Network Behavior Analysis Tools

Industrial Network Security
Behavior Analysis with Machine Learning Using R
Network Protocols for Security Professionals
Advances on P2P, Parallel, Grid, Cloud and Internet Computing
Behavior Dynamics in Media-sharing Social Networks
Mastering Attack Surface Management
Operations Support Systems: Solutions and Strategies for the Emerging Network
Mobile Web and Intelligent Information Systems
Software-Defined Networking for Future Internet Technology
Network Security Through Data Analysis
Information and Business Intelligence
Advances in Cross-Cultural Decision Making
Managing Trust in Cyberspace
Learning Malware Analysis
Psychological and Behavioral Examinations in Cyber Security
Criticality in neural network behavior and its implications for computational processing in healthy and perturbed conditions
Network Behavior Analysis
Predicting Malicious Behavior
IoT as a Service
Mastering Viruses
Cloud Computing and Security
Network Traffic Anomaly Detection and Prevention
Mastering Security Operations
DDoS Attacks
Simulation Tools and Techniques
Models and Methods in Social Network Analysis
CSO
Data Traffic Monitoring and Analysis
Exploring Animal Social Networks
Large Scale Networks
Internet and Distributed Computing Systems
Network Security Through Data Analysis
Big Data Analytics
Advances in Intelligent Networking and Collaborative Systems
Wireless Mobile Internet Security
Defending Cyber Systems through Reverse Engineering of Criminal Malware
Computational Social Network Analysis
Advanced Data Mining Tools and Methods for Social Computing
Practical Intrusion Analysis

STOKES PAGE

Industrial Network Security Springer
This indispensable text/reference presents a comprehensive overview on the detection and prevention of anomalies in computer network traffic, from coverage of the fundamental theoretical concepts to in-depth analysis of systems and methods. Readers will benefit from invaluable practical guidance on how to design an intrusion detection technique and incorporate it into a system, as well as on how to analyze and correlate alerts without prior information. Topics and features: introduces the essentials of traffic management in high speed networks, detailing types of anomalies, network vulnerabilities, and a taxonomy of network attacks; describes a systematic approach to generating large network intrusion datasets, and reviews existing synthetic, benchmark, and real-life datasets; provides a detailed study of network anomaly detection techniques and systems under six different categories: statistical, classification, knowledge-base, cluster and outlier detection, soft computing, and combination learners; examines alert management and anomaly prevention techniques, including alert preprocessing, alert correlation, and alert post-processing; presents a hands-on approach to developing network traffic monitoring and analysis tools, together with a survey of existing tools; discusses various evaluation criteria and metrics, covering issues of accuracy, performance, completeness, timeliness, reliability, and quality; reviews open issues and challenges in network traffic anomaly detection and prevention. This informative work is ideal for graduate and advanced undergraduate students interested in network security and privacy, intrusion detection systems, and data mining in security. Researchers and practitioners specializing in network security will also find the book to be a useful reference.

Behavior Analysis with Machine Learning Using R John Wiley & Sons
This book presents the latest research findings, as well as innovative theoretical and practical research results, methods and development techniques related to P2P, grid, cloud and Internet computing. It also reveals the synergies among such large scale computing paradigms. P2P, Grid, Cloud and Internet computing technologies have rapidly become established as breakthrough paradigms for solving complex problems by

enabling aggregation and sharing of an increasing variety of distributed computational resources on a large scale. Grid computing originated as a paradigm for high-performance computing, offering an alternative to expensive supercomputers through different forms of large-scale distributed computing. P2P computing emerged as a new paradigm following on from client-server and web-based computing and has proved useful in the development of social networking, B2B (Business to Business), B2C (Business to Consumer), B2G (Business to Government), and B2E (Business to Employee). Cloud computing has been described as a “computing paradigm where the boundaries of computing are determined by economic rationale rather than technical limits”. Cloud computing has fast become the computing paradigm with applicability and adoption in all domains and providing utility computing at large scale. Lastly, Internet computing is the basis of any large-scale distributed computing paradigm; it has very quickly developed into a vast and flourishing field with enormous impact on today’s information societies and serving as a universal platform comprising a large variety of computing forms such as grid, P2P, cloud and mobile computing.

Network Protocols for Security Professionals Springer

Network Behavior AnalysisSpringer Nature

Advances on P2P, Parallel, Grid, Cloud and Internet Computing Cybellium Ltd

The aim of this book is to provide the latest research findings, innovative research results, methods and development techniques from both theoretical and practical perspectives related to intelligent social networks and collaborative systems, intelligent networking systems, mobile collaborative systems, secure intelligent cloud systems, etc., and to reveal synergies among various paradigms in the multi-disciplinary field of intelligent collaborative systems. It presents the Proceedings of the 9th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2017), held on August 24–26, 2017 in Toronto, Canada. With the rapid evolution of the Internet, we are currently experiencing a shift from the traditional sharing of information and applications as the main purpose of the Web to an emergent paradigm that puts people at the very centre of networks and exploits the value of people’s connections, relations and collaborations. Social networks are also pla ying a major role in the dynamics and structure of intelligent Web-based networking and collaborative systems. Virtual campuses, virtual communities and organizations effectively leverage intelligent networking and collaborative systems by tapping into a broad range of formal and informal electronic relations, such as business-to-business, peer-to-peer and many types of online collaborative learning interactions, including the emerging e-learning systems. This has resulted in entangled systems that need to be managed efficiently and autonomously. In addition, the latest and powerful technologies based on Grid and wireless infrastructure as well as Cloud computing are now greatly enhancing collaborative and networking applications, but are also facing new issues and challenges. The principal objective of the research and development community is to stimulate research that leads to the creation of responsive environments for networking and, in the longer-term, the developmen t of adaptive, secure, mobile, and intuitive intelligent systems for collaborative work and learning.

Behavior Dynamics in Media-sharing Social Networks CRC Press

In this practical guide, security researcher Michael Collins shows you several techniques and tools for collecting and analyzing network traffic datasets. You'll understand how your network is used, and what actions are necessary to protect and improve it. Divided into three sections, this book examines the process of collecting and organizing data, various tools for analysis, and several different analytic scenarios and techniques.

Mastering Attack Surface Management Princeton University Press

Network infrastructures are growing rapidly to meet the needs of business, but the required repolicing and reconfiguration provide challenges that need to be addressed. The software-defined network (SDN) is the future generation of Internet technology that can help meet these challenges of network management. This book includes quantitative research, case studies, conceptual papers, model papers, review papers, and theoretical backing on SDN. This book investigates areas where SDN can help other emerging technologies deliver more efficient services, such as IoT, industrial IoT, NFV, big data, blockchain, cloud computing, and edge computing. The book demonstrates the many benefits of SDNs, such as reduced costs, ease of deployment and management, better scalability, availability, flexibility and fine-grained control of traffic, and security. The book demonstrates the many benefits of SDN, such as reduced costs, ease of deployment and management, better scalability, availability, flexibility and fine-grained control of traffic, and security. Chapters in the volume address: Design considerations for security issues and detection methods State-of-the-art approaches for mitigating DDos attacks using SDN Big data using Apache Hadoop for processing and analyzing large amounts of data Different tools used for attack simulation Network policies and policy management approaches that are widely used in the context of SDN Dynamic flow tables, or static flow table management A new four-tiered architecture that includes cloud, SDN-controller, and fog computing Architecture for keeping computing resources available near the industrial IoT network through edge computing The impact of SDN as an innovative approach for smart city development More. The book will be a valuable resource for SDN researchers as well as academicians, research scholars, and students in the related areas.

Operations Support Systems: Solutions and Strategies for the Emerging Network Springer

This book constitutes the refereed proceedings of the 18th International Conference on Mobile Web and Intelligent Information Systems, MobiWIS 2022, held in Rome, Italy, in August 2022.The 18 full papers and 1 short paper presented in this book were carefully reviewed and selected from 51 submissions. The papers of MobiWIS 2022 deal focus on topics such as security and privacy; web and mobile applications; networking and communication; intelligent information systems; and IoT and ubiquitous computing.

