User Guide Fireeye

KIM EVELIN

Kirikon: Kurse of the Tigris Orb FireEye Deployment Made Easy
This book constitutes the refereed proceedings of the International Symposium on Security in Computing and Communications, SSCC 2015, held in Kochi, India, in August 2015. The 36 revised full papers presented together with 13 short papers were carefully reviewed and selected from 157 submissions. The papers are organized in topical sections on security in cloud computing; authentication and access control systems; cryptography and steganography; system and network security; application security.
Information Technology for Peace and Security Rutgers University Press
The implementation of wireless sensor networks has wide-ranging applications for monitoring various physical and environmental settings. However, certain limitations with these technologies must be addressed in order to effectively utilize them. The Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures is a pivotal reference source for the latest research on recent innovations and developments in the field of wireless sensors. Examining the advantages and challenges presented by the application of these networks in various areas, this book is ideally designed for academics, researchers, students, and IT developers.
NTP Security IGI Global
This book includes best selected, high-quality research papers presented at the International Conference on Intelligent Manufacturing and Energy Sustainability (ICIMES 2020) held at the Department of Mechanical Engineering, Malla Reddy College of Engineering & Technology (MRCET), Maisammaguda, Hyderabad, India, during August 21-22, 2020. It covers topics in the areas of automation, manufacturing technology and energy sustainability and also includes original works in the intelligent systems, manufacturing, mechanical, electrical, aeronautical, materials, automobile, bioenergy and energy sustainability.
Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings Apress
Learn the key objectives and most crucial concepts covered by the Security+ Exam SY0-601 with this comprehensive and practical Deluxe Study Guide Covers 100% of exam objectives including threats, attacks, and vulnerabilities; technologies and tools; architecture and design; identity and access management; risk management; cryptography and PKI, and much more... Includes interactive online learning environment and study tools with: 4 custom practice exams 100 Electronic Flashcards Searchable key term glossary Plus 33 Online Security+ Practice Lab Modules Expert Security+ SY0-601 exam preparation--Now with 33 Online Lab Modules The Fifth edition of CompTIA Security+ Deluxe Study Guide offers invaluable preparation for Exam SY0-601. Written by expert authors, Mike Chapple and David Seidl, the book covers 100% of the exam objectives with clear and concise explanations. Discover how to handle threats, attacks, and vulnerabilities using industry-standard tools and technologies, while gaining and understanding the role of architecture and design. Spanning topics from everyday tasks like identity and access management to complex subjects such as risk management and cryptography, this study guide helps you consolidate your knowledge base in preparation for the Security+ exam. Illustrative examples show how these processes play out in real-world scenarios, allowing you to immediately translate essential concepts to on-the-job application. Coverage of 100% of all exam objectives in this Study Guide means you'll be ready for: Attacks, Threats, and Vulnerabilities Architecture and Design Implementation Operations and Incident Response Governance, Risk, and Compliance Interactive learning environment Take your exam prep to the next level with Sybex's superior interactive online study tools. To access our learning environment, simply visit www.wiley.com/go/sybextestprep, register your book to receive your unique PIN, and instantly gain one year of FREE access after activation to: Interactive test bank with 4 bonus exams. Practice questions help you identify areas where further review is needed. 100 Electronic Flashcards to reinforce learning and last-minute prep before the exam. Comprehensive glossary in PDF format gives you instant access to the key terms so you are fully prepared. ABOUT THE PRACTICE LABS SECURITY+ LABS So you can practice with hands-on learning in a real environment, Sybex has bundled Practice Labs virtual labs that run from your browser. The registration code is included with the book and gives you 6 months unlimited access to Practice Labs CompTIA Security+ Exam SY0-601 Labs with 33 unique lab modules to practice your skills.
Cengage Learning
Competitors are contesting the rules of the international system and U.S. leadership and their approaches lie in the “gray zone.” The United States needs a concrete and actionable campaign plan is needed to deal with this challenge.
Security in Computing and Communications Oxford University Press
This best-selling guide provides a complete, practical, up-to-date introduction to network and computer security. SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS, Fifth Edition, maps to the new CompTIA Security+ SY0-401 Certification Exam, providing thorough coverage of all domain objectives to help readers prepare for professional certification and career success. The text covers the essentials of network security, including compliance and operational security; threats and vulnerabilities; application, data, and host security; access control and identity management; and cryptography. The extensively updated Fifth Edition features a new structure based on major domains, a new chapter dedicated to mobile device security, expanded coverage of attacks and defenses, and new and updated information reflecting recent developments and emerging trends in information security, such as virtualization. New hands-on and case activities help readers review and apply what they have learned, and end-of-chapter exercises direct readers to the Information Security Community Site for additional activities and a wealth of learning resources, including blogs, videos , and current news and information relevant to the information security field. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.
CompTIA CySA+ Guide to Cybersecurity Analyst (CS0-002) Lulu.com
The Oxford Handbook of Cyber Security presents forty-eight chapters examining the technological, economic, commercial, and strategic aspects of cyber security, including studies at the international, regional, amd national level.
Concepts, Methodologies, Tools, and Applications Routledge
The United States is at a crossroads. Despite a defense budget that dwarfs that of any of the nation's rivals, the marginal return on this investment has decreased dramatically since the end of World War II. Why? Why have America's rivals, despite inferior resources, increasingly set the terms of international competition? How might America's leaders reconsider the application of power to ensure a favorable place on an increasingly crowded global stage? By tracing the geographic and historical development of four global actors--Russia, Iran, China, and the United States--Phillip T. Lohaus illuminates four equally distinct approaches to competition outside of warfare. He argues that while America's actions may have birthed information as a currency of power, the nation's failure to fully grasp the implications of this transition has created critical opportunities for its rivals to increase their power at the expense of the United States. The American way of competition, rooted in a scientific understanding of warfare, may impede effectiveness in the amorphous and unscientific landscape of twenty-first-century competition. From Rome to Britain, complacency has contributed to the downfall of many empires. Yet the slow bleed of American power may still be stanched by an approach to competition that emphasizes subtlety, diffusion, and ubiquity. America has developed and used these tools in the past--its very survival may hinge on returning to them. Power and Complacency defines the differing perspectives of America's international conflicts and

offers possible solutions for reformulating its superpower strengths.
Moving Forward EU-India Relations Jones & Bartlett Learning
This book is a multi-disciplinary analysis of cyber warfare, featuring contributions by leading experts from a mixture of academic and professional backgrounds. Cyber warfare, meaning interstate cyber aggression, is an increasingly important emerging phenomenon in international relations, with state-orchestrated (or apparently state-orchestrated) computer network attacks occurring in Estonia (2007), Georgia (2008) and Iran (2010). This method of waging warfare – given its potential to, for example, make planes fall from the sky or cause nuclear power plants to melt down – has the capacity to be as devastating as any conventional means of conducting armed conflict. Every state in the world now has a cyber-defence programme and over 120 states also have a cyber-attack programme. While the amount of literature on cyber warfare is growing within disciplines, our understanding of the subject has been limited by a lack of cross-disciplinary engagement. In response, this book, drawn from the fields of computer science, military strategy, international law, political science and military ethics, provides a critical overview of cyber warfare for those approaching the topic from whatever angle. Chapters consider the emergence of the phenomena of cyber warfare in international affairs; what cyber-attacks are from a technological standpoint; the extent to which cyber-attacks can be attributed to state actors; the strategic value and danger posed by cyber conflict; the legal regulation of cyber-attacks, both as international uses of force and as part of an on-going armed conflict, and the ethical implications of cyber warfare. This book will be of great interest to students of cyber warfare, cyber security, military ethics, international law, security studies and IR in general.
The Fire Eye Kronicles Springer
This book constitutes the refereed post-conference proceedings of the International Conference on Safety and Security in Internet of Things , SaSeIoT 2016, which was collocated with InterIoT and took place in Paris, France, in October 2016. The 14 revised full papers were carefully reviewed and selected from 22 submissions and cover all aspects of the latest research findings in the area of Internet of Things (IoT).
By Other Means Part I Springer
Relations between the European Union (EU) and India have been growing in quantity and quality in the last two decades. Alongside the economic dimension, the political and security elements of the relationship have emerged as the most promising area for further collaboration between the two sides. This volume brings together analyses and recommendations on EU-India security relations in the fields of: (i) maritime security and freedom of navigation; (ii) cyber security and data protection; (iii) space policy and satellite navigation; (iv) defence cooperation. The chapters have been written by a select pan-European and Indian group of experts tasked by the Rome-based Istituto Affari Internazionali (IAI) and the Mumbai-based Gateway House (GH) in the framework of the EU-India Think Tank Twinning Initiative – a public diplomacy project aimed at connecting research institutions in Europe and India funded by the EU. The book provides the reader with original research and innovative insights into how to move forward EU-India relations. It will be essential reading for scholars and policy makers interested in the subject.
Principles of Incident Response and Disaster Recovery Cisco Press
This updated and expanded edition of Cyberspace in Peace and War by Martin C. Libicki presents a comprehensive understanding of cybersecurity, cyberwar, and cyber-terrorism. From basic concepts to advanced principles, Libicki examines the sources and consequences of system compromises, addresses strategic aspects of cyberwar, and defines cybersecurity in the context of military operations while highlighting unique aspects of the digital battleground and strategic uses of cyberwar. This new edition provides updated analysis on cyberespionage, including the enigmatic behavior of Russian actors, making this volume a timely and necessary addition to the cyber-practitioner's library. Cyberspace in Peace and War guides readers through the complexities of cybersecurity and cyberwar and challenges them to understand the topics in new ways. Libicki provides the technical and geopolitical foundations of cyberwar necessary to understand the policies, operations, and strategies required for safeguarding an increasingly online infrastructure.
The Oxford Handbook of Cyber Security AuthorHouse
Jena is asked to guide a large group of hierophants into the dangerous mountains of Atlantis to perform a religious ceremony. Earthquakes are tearing the nation apart, and sending carnivorous reptiles into everyone’s kitchens, and this is an attempt to contact the earth elementals to begin a reversal. She has the usual wacky group of companions, and meets more along the way. The clock is ticking as other armies attempt to destroy the temple, and it’s a rough ride for all. A thorough exploration of this part of the continent, with its even more ancient ruins and underground caverns, Jena must turn from weapons to accomplish this with wit and humor
An Introductory Guide to Artificial Intelligence for Legal Professionals MIT Press
Computer security touches every part of our daily lives from our computers and connected devices to the wireless signals around us. Breaches have real and immediate financial, privacy, and safety consequences. This handbook has compiled advice from top professionals working in the real world about how to minimize the possibility of computer security breaches in your systems. Written for professionals and college students, it provides comprehensive best guidance about how to minimize hacking, fraud, human error, the effects of natural disasters, and more. This essential and highly-regarded reference maintains timeless lessons and is fully revised and updated with current information on security issues for social networks, cloud computing, virtualization, and more.
Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures IGI Global
The Arctic-Barents Region is facing numerous pressures from a variety of sources, including the effect of environmental changes and extractive industrial developments. The threats arising out of these pressures result in human security challenges. This book analyses the formation, and promotion, of societal security within the context of the Arctic-Barents Region. It applies the human security framework, which has increasingly gained currency at the UN level since 1994 (UNDP), as a tool to provide answers to many questions that face the Barents population today. The study explores human security dimensions such as environmental security, economic security, health, food, water, energy, communities, political security and digital security in order to assess the current challenges that the Barents population experiences today or may encounter in the future. In doing so, the book develops a comprehensive analysis of vulnerabilities, challenges and needs in the Barents Region and provides recommendations for new strategies to tackle insecurity and improve the wellbeing of both indigenous and local communities. This book will be a valuable tool for academics, policy-makers and students interested in environmental and human security, sustainable development, environmental studies and the Arctic and Barents Region in particular.
Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications Cengage Learning
Cyber security has become a topic of concern over the past decade as private industry, public administration, commerce, and communication have gained a greater online presence. As many individual and organizational activities continue to evolve in the digital sphere, new vulnerabilities arise. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications contains a compendium of the latest academic material on new methodologies and applications in the areas of digital security and threats. Including innovative studies on cloud security, online threat protection, and cryptography, this multi-volume book is an ideal source for IT specialists, administrators, researchers, and students interested in uncovering new ways to thwart cyber breaches and protect sensitive digital information.
Cybersecurity Policies and Strategies for Cyberwarfare Prevention Naval Institute Press
Eons ago, the Conclave of Sensi chose Cera as a laboratory for creating consciousness. True, the work was experimental, but it had been successful long before the rebellion that threatened to destroy the planet. Led by the High Priestess Khyan and her first apostle, Rhee, ten members of the Khyan Circle of Fostering decide upon a desperate plan for survival. Escaping a fiery destruction is only the beginning. The bizarre world that appears beneath them demands new risks. They must become something far different than what they have been. High up in the Fourth Valley of the White Mountains in this strange new homeland, the repulsive upright ones await their destiny. They have lived here for ages past, but they aren’t prepared for life in the future. Symbolic features in Legend of the Fire Eye promise to give it a niche in the "New Myth" now being written. At the same time, it will fit well on the traditional fantasy bookshelf.
Proceedings of ICIMES 2020 Springer
Learn the key objectives and most crucial concepts covered by the Security+ Exam SY0-601 with this comprehensive and practical study guide The Eighth Edition of the CompTIA Security+ Study Guide Exam SY0-601 efficiently and comprehensively prepares you for the SY0-601 Exam. Accomplished authors and security experts Mike Chapple and David Seidl walk you through the fundamentals of crucial security topics, including the five domains covered by the SY0-601 Exam: Attacks, Threats, and Vulnerabilities Architecture and Design Implementation Operations and Incident Response Governance, Risk, and Compliance The study guide comes with the Sybex online, interactive learning environment that includes a pre-assessment test, hundreds of review questions, practice exams, flashcards, and a glossary of key terms. The book is written in a practical and straightforward manner, ensuring you can easily learn and retain the material. Perfect for everyone planning to take the SY0-601 Exam—as well as those who hope to secure a high-level certification like the CASP+, CISSP, or CISA—the study guide also belongs on the bookshelves of everyone who has ever wondered if the field of IT security is right for them. It’s a must-have reference!
Jena of Atlantis, The Fire Eye iUniverse
FireEye Deployment Made EasyLulu.comCyber Warfare: A Documentary and Reference GuideABC-CLIO
CCNA Cybersecurity Operations Companion Guide John Wiley & Sons
Providing an invaluable introductory resource for students studying cyber warfare, this book highlights the evolution of cyber conflict in modern times through dozens of key primary source documents related to its development and implementation. This meticulously curated primary source collection is designed to offer a broad examination of key documents related to cyber warfare, covering the subject from multiple perspectives. The earliest documents date from the late 20th century, when the concept and possibility of cyber attacks became a reality, while the most recent documents are from 2019. Each document is accompanied by an introduction and analysis written by an expert in the field that provides the necessary context for readers to learn about the complexities of cyber warfare. The title's nearly 100 documents are drawn primarily but not exclusively from government sources and allow readers to understand how policy, strategy, doctrine, and tactics of cyber warfare are created and devised, particularly in the United States. Although the United States is the global leader in cyber capabilities and is largely driving the determination of norms within the cyber domain, the title additionally contains a small number of international documents. This invaluable work will serve as an excellent starting point for anyone seeking to understand the nature and character of international cyber warfare. Covers in detail one of the defining forms of conflict of the 21st century—cyber warfare will significantly impact virtually every American citizen over the next two decades Provides more than 90 primary source documents and matching analysis, allowing readers to investigate the underpinnings of cyber warfare Enables readers to see the development of different concepts of cyber warfare through its chronological organization Reflects the deep knowledge of an editor who is a noted expert in cyber warfare and has taught for the United States Air Force for more than a decade