Computational Intelligence Cyber Security And Computational Models Proceedings Of Icc3 2015 Advances In Intelligent Systems And Computing

This book provides stepwise discussion, exhaustive literature review, detailed analysis and discussion, rigorous experimentation results (using several analytics tools), and an application-oriented approach that can be demonstrated with respect to data analytics using artificial intelligence to make systems stronger (i.e., impossible to breach). We can see many serious cyber breaches on Government databases or public profiles at online social networking in the recent decade. Today artificial intelligence or machine learning is redefining every aspect of cyber security. From improving organizations' ability to anticipate and thwart breaches, protecting the proliferating number of threat surfaces with Zero Trust Security frameworks to making passwords obsolete, AI and machine learning are essential to securing the perimeters of any business. The book is useful for researchers, academics, industry players, data engineers, data scientists, governmental organizations, and non-governmental organizations. The book provides an advanced vision and trends of computational intelligence in cyberspace and cyber-enabled spaces. It reviews architectures and models, as well as state-of-the-art computational and interpretation capabilities for social, industrial, and multimedia applications. Cyber-enabled intelligence involves the design and development of intelligent and innovative application scenarios in social networks, computer vision, multimedia, and image processing. Application scenarios can also cover the applicability of intelligent sensing, data collection and predictive analysis in Internet of Things.

Artificial intelligence (AI) and data mining is the fastest growing field in computer science. AI and data mining algorithms and techniques are found to be useful in different areas like pattern recognition, automatic threat detection, automatic problem solving, visual recognition, fraud detection, detecting developmental delay in children, and many other applications. However, applying AI and data mining techniques or algorithms successfully in these areas needs a concerted effort, fostering integrative research between experts ranging from diverse disciplines from data science to Artificial Intelligence. Successful application of security frameworks to enable meaningful, cost effective, personalize security service is a primary aim of engineers and researchers today. However realizing this goal requires effective understanding, application and amalgamation of AI and Data Mining and several other computing technologies to deploy such system in an effective manner. This book provides state of the art approaches of artificial intelligence and data mining in these areas. It includes areas of detection, prediction, as well as future framework identification, development, building service systems and analytical aspects. In all these topics, applications of AI and data mining, such as artificial neural networks, fuzzy logic, genetic algorithm and hybrid mechanisms, are explained and explored. This book is aimed at the modeling and performance prediction of efficient security framework systems, bringing to light a new dimension in the theory and practice. This groundbreaking new volume presents these topics and trends, bridging the research gap on AI and data mining to enable wide-scale implementation. Whether for the veteran engineer or the student, this is a must-have for any library.

Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or OpportunitiesSpringer

Recently, cryptology problems, such as designing good cryptographic systems and analyzing them, have been challenging researchers. Many algorithms that take advantage of approaches based on computational intelligence techniques, such as genetic algorithms, genetic programming, and so on, have been proposed to solve these issues. Implementing Computational Intelligence Techniques for Security Systems Design is an essential research

book that explores the application of computational intelligence and other advanced techniques in information security, which will contribute to a better understanding of the factors that influence successful security systems design. Featuring a range of topics such as encryption, self-healing systems, and cyber fraud, this book is ideal for security analysts, IT specialists, computer engineers, software developers, technologists, academicians, researchers, practitioners, and students.

This book aims at promoting high-quality research by researchers and practitioners from academia and industry at the International Conference on Computational Intelligence, Cyber Security, and Computational Models ICC3 2015 organized by PSG College of Technology, Coimbatore, India during December 17 – 19, 2015. This book enriches with innovations in broad areas of research like computational modeling, computational intelligence and cyber security. These emerging inter disciplinary research areas have helped to solve multifaceted problems and gained lot of attention in recent years. This encompasses theory and applications, to provide design, analysis and modeling of the aforementioned key areas.

This book presents the outcomes of the 2020 International Conference on Cyber Security Intelligence and Analytics (CSIA 2020), an international conference dedicated to promoting novel theoretical and applied research advances in the interdisciplinary field of cyber security, particularly focusing on threat intelligence, analytics, and countering cyber crime. The conference provides a forum for presenting and discussing innovative ideas, cutting-edge research findings, and novel techniques, methods and applications on all aspects of Cyber Security Intelligence and Analytics. The 2020 International Conference on Cyber Security Intelligence and Analytics (CSIA 2020) is held at Feb. 28-29, 2020, in Haikou, China, building on the previous successes in Wuhu, China (2019) is proud to be in the 2nd consecutive conference year.

This book contains cutting-edge research material presented by researchers, engineers, developers, and practitioners from academia and industry at the International Conference on Computational Intelligence, Cyber Security and Computational Models (ICC3) organized by PSG College of Technology, Coimbatore, India during December 19–21, 2013. The materials in the book include theory and applications to provide design, analysis, and modeling of the key areas. The book will be useful material for students, researchers, professionals, as well academicians in understanding current research trends and findings and future scope of research in computational intelligence, cyber security, and computational models.

This book presents the outcomes of the 2020 International Conference on Cyber Security Intelligence and Analytics (CSIA 2020), which was dedicated to promoting novel theoretical and applied research advances in the interdisciplinary field of cyber security, particularly those focusing on threat intelligence, analytics, and preventing cyber crime. The conference provides a forum for presenting and discussing innovative ideas, cutting-edge research findings, and novel techniques, methods, and applications concerning all aspects of cyber security intelligence and analytics. CSIA 2020, which was held in Haikou, China on February 28–29, 2020, built on the previous conference in Wuhu, China (2019), and marks the series' second successful installment.

This book presents state-of-the-art solutions to the theoretical and practical challenges stemming from the leverage of big data and its computational intelligence in supporting smart network operation, management, and optimization. In particular, the technical focus covers the comprehensive understanding of network big data, efficient collection and management of network big data, distributed and scalable online analytics for network big data, and emerging applications of network big data for computational intelligence.

This book presents the latest advances in machine intelligence and big data analytics to improve early warning of cyber-attacks, for cybersecurity intrusion detection and monitoring, and malware analysis. Cyber-attacks have posed real and wide-ranging threats for the

information society. Detecting cyber-attacks becomes a challenge, not only because of the sophistication of attacks but also because of the large scale and complex nature of today's IT infrastructures. It discusses novel trends and achievements in machine intelligence and their role in the development of secure systems and identifies open and future research issues related to the application of machine intelligence in the cybersecurity field. Bridging an important gap between machine intelligence, big data, and cybersecurity communities, it aspires to provide a relevant reference for students, researchers, engineers, and professionals working in this area or those interested in grasping its diverse facets and exploring the latest advances on machine intelligence and big data analytics for cybersecurity applications.

As industries are rapidly being digitalized and information is being more heavily stored and transmitted online, the security of information has become a top priority in securing the use of online networks as a safe and effective platform. With the vast and diverse potential of artificial intelligence (AI) applications, it has become easier than ever to identify cyber vulnerabilities, potential threats, and the identification of solutions to these unique problems. The latest tools and technologies for AI applications have untapped potential that conventional systems and human security systems cannot meet, leading AI to be a frontrunner in the fight against malware, cyber-attacks, and various security issues. However, even with the tremendous progress AI has made within the sphere of security, it's important to understand the impacts, implications, and critical issues and challenges of AI applications along with the many benefits and emerging trends in this essential field of security-based research. Research Anthology on Artificial Intelligence Applications in Security seeks to address the fundamental advancements and technologies being used in AI applications for the security of digital data and information. The included chapters cover a wide range of topics related to AI in security stemming from the development and design of these applications, the latest tools and technologies, as well as the utilization of AI and what challenges and impacts have been discovered along the way. This resource work is a critical exploration of the latest research on security and an overview of how AI has impacted the field and will continue to advance as an essential tool for security, safety, and privacy online. This book is ideally intended for cyber security analysts, computer engineers, IT specialists, practitioners, stakeholders, researchers, academicians, and students interested in AI applications in the realm of security research.

Cyberwarfare has become an important concern for governmental agencies as well businesses of various types. This timely volume, with contributions from some of the internationally recognized, leaders in the field, gives readers a glimpse of the new and emerging ways that Computational Intelligence and Machine Learning methods can be applied to address problems related to cyberwarfare. The book includes a number of chapters that can be conceptually divided into three topics: chapters describing different data analysis methodologies with their applications to cyberwarfare, chapters presenting a number of intrusion detection approaches, and chapters dedicated to analysis of possible cyber attacks and their impact. The book provides the readers with a variety of methods and techniques, based on computational intelligence, which can be applied to the broad domain of cyberwarfare.