Mobile Web and Intelligent Information Systems Syngress

Cybellium Ltd is dedicated to empowering individuals and organizations with the knowledge and skills they need to navigate the ever-evolving computer science landscape securely and learn only the latest information available on any subject in the category of computer science including: - Information Technology (IT) - Cyber Security - Information Security - Big Data - Artificial Intelligence (AI) - Engineering - Robotics - Standards and compliance Our mission is to be at the forefront of computer science education, offering a wide and comprehensive range of resources, including books, courses, classes and training programs, tailored to meet the diverse needs of any subject in computer science. Visit https://www.cybellium.com for more books.

Software-Defined Networking for Future Internet Technology CRC Press

This book provides a comprehensive overview of network behavior analysis that mines Internet traffic data in order to extract, model, and make sense of behavioral patterns in Internet

“objects” such as end hosts, smartphones, Internet of things, and applications. The objective of this book is to fill the book publication gap in network behavior analysis, which has recently become an increasingly important component of comprehensive network security solutions for data center networks, backbone networks, enterprise networks, and edge networks. The book presents fundamental principles and best practices for measuring, extracting, modeling and analyzing network behavior for end hosts and applications on the basis of Internet traffic data. In addition, it explains the concept and key elements (e.g., what, who, where, when, and why) of communication patterns and network behavior of end hosts and network applications, drawing on data mining, machine learning, information theory, probabilistic graphical and structural modeling to do so. The book also discusses the benefits of network behavior analysis for applications in cybersecurity monitoring, Internet traffic profiling, anomaly traffic detection, and emerging application detections. The book will be of particular interest to researchers and practitioners in the fields of Internet measurement, traffic analysis, and cybersecurity, since it provides a spectrum of innovative techniques for summarizing behavior models, structural models, and graphic models of Internet traffic, and explains how to leverage the results for a broad range of real-world applications in network management, security operations, and cyber-intelligent analysis. After finishing this book, readers will 1) have learned the principles and practices of measuring, modeling, and analyzing network behavior on the basis of massive Internet traffic data; 2) be able to make sense of network behavior for a spectrum of applications ranging from cybersecurity and network monitoring to emerging application detection; and 3) understand how to explore network behavior analysis to complement traditional perimeter-based firewall and intrusion detection systems in order to detect unusual traffic patterns or zero-day security threats using data mining and machine learning techniques. To ideally benefit from this book, readers should have a basic grasp of TCP/IP protocols, data packets, network flows, and Internet applications.

Network Security Through Data Analysis IGI Global

This book constitutes the refereed post-conference proceedings of the Fourth International Conference on IoT as a Service, IoTaaS 2018, which took place in Xi’an, China, in November 2018. The 50 revised full papers were carefully reviewed and selected from 83 submissions. The technical track present IoT-based services in various applications. In addition, there are three workshops: international workshop on edge computing for 5G/IoT, international workshop on green communications for internet of things, and international workshop on space-based internet of things.

Information and Business Intelligence Packt Publishing Ltd

This SpringerBrief discusses underlying principles of malware reverse engineering and introduces the major techniques and tools needed to effectively analyze malware that targets business organizations. It also covers the examination of real-world malware samples, which illustrates the knowledge and skills necessary to take control of cyberattacks. This SpringerBrief explores key tools and techniques to learn the main elements of malware analysis from the inside out. It also presents malware reverse engineering using several methodical phases, in order to gain a window into the mind set of hackers. Furthermore, this brief examines malicious program’s behavior and views its code-level patterns. Real world malware specimens are used to demonstrate the emerging behavioral patterns of battlefield malware as well. This SpringerBrief is unique, because it demonstrates the capabilities of emerging malware by conducting reverse-code engineering on real malware samples and conducting behavioral analysis in isolated lab system. Specifically, the author focuses on analyzing malicious Windows executables. This type of malware poses a large threat to modern enterprises. Attackers often deploy malicious documents and browser-based exploits to attack Windows enterprise environment. Readers learn how to take malware inside-out using static properties analysis, behavioral analysis and code-level analysis techniques. The primary audience for this SpringerBrief is undergraduate students studying cybersecurity and researchers working in this field. Cyber security professionals that desire to learn more about malware analysis tools and techniques will also want to purchase this SpringerBrief.

Advances in Cross-Cultural Decision Making Springer

DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance discusses the evolution of distributed denial-of-service (DDoS) attacks, how to detect a DDoS attack when one is mounted, how to prevent such attacks from taking place, and how to react when a DDoS attack is in progress, with the goal of tolerating the attack. It introduces types and characteristics of DDoS attacks, reasons why such attacks are often successful, what aspects of the network infrastructure are usual targets, and methods used to launch attacks. The book elaborates upon the emerging botnet technology, current trends in the evolution and use of botnet technology, its role in facilitating the launching of DDoS attacks, and challenges in countering the role of botnets in the proliferation of DDoS attacks. It introduces statistical and machine learning methods applied in the detection and prevention of DDoS attacks in order to provide a clear understanding of the state of the art. It presents DDoS reaction and tolerance mechanisms with a view to studying their effectiveness in protecting network resources without compromising the quality of services. To practically understand how attackers plan and mount DDoS attacks, the authors discuss the development of a testbed that can be used to perform experiments such as attack launching, monitoring of network traffic, and detection of attacks, as well as for testing strategies for prevention, reaction, and mitigation. Finally, the authors address current issues and challenges that need to be overcome to provide even better defense against DDoS attacks.

Managing Trust in Cyberspace Springer

Traditional intrusion detection and logfile analysis are no longer enough to protect today’s complex networks. In the updated second edition of this practical guide, security researcher Michael Collins shows InfoSec personnel the latest techniques and tools for collecting and analyzing network traffic datasets. You’ll understand how your network is used, and what actions are necessary to harden and defend the systems within it. In three sections, this book examines the process of collecting and organizing data, various tools for analysis, and several different analytic scenarios and techniques. New chapters focus on active monitoring and traffic manipulation, insider threat detection, data mining, regression and machine learning, and other topics. You’ll learn how to: Use sensors to collect network, service, host, and active domain data Work with the SiLK toolset, Python, and other tools and techniques for manipulating data you collect Detect unusual phenomena through exploratory data analysis (EDA), using visualization and mathematical techniques Analyze text data, traffic behavior, and communications mistakes Identify significant structures in your network with graph analysis Examine insider threat data and acquire threat intelligence Map your network and identify significant hosts within it Work with operations to develop defenses and analysis techniques

Learning Malware Analysis "O'Reilly Media, Inc."

“Practical Intrusion Analysis provides a solid fundamental overview of the art and science of intrusion analysis.” –Nate

Miller, Cofounder, Stratum Security The Only Definitive Guide to New State-of-the-Art Techniques in Intrusion Detection and Prevention Recently, powerful innovations in intrusion detection and prevention have evolved in response to emerging threats and changing business environments. However, security practitioners have found little reliable, usable information about these new IDS/IPS technologies. In Practical Intrusion Analysis, one of the field's leading experts brings together these innovations for the first time and demonstrates how they can be used to analyze attacks, mitigate damage, and track attackers. Ryan Trost reviews the fundamental techniques and business drivers of intrusion detection and prevention by analyzing today's new vulnerabilities and attack vectors. Next, he presents complete explanations of powerful new IDS/IPS methodologies based on Network Behavioral Analysis (NBA), data visualization, geospatial analysis, and more. Writing for security practitioners and managers at all experience levels, Trost introduces new solutions for virtually every environment. Coverage includes Assessing the strengths and limitations of mainstream monitoring tools and IDS technologies Using Attack Graphs to map paths of network vulnerability and becoming more proactive about preventing intrusions Analyzing network behavior to immediately detect polymorphic worms, zero-day exploits, and botnet DoS attacks Understanding the theory, advantages, and disadvantages of the latest Web Application Firewalls Implementing IDS/IPS systems that protect wireless data traffic Enhancing your intrusion detection efforts by converging with physical security defenses Identifying attackers' "geographical fingerprints" and using that information to respond more effectively Visualizing data traffic to identify suspicious patterns more quickly Revisiting intrusion detection ROI in light of new threats, compliance risks, and technical alternatives Includes contributions from these leading network security experts: Jeff Forristal, a.k.a. Rain Forest Puppy, senior security professional and creator of libwhisker Seth Fogie, CEO, Airscanner USA; leading-edge mobile security researcher; coauthor of Security Warrior Dr. Sushil Jajodia, Director, Center for Secure Information Systems; founding Editor-in-Chief, Journal of Computer Security Dr. Steven Noel, Associate Director and Senior Research Scientist, Center for Secure Information Systems, George Mason University Alex Kirk, Member, Sourcefire Vulnerability Research Team

