapter Summary 41 5 Open Source Intelligence (OSINT): A Practical Example 43 5.1 Technical Investigation of a Website 43 5.2 Analytics and Tracking 45 5.3 Website History 46 5.4 Subdomain Discovery 47 5.5 Type and Versions of IT Infrastructure of the Target Company 49 5.6 Harvest Digital Files Hosted on Domains 50 5.7 Information Contained in File Metadata 51 5.8 Tools to Retrieve Digital File Metadata 53 5.9 Chapter Summary 54 6 Using AI in OSINT Research 57 6.1 Data Collection and Scraping 57 6.2 Analysis of Unstructured Text Data 58 6.3 Analysis of Multimedia Files (Images and Videos) 60 6.4 Content Summarization 60 6.5 Social Network Analysis 61 6.6 Chapter Summary 62 7 Social Media Intelligence (SOCMINT) 63 7.1 Privacy Issues In SOCMINT 65 7.2 OSINT Roadmap for Investigating Social Media Platforms 66 7.3 Chapter Summary 72 8 The Web Layers: Introduction to Surface, Deep and Darknet 75 8.1 Surface Web

76 8.2 Deep Web 77 8.3 Darknet 78 8.4 Chapter Summary 79 9 Darkweb and Internet Anonymity: Exploring the Hidden Internet 81 9.1 TOR Network 82 9.2 Searching the TOR Network 85 9.3 Chapter Summary 86 10 Introduction to Digital Forensics 87 10.1 Digital Evidence 88 10.2 Digital Forensics Process 90 10.3 Digital Investigation Types 91 10.4 Digital Forensics Readiness 92 10.5 Chapter Summary 93 11 OSINT for Digital Forensics Investigations 95 11.1 OSINT to Collect Individual Intelligence 95 11.2 Investigating Social Networking Sites 100 11.3 Investigating a Digital File???s Metadata 101 11.4 Searching for Leaked Credentials on the Darknet 104 11.5 Chapter Summary 106 12 Data Protection and Cybersecurity Laws for the Asia Pacific Region 107 12.1 Classifications of Personal Information 108 12.2 Singapore 110 12.3 Japan 110 12.4 Vietnam 111 12.5 China 111 12.6 Thailand 113 12.7 Chapter Summary 114 Index 115

Résumé ou extrait : This practical book introduces open-source intelligence (OSINT) and explores how it can be executed in different intelligence scenarios. It covers varying supporting topics, such as online tracking techniques, privacy best practices for OSINT researchers, and practical examples of OSINT investigations. The book also delves into the integration of artificial intelligence (AI) and machine learning (ML) in OSINT, social media intelligence methodologies, and the unique characteristics of the surface web, deep web, and dark web. Open-source intelligence (OSINT) is a powerful tool that leverages publicly available data for security purposes. OSINT derives its value from various sources, including the internet, traditional media, academic publications, corporate papers, and geospatial information. Further topics include an examination of the dark web's uses and potential risks, an introduction to digital forensics and its methods for recovering and analyzing digital evidence, and the crucial role of OSINT in digital forensics investigations. The book concludes by addressing the legal considerations surrounding the use of the information and techniques presented. This book provides a comprehensive understanding of CTI, TI, and OSINT. It sets the stage for the best ways to leverage OSINT to support different intelligence needs to support decision-makers in today's complex IT threat landscape.

Sujet - Nom commun : Données ouvertes

Recherche sur Internet

Technologies de l'information et de la communication

Renseignement électronique

Recherche de l'information

Sources d'information électroniques