This book is dedicated to applied computational intelligence and soft computing techniques with special reference to decision support in Cyber Physical Systems (CPS), where the physical as well as the communication segment of the networked entities interact with each other. The joint dynamics of such systems result in a complex combination of computers, software, networks and physical processes all combined to establish a process flow at system level. This volume provides the audience with an in-depth vision about how to ensure dependability, safety, security and efficiency in real time by making use of computational intelligence in various CPS applications ranging from the nano-world to large scale wide area systems of systems. Key application areas include healthcare, transportation, energy, process

control and robotics where intelligent decision support has key significance in establishing dynamic, ever-changing and high confidence future technologies. A recommended text for graduate students and researchers working on the applications of computational intelligence methods in CPS.

This book presents a collection of state-of-the-art AI approaches to cybersecurity and cyberthreat intelligence, offering strategic defense mechanisms for malware, addressing cybercrime, and assessing vulnerabilities to yield proactive rather than reactive countermeasures. The current variety and scope of cybersecurity threats far exceed the capabilities of even the most skilled security professionals. In addition, analyzing yesterday's security incidents no longer enables experts to predict and prevent tomorrow's attacks, which necessitates approaches that go far beyond identifying known threats. Nevertheless, there are promising avenues: complex behavior matching can isolate threats based on the actions taken, while machine learning can help detect anomalies, prevent malware infections, discover signs of illicit activities, and protect assets from hackers. In turn, knowledge representation enables automated reasoning over network data, helping achieve cybersituational awareness. Bringing together contributions by high-caliber experts, this book suggests new research directions in this critical and rapidly growing field.

Experts from MIT explore recent advances in cybersecurity, bringing together management, technical, and sociological perspectives. Ongoing cyberattacks, hacks, data breaches, and privacy concerns demonstrate vividly the inadequacy of existing methods of cybersecurity and the need to develop new and better ones. This book brings together experts from across MIT to explore recent advances in cybersecurity from management, technical, and sociological perspectives. Leading researchers from MIT's Computer Science & Artificial Intelligence Lab, the MIT Media Lab, MIT Sloan School of Management, and MIT Lincoln Lab, along with their counterparts at Draper Lab, the University of Cambridge, and SRI, discuss such varied topics as a systems perspective on managing risk, the development of inherently secure hardware, and the Dark Web. The contributors suggest approaches that range from the market-driven to the theoretical, describe problems that arise in a decentralized, IoT world, and reimagine what optimal systems architecture and effective management might look like. Contributors YNadav Aharon, Yaniv Altshuler, Manuel Cebrian, Nazli Choucri, André DeHon, Ryan Ellis, Yuval Elovici, Harry Halpin, Thomas Hardjono, James Houghton, Keman Huang, Mohammad S. Jalali, Priscilla Koepke, Yang Lee, Stuart Madnick, Simon W. Moore, Katie Moussouris, Peter G. Neumann, Hamed Okhravi, Jothy Rosenberg, Hamid Salim,Michael Siegel, Diane Strong, Gregory T. Sullivan, Richard Wang, Robert N. M. Watson, Guy Zyskind An MIT Connection Science and Engineering Book

This book presents the outcomes of the 2021 International Conference on Cyber Security Intelligence and Analytics (CSIA 2021), an international conference dedicated to promoting novel theoretical and applied research advances in the interdisciplinary field of cyber security, particularly focusing on threat intelligence, analytics, and countering cybercrime. The conference provides a forum for presenting and discussing innovative ideas, cutting-edge research findings and novel techniques, methods and applications on all aspects of cyber security intelligence and analytics. Due to COVID-19, Authors, Keynote Speakers and PC committees will attend the conference online. .

This book is a pioneering yet primary general reference resource on cyber physical systems and their security concerns. Providing a fundamental theoretical background, and a clear and comprehensive overview of security issues in the domain of cyber physical systems, it is useful for students in the fields of information technology, computer science, or computer engineering where this topic is a substantial emerging area of study.

In recent years, interest and progress in the area of artificial intelligence (AI) and machine learning (ML) have boomed, with new applications vigorously pursued across many sectors. At

the same time, the computing and communications technologies on which we have come to rely present serious security concerns: cyberattacks have escalated in number, frequency, and impact, drawing increased attention to the vulnerabilities of cyber systems and the need to increase their security. In the face of this changing landscape, there is significant concern and interest among policymakers, security practitioners, technologists, researchers, and the public about the potential implications of AI and ML for cybersecurity. The National Academies of Sciences, Engineering, and Medicine convened a workshop on March 12-13, 2019 to discuss and explore these concerns. This publication summarizes the presentations and discussions from the workshop.

This book constitutes the proceedings of the Third International Conference on Computational Intelligence, Cyber Security, and Computational Models, ICC3 2017, which was held in Coimbatore, India, in December 2017. The 15 papers presented in this volume were carefully reviewed and selected from 63 submissions. They were organized in topical sections named: computational intelligence; cyber security; and computational models.

The history of robotics and artificial intelligence in many ways is also the history of humanity's attempts to control such technologies. From the Golem of Prague to the military robots of modernity, the debate continues as to what degree of independence such entities should have and how to make sure that they do not turn on us, its inventors. Numerous recent advancements in all aspects of research, development and deployment of intelligent systems are well publicized but safety and security issues related to AI are rarely addressed. This book is proposed to mitigate this fundamental problem. It is comprised of chapters from leading AI Safety researchers addressing different aspects of the AI control problem as it relates to the development of safe and secure artificial intelligence. The book is the first edited volume dedicated to addressing challenges of constructing safe and secure advanced machine intelligence. The chapters vary in length and technical content from broad interest opinion essays to highly formalized algorithmic approaches to specific problems. All chapters are self-contained and could be read in any order or skipped without a loss of comprehension.

This book provides readers with up-to-date research of emerging cyber threats and defensive mechanisms, which are timely and essential. It covers cyber threat intelligence concepts against a range of threat actors and threat tools (i.e. ransomware) in cutting-edge technologies, i.e., Internet of Things (IoT), Cloud computing and mobile devices. This book also provides the technical information on cyber-threat detection methods required for the researcher and digital forensics experts, in order to build intelligent automated systems to fight against advanced cybercrimes. The ever increasing number of cyber-attacks requires the cyber security and forensic specialists to detect, analyze and defend against the cyber threats in almost real-time, and with such a large number of attacks is not possible without deeply perusing the attack features and taking corresponding intelligent defensive actions – this in essence defines cyber threat intelligence notion. However, such intelligence would not be possible without the aid of artificial intelligence, machine learning and advanced data mining techniques to collect, analyze, and interpret cyber-attack campaigns which is covered in this book. This book will focus on cutting-edge research from both academia and industry, with a particular emphasis on providing wider knowledge of the field, novelty of approaches, combination of tools and so forth to perceive reason, learn and act on a wide range of data collected from different cyber security and forensics solutions. This book introduces the notion of cyber threat intelligence and analytics and presents different attempts in utilizing machine learning and data mining techniques to create threat feeds for a range of consumers. Moreover, this book sheds light on existing and

emerging trends in the field which could pave the way for future works. The inter-disciplinary nature of this book, makes it suitable for a wide range of audiences with backgrounds in artificial intelligence, cyber security, forensics, big data and data mining, distributed systems and computer networks. This would include industry professionals, advanced-level students and researchers that work within these related fields.

This book constitutes the proceedings of the 4th International Conference on Computational Intelligence, Cyber Security, and Computational Models, ICC3 2019, which was held in Coimbatore, India, in December 2019. The 9 papers presented in this volume were carefully reviewed and selected from 38 submissions. They were organized in topical sections named: computational intelligence; cyber security; and computational models.

The rate of cybercrimes is increasing because of the fast-paced advancements in computer and internet technology. Crimes employing mobile devices, data embedding/mining systems, computers, network communications, or any malware impose a huge threat to data security. Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems addresses current problems and issues emerging in cyber forensics and investigations and proposes new solutions that can be adopted and implemented to counter security breaches within various organizations. The publication examines a variety of topics such as advanced techniques for forensic developments in computer and communication-link environments and legal perspectives including procedures for cyber investigations, standards, and policies. It is designed for policymakers, forensic analysts, technology developers, security administrators, academicians, researchers, and students.

This book reviews IoT-centric vulnerabilities from a multidimensional perspective by elaborating on IoT attack vectors, their impacts on well-known security objectives, attacks which exploit such vulnerabilities, coupled with their corresponding remediation methodologies. This book further highlights the severity of the IoT problem at large, through disclosing incidents of Internet-scale IoT exploitations, while putting forward a preliminary prototype and associated results to aid in the IoT mitigation objective. Moreover, this book summarizes and discloses findings, inferences, and open challenges to inspire future research addressing theoretical and empirical aspects related to the imperative topic of IoT security. At least 20 billion devices will be connected to the Internet in the next few years. Many of these devices transmit critical and sensitive system and personal data in real-time. Collectively known as “the Internet of Things” (IoT), this market represents a $267 billion per year industry. As valuable as this market is, security spending on the sector barely breaks 1%. Indeed, while IoT vendors continue to push more IoT devices to market, the security of these devices has often fallen in priority, making them easier to exploit. This drastically threatens the privacy of the consumers and the safety of mission-critical systems. This book is intended for cybersecurity researchers and advanced-level students in computer science. Developers and operators working in this field, who are eager to comprehend the vulnerabilities of the Internet of Things (IoT) paradigm and understand the severity of accompanied security issues will also be interested in this book.

Cyber-physical systems (CPS) have emerged as a unifying name for systems where

cyber parts (i.e., the computing and communication parts) and physical parts are tightly integrated, both in design and during operation. Such systems use computations and communication deeply embedded in and interacting with human physical processes as well as augmenting existing and adding new capabilities. As such, CPS is an integration of computation, networking, and physical processes. Embedded computers and networks monitor and control the physical processes, with feedback loops where physical processes affect computations and vice versa. The economic and societal potential of such systems is vastly greater than what has been realized, and major investments are being made worldwide to develop the technology.

Artificial Intelligence Paradigms for Smart Cyber-Physical Systems focuses on the recent advances in Artificial intelligence-based approaches towards affecting secure cyber-physical systems. This book presents investigations on state-of-the-art research issues, applications, and achievements in the field of computational intelligence paradigms for CPS. Covering topics that include autonomous systems, access control, machine learning, and intrusion detection and prevention systems, this book is ideally designed for engineers, industry professionals, practitioners, scientists, managers, students, academicians, and researchers seeking current research on artificial intelligence and cyber-physical systems.

This book contains accepted papers presented at CISIS 2020 held in the beautiful and historic city of Burgos (Spain), in September 2020. The aim of the CISIS 2020 conference is to offer a meeting opportunity for academic and industry-related researchers belonging to the various, vast communities of computational intelligence, information security, and data mining. The need for intelligent, flexible behaviour by large, complex systems, especially in mission-critical domains, is intended to be the catalyst and the aggregation stimulus for the overall event. After a thorough peer-review process, the CISIS 2020 International Program Committee selected 43 papers which are published in these conference proceedings achieving an acceptance rate of 28%. Due to the COVID-19 outbreak, the CISIS 2020 edition was blended, combining on-site and on-line participation. In this relevant edition, a special emphasis was put on the organization of five special sessions related to relevant topics as Fake News Detection and Prevention, Mathematical Methods and Models in Cybersecurity, Measurements for a Dynamic Cyber-Risk Assessment, Cybersecurity in a Hybrid Quantum World, Anomaly/Intrusion Detection, and From the least to the least: cryptographic and data analytics solutions to fulfil least minimum privilege and endorse least minimum effort in information systems. The selection of papers was extremely rigorous in order to maintain the high quality of the conference and we would like to thank the members of the Program Committees for their hard work in the reviewing process. This is a crucial process to the creation of a high standard conference, and the CISIS conference would not exist without their help.
This book presents the outcomes of the 2021 International Conference on Cyber Security Intelligence and Analytics (CSIA 2021), an international conference dedicated to promoting novel theoretical and applied research advances in the interdisciplinary field of cyber security, particularly focusing on threat intelligence, analytics, and countering cybercrime. The conference provides a forum for presenting and discussing

innovative ideas, cutting-edge research findings and novel techniques, methods and applications on all aspects of cyber security intelligence and analytics. Due to COVID-19, Authors, Keynote Speakers and PC committees will attend the conference online.

The aim of the book is to analyse and understand the impacts of artificial intelligence in the fields of national security and defense; to identify the political, geopolitical, strategic issues of AI; to analyse its place in conflicts and cyberconflicts, and more generally in the various forms of violence; to explain the appropriation of artificial intelligence by military organizations, but also law enforcement agencies and the police; to discuss the questions that the development of artificial intelligence and its use raise in armies, police, intelligence agencies, at the tactical, operational and strategic levels.

The world of cybersecurity and the landscape that it possesses is changing on a dynamic basis. It seems like that hardly one threat vector is launched, new variants of it are already on the way. IT Security teams in businesses and corporations are struggling daily to fight off any cyberthreats that they are experiencing. On top of this, they are also asked by their CIO or CISO to model what future Cyberattacks could potentially look like, and ways as to how the lines of defenses can be further enhanced. IT Security teams are overburdened and are struggling to find ways in order to keep up with what they are being asked to do. Trying to model the cyberthreat landscape is a very laborious process, because it takes a lot of time to analyze datasets from many intelligence feeds. What can be done to accomplish this Herculean task? The answer lies in Artificial Intelligence (AI). With AI, an IT Security team can model what the future Cyberthreat landscape could potentially look like in just a matter of minutes. As a result, this gives valuable time for them not only to fight off the threats that they are facing, but to also come up with solutions for the variants that will come out later. Practical AI for Cybersecurity explores the ways and methods as to how AI can be used in cybersecurity, with an emphasis upon its subcomponents of machine learning, computer vision, and neural networks. The book shows how AI can be used to help automate the routine and ordinary tasks that are encountered by both penetration testing and threat hunting teams. The result is that security professionals can spend more time finding and discovering unknown vulnerabilities and weaknesses that their systems are facing, as well as be able to come up with solid recommendations as to how the systems can be patched up quickly.

This book presents state-of-the-art research on artificial intelligence and blockchain for future cybersecurity applications. The accepted book chapters covered many themes, including artificial intelligence and blockchain challenges, models and applications, cyber threats and intrusions analysis and detection, and many other applications for smart cyber ecosystems. It aspires to provide a relevant reference for students, researchers, engineers, and professionals working in this particular area or those interested in grasping its diverse facets

and exploring the latest advances on artificial intelligence and blockchain for future cybersecurity applications.

Build smart cybersecurity systems with the power of machine learning and deep learning to protect your corporate assets Key Features Identify and predict security threats using artificial intelligence Develop intelligent systems that can detect unusual and suspicious patterns and attacks Learn how to test the effectiveness of your AI cybersecurity algorithms and tools Book Description Today's organizations spend billions of dollars globally on cybersecurity. Artificial intelligence has emerged as a great solution for building smarter and safer security systems that allow you to predict and detect suspicious network activity, such as phishing or unauthorized intrusions. This cybersecurity book presents and demonstrates popular and successful AI approaches and models that you can adapt to detect potential attacks and protect your corporate systems. You'll learn about the role of machine learning and neural networks, as well as deep learning in cybersecurity, and you'll also learn how you can infuse AI capabilities into building smart defensive mechanisms. As you advance, you'll be able to apply these strategies across a variety of applications, including spam filters, network intrusion detection, botnet detection, and secure authentication. By the end of this book, you'll be ready to develop intelligent systems that can detect unusual and suspicious patterns and attacks, thereby developing strong network security defenses using AI. What you will learn Detect email threats such as spamming and phishing using AI Categorize APT, zero-days, and polymorphic malware samples Overcome antivirus limits in threat detection Predict network intrusions and detect anomalies with machine learning Verify the strength of biometric authentication procedures with deep learning Evaluate cybersecurity strategies and learn how you can improve them Who this book is for If you’re a cybersecurity professional or ethical hacker who wants to build intelligent systems using the power of machine learning and AI, you’ll find this book useful. Familiarity with cybersecurity concepts and knowledge of Python programming is essential to get the most out of this book.

This book presents a collection of state-of-the-art approaches to utilizing machine learning, formal knowledge bases and rule sets, and semantic reasoning to detect attacks on communication networks, including IoT infrastructures, to automate malicious code detection, to efficiently predict cyberattacks in enterprises, to identify malicious URLs and DGA-generated domain names, and to improve the security of mHealth wearables. This book details how analyzing the likelihood of vulnerability exploitation using machine learning classifiers can offer an alternative to traditional penetration testing solutions. In addition, the book describes a range of techniques that support data aggregation and data fusion to automate data-driven analytics in cyberthreat intelligence, allowing complex and previously unknown cyberthreats to be identified and classified, and countermeasures to be incorporated in novel incident response and intrusion detection mechanisms.