Psychological and Behavioral Examinations in Cyber Security Springer

In distributed, open systems like cyberspace, where the behavior of autonomous agents is uncertain and can affect other agents' welfare, trust management is used to allow agents to determine what to expect about the behavior of other agents. The role of trust management is to maximize trust between the parties and thereby provide a basis for cooperation to develop. Bringing together expertise from technology-oriented sciences, law, philosophy, and social sciences, Managing Trust in Cyberspace addresses fundamental issues underpinning computational trust models and covers trust management processes for dynamic open systems and applications in a tutorial style that aids in understanding. Topics include trust in autonomic and self-organized networks, cloud computing, embedded computing, multi-agent systems, digital rights management, security and quality issues in trusting e-government service delivery, and context-aware e-commerce applications. The book also presents a walk-through of online identity management and examines using trust and argumentation in recommender systems. It concludes with a comprehensive survey of anti-forensics for network security and a review of password security and protection. Researchers and practitioners in fields such as distributed computing, Internet technologies, networked systems, information systems, human computer interaction, human behavior modeling, and intelligent informatics especially benefit from a discussion of future trust management research directions including pervasive and ubiquitous computing, wireless ad-hoc and sensor networks, cloud computing, social networks, e-services, P2P networks, near-field communications (NFC), electronic knowledge management, and nano-communication networks.

Criticality in neural network behavior and its implications for computational processing in healthy and perturbed conditions Springer Nature

Advanced Data Mining Tools and Methods for Social Computing explores advances in the latest data mining tools, methods, algorithms and the architectures being developed specifically for social computing and social network analysis. The book reviews major emerging trends in technology that are supporting current advancements in social networks, including data mining techniques and tools. It also aims to highlight the advancement of conventional approaches in the field of social networking. Chapter coverage includes reviews of novel techniques and state-of-the-art advances in the area of data mining, machine learning, soft computing techniques, and their applications in the field of social network analysis. Provides insights into the latest research trends in social network analysis Covers a broad range of data mining tools and methods for social computing and analysis Includes practical examples and case studies across a range of tools and methods Features coding examples and supplementary data sets in every chapter

Network Behavior Analysis "O'Reilly Media, Inc."

Social networks provide a powerful abstraction of the structure and dynamics of diverse kinds of people or people-to-technology interaction. Web 2.0 has enabled a new generation of web-based communities, social networks, and folksonomies to facilitate collaboration among different communities. This unique text/reference compares and contrasts the ethological approach to social behavior in animals with web-based evidence of social interaction, perceptual learning, information granulation, the behavior of humans and affinities between web-based social networks. An international team of leading experts present the latest advances of various topics in intelligent-social-networks and illustrates how organizations can gain competitive advantages by applying the different emergent techniques in real-world scenarios. The work incorporates experience reports, survey articles, and intelligence techniques and theories with specific network technology problems. Topics and Features: Provides an overview social network tools, and explores methods for discovering key players in social networks, designing self-organizing search systems, and clustering blog sites, surveys techniques for exploratory analysis and text mining of social networks, approaches to tracking online community interaction, and examines how the topological features of a system affects the flow of information, reviews the models of network evolution, covering scientific co-citation networks, nature-inspired frameworks, latent social networks in e-Learning systems, and compound communities, examines the relationship between the intent of web pages, their architecture and the communities who take part in their usage and creation, discusses team selection based on members' social context, presents social network applications, including music recommendation and face recognition in photographs, explores the use of social networks in web services that focus on the discovery stage in the life cycle of these web services. This useful and comprehensive volume will be indispensible to senior undergraduate and postgraduate students taking courses in Social Intelligence, as well as to

researchers, developers, and postgraduates interested in intelligent-social-networks research and related areas.

Predicting Malicious Behavior John Wiley & Sons

As the sophistication of cyber-attacks increases, understanding how to defend critical infrastructure systems—energy production, water, gas, and other vital systems—becomes more important, and heavily mandated. Industrial Network Security, Second Edition arms you with the knowledge you need to understand the vulnerabilities of these distributed supervisory and control systems. The book examines the unique protocols and applications that are the foundation of industrial control systems, and provides clear guidelines for their protection. This how-to guide gives you thorough understanding of the unique challenges facing critical infrastructures, new guidelines and security measures for critical infrastructure protection, knowledge of new and evolving security tools, and pointers on SCADA protocols and security implementation. All-new real-world examples of attacks against control systems, and more diagrams of systems Expanded coverage of protocols such as 61850, Ethernet/IP, CIP, ISA-99, and the evolution to IEC62443 Expanded coverage of Smart Grid security New coverage of signature-based detection, exploit-based vs. vulnerability-based detection, and signature reverse engineering

IoT as a Service Springer Nature

This book constitutes the refereed proceedings of the 8th International Conference on Internet and Distributed Computing Systems, IDCS 2015, held in Windsor, UK, in September 2015. The 19 revised full and 6 revised short papers presented were carefully reviewed and selected from 42 submissions. The selected contributions covered cutting-edge aspects of Cloud Computing and Internet of Things, sensor networks, parallel and distributed computing, advanced networking, smart cities and smart buildings, Big Data and social networks.

Mastering Viruses Springer Nature

Understand malware analysis and its practical implementation Key Features Explore the key concepts of malware analysis and memory forensics using real-world examples Learn the art of detecting, analyzing, and investigating malware threats Understand adversary tactics and techniques Book Description Malware analysis and memory forensics are powerful analysis and investigation techniques used in reverse engineering, digital forensics, and incident response. With adversaries becoming sophisticated and carrying out advanced malware attacks on critical infrastructures, data centers, and private and public organizations, detecting, responding to, and investigating such intrusions is critical to information security professionals. Malware analysis and memory forensics have become must-have skills to fight advanced malware, targeted attacks, and security breaches. This book teaches you the concepts, techniques, and tools to understand the behavior and characteristics of malware through malware analysis. It also teaches you techniques to investigate and hunt malware using memory forensics. This book introduces you to the basics of malware analysis, and then gradually progresses into the more advanced concepts of code analysis and memory forensics. It uses real-world malware samples, infected memory images, and visual diagrams to help you gain a better understanding of the subject and to equip you with the skills required to analyze, investigate, and respond to malware-related incidents. What you will learn Create a safe and isolated lab environment for malware analysis Extract the metadata associated with malware Determine malware's interaction with the system Perform code analysis using IDA Pro and x64dbg Reverse-engineer various malware functionalities Reverse engineer and decode common encoding/encryption algorithms Reverse-engineer malware code injection and hooking techniques Investigate and hunt malware using memory forensics Who this book is for This book is for incident responders, cyber-security investigators, system administrators, malware analyst, forensic practitioners, student, or curious security professionals interested in learning malware analysis and memory forensics. Knowledge of programming languages such as C and Python is helpful but is not mandatory. If you have written few lines of code and have a basic understanding of programming concepts, you'll be able to get most out of this book.

Related with Network Behavior Analysis Tools:
© Network Behavior Analysis Tools What Is Torsional Strain In Organic Chemistry
© Network Behavior Analysis Tools What Is The Solution To Mc003 1jpg
© Network Behavior Analysis Tools What Is The Official Language Of Guatemala