Cyber Threat Assessment Fortinet

Commerce, Justice, Science, and Related Agencies Appropriations for 2012
Collective Creativity for Responsible and Sustainable Business Practice
Next-Generation Enterprise Security and Governance
Regulating Cyber Technologies: Privacy Vs Security
Cybersecurity Best Practices
Times Business Directory of Singapore
Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution
Fight Fire with Fire
Code und andere Gesetze des Cyberspace
Assessing Cyber Security
Security and Organization within IoT and Smart Cities
Cyber-Sicherheit
Network Access Control
Managing Cyber Risk
Building an Effective Cybersecurity Program, 2nd Edition
Strategic Cyber Deterrence
The Rise of Politically Motivated Cyber Attacks
Click Here to Kill Everybody
Web Application Security
Botnets
Terrorismus
Information Security Technologies for Controlling Pandemics
Enabling Technologies for Effective Planning and Management in Sustainable Smart Cities
Tech impact. Luci e ombre dello sviluppo tecnologico
Inside the Dark Web
Журнал сетевых решений / LAN No10/2016
21st European Conference on Cyber Warfare and Security
Policy Design in the Age of Digital Adoption
Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications
Cyber Forensics
Die Kunst der Täuschung
CompTIA Network+ N10-008 Certification Guide
What is to Be Done About Crime and Punishment?
Hacking
Inside Anonymous
Cybersecurity – Attack and Defense Strategies
Computational Science and Its Applications – ICCSA 2023 Workshops
Dataquest

DAKOTA CARLA

Commerce, Justice, Science, and Related Agencies Appropriations for 2012 CRC Press
The Internet is making our daily lives as digital as possible, and this new era is called the Internet of Everything (IoE). The key force behind the rapid growth of the Internet is the technological advancement of enterprises. The digital world we live in is facilitated by these enterprises' advances and business intelligence. These enterprises need to deal with gazillions of bytes of data, and in today's age of General Data Protection Regulation, enterprises are required to ensure privacy and security of large-scale data collections. However, the increased connectivity and devices used to facilitate IoE are continually creating more room for cybercriminals to find vulnerabilities in enterprise systems and flaws in their corporate governance. Ensuring cybersecurity and corporate governance for enterprises should not be an afterthought or present a huge challenge. In recent times, the complex diversity of cyber-attacks has been skyrocketing, and zero-day attacks, such as ransomware, botnet, and telecommunication attacks, are happening more frequently than before. New hacking strategies would easily bypass existing enterprise security and governance platforms using advanced, persistent threats. For example, in 2020, the Toll Group firm was exploited by a new crypto-attack family for violating its data privacy, where an advanced ransomware technique was launched to exploit the corporation and request a huge figure of monetary ransom. