User Guide Fireeye

TOWNSEND BROWN

Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications Cengage Learning
Learn how to identify vulnerabilities within computer networks and implement countermeasures that mitigate risks and damage with Whitman/Mattord's PRINCIPLES OF INCIDENT RESPONSE & DISASTER RECOVERY, 3rd Edition. This edition offers the knowledge you need to help organizations prepare for and avert system interruptions and natural disasters. Comprehensive coverage addresses information security and IT in contingency planning today. Updated content focuses on incident response and disaster recovery. You examine the complexities of organizational readiness from an IT and business perspective with emphasis on management practices and policy requirements. You review industry's best practices for minimizing downtime in emergencies and curbing losses during and after system service interruptions. This edition includes the latest NIST knowledge, expanded coverage of security information and event management (SIEM) and unified threat management, and more explanation of cloud-based systems and Web-accessible tools to prepare you for success. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Exam SY0-601 Cengage Learning
This book offers an introduction to Information Technology with regard to peace, conflict, and security research, a topic that it approaches from natural science, technical and computer science perspectives. Following an initial review of the fundamental roles of IT in connection with peace, conflict and security, the contributing authors address the rise of cyber conflicts via information warfare, cyber espionage, cyber defence and Darknets. The book subsequently explores recent examples of cyber warfare, including: • The Stuxnet attack on Iran’s uranium refining capability • The hacking of the German Federal Parliament’s internal communication system • The Wannacry malware campaign, which used software stolen from a US security agency to launch ransomware attacks worldwide The book then introduces readers to the concept of cyber peace, including a discussion of confidence and security-building

measures. A section on Cyber Arms Control draws comparisons to global efforts to control chemical warfare, to reduce the risk of nuclear war, and to prevent the militarization of space. Additional topics include the security of critical information infrastructures, and cultural violence and peace in social media. The book concludes with an outlook on the future role of IT in peace and security. Information Technology for Peace and Security breaks new ground in a largely unexplored field of study, and offers a valuable asset for a broad readership including students, educators and working professionals in computer science, IT security, peace and conflict studies, and political science.
American Survival in an Age of International Competition ABC-CLIO
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.
FireEye Deployment Made Easy Springer Nature
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).
Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings Springer
This book constitutes the thoroughly refereed proceedings of the 21st International Conference on Computer Networks, CN 2014, held in Brunów, Poland, in June 2014. The 34 revised full papers presented were carefully reviewed and selected for inclusion in the book. The papers in these proceedings cover the following topics: computer networks, tele informatics and communications, new technologies, queueing theory, innovative applications and networked and IT-related aspects of e-business.
Concepts, Methodologies, Tools, and Applications John Wiley & Sons
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.
The Fire Eye Kronicles Routledge
Scrappy fifteen-year-old Dallas Marge and his older brother, Logan, strive to live a normal life, in the infamous city of kaspers, Starfall City. However, an unspoken truth between the two siblings leads Dallas to find a mysterious orb imprisoning a malevolent entity called Oryga, the tiger god, that curses him with an unimaginable power. Training under the supervision of the formerly villainous dragon kasper, Singuard, Dallas adapts to his newfound strength. Anxious to test himself, he disregards Singuard’s warnings about the dangerously ominous and superpowered criminal underworld and the kasper hunting militia, GAUNTLET, challenging them both as Starfall’s first-ever vigilante, Kirikon. However, the novice mask, alongside his friends, struggle to save Starfall from a sinister duo of otherworldly creatures when they target him for reasons unknown. Discover the truth behind the tigris orb as Kirikon blasts his way into action in this adventurous and gripping chapter of a brand new series, The Fire Eye Kronicles.
CompTIA CySA+ Guide to Cybersecurity Analyst (CS0-002) Springer
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.
A Guide to Detecting and Responding to Healthcare Breaches and Events Springer
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.
Cyberwarfare: Information Operations in a Connected World Rowman & Littlefield
This book provides profound insights into industrial control system resilience, exploring fundamental and advanced topics and including practical examples and scenarios to support the theoretical approaches. It examines issues related to the safe operation of control systems, risk analysis and assessment, use of attack graphs to evaluate the resiliency of control systems, preventive maintenance, and malware detection and analysis. The book also discusses sensor networks and Internet of Things devices. Moreover, it covers timely responses to malicious attacks and hazardous situations, helping readers select the best approaches to handle such unwanted situations. The book is essential reading for engineers, researchers, and specialists addressing security and safety issues related to the implementation of modern industrial control systems. It is also a valuable resource for students interested in this area.
Information Technology: New Generations Jones & Bartlett Learning
The Internet of Things (IoT) is the notion that nearly everything we use, from gym shorts to streetlights, will soon be connected to the Internet; the Internet of Everything (IoE) encompasses not just objects, but the social connections, data, and processes that the IoT makes possible. Industry and financial analysts have predicted that the number of Internet-enabled devices will increase from 11 billion to upwards of 75 billion by 2020. Regardless of the number, the end result looks to be a mind-boggling explosion in Internet connected stuff. Yet, there has been relatively little attention paid to how we should go about regulating smart devices, and still less about how cybersecurity should be enhanced. Similarly, now that everything from refrigerators to stock exchanges can be connected to a ubiquitous Internet, how can we better safeguard privacy across networks and borders? Will security scale along with this increasingly crowded field? Or, will a combination of perverse incentives, increasing complexity, and new problems derail progress and exacerbate cyber insecurity? For all the press that such questions have received, the Internet of Everything remains a topic little understood or appreciated by the public. This volume demystifies our increasingly "smart" world, and unpacks many of the outstanding security, privacy, ethical, and policy challenges and opportunities represented by the IoE. Scott J. Shackelford provides real-world examples and straightforward discussion about how the IoE is impacting our lives, companies, and nations, and explain how it is increasingly shaping the international community in the twenty-first century. Are there any downsides of your phone being able to unlock your front door, start your car, and control your thermostat? Is your smart speaker always listening? How are other countries dealing with these issues? This book answers these questions, and more, along with offering practical guidance for how you can join the effort to help build an Internet of Everything that is as secure, private, efficient, and fun as possible.
Exam SY0-601 Kluwer Law International B.V.
Cyberwars in the Middle East argues that hacking is a form of online political disruption whose influence flows vertically in two directions (top-bottom or bottom-up) or horizontally. These hacking activities are performed along three political dimensions: international, regional, and local. Author Ahmed Al-Rawi argues that political hacking is an aggressive and militant form of public communication employed by tech-savvy individuals, regardless of their affiliations, in order to influence politics and policies. Kenneth Waltz's structural realism theory is linked to this argument as it provides a relevant framework to explain why nation-states employ cyber tools against each other. On the one hand, nation-states as well as their affiliated hacking groups like cyber warriors employ hacking as offensive and defensive tools in connection to the cyber activity or inactivity of other nation-states, such as the role of Russian Trolls disseminating disinformation on social media during the US 2016 presidential election. This is regarded as a horizontal flow of political disruption. Sometimes, nation-states, like the UAE, Saudi Arabia, and Bahrain, use hacking and surveillance tactics as a vertical flow (top-bottom) form of online political disruption by targeting their own citizens due to their oppositional or activists' political views. On the other hand, regular hackers who are often politically independent practice a form of bottom-top political disruption to address issues related to the internal politics of their respective nation-states such as the case of a number of Iraqi, Saudi, and Algerian hackers. In some cases, other hackers target ordinary citizens to express opposition to their political or ideological views which is regarded as a horizontal form of online political disruption. This book is the first of its kind to shine a light on many ways that governments and hackers are perpetrating cyber attacks in the Middle East and beyond, and to show the ripple effect of these attacks.
Security in Computing and Communications Springer
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.
NTP Security Springer
Develop a comprehensive plan for building a HIPAA-compliant security operations center, designed to detect and respond to an increasing number of healthcare data breaches and events. Using risk analysis, assessment, and management data combined with knowledge of cybersecurity program maturity, this book gives you the tools you need to operationalize threat intelligence, vulnerability management, security monitoring, and incident response processes to effectively meet the challenges presented by healthcare's current threats. Healthcare entities are bombarded with data. Threat intelligence feeds, news updates, and messages come rapidly and in many forms such as email, podcasts, and more. New vulnerabilities are found every day in applications, operating systems, and databases while older vulnerabilities remain exploitable. Add in the number of

dashboards, alerts, and data points each information security tool provides and security teams find themselves swimming in oceans of data and unsure where to focus their energy. There is an urgent need to have a cohesive plan in place to cut through the noise and face these threats. Cybersecurity operations do not require expensive tools or large capital investments. There are ways to capture the necessary data. Teams protecting data and supporting HIPAA compliance can do this. All that's required is a plan—which author Eric Thompson provides in this book. What You Will Learn Know what threat intelligence is and how you can make it useful Understand how effective vulnerability management extends beyond the risk scores provided by vendors Develop continuous monitoring on a budget Ensure that incident response is appropriate Help healthcare organizations comply with HIPAA Who This Book Is For Cybersecurity, privacy, and compliance professionals working for organizations responsible for creating, maintaining, storing, and protecting patient information.

The Significance of the Security Dialogues IGI Global
FireEye Deployment Made EasyLulu.comCyber Warfare: A Documentary and Reference GuideABC-CLIO
Apress
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.

A substantive dialogue Springer
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.

An Introductory Guide to Artificial Intelligence for Legal Professionals John Wiley & Sons
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.

The Oxford Handbook of Cyber Security Edizioni Nuova Cultura
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

Interoperability, Safety and Security in IoT Page Publishing, Inc
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!

Related with User Guide Fireeye:
• How To Practice Crawling Sims 4 : click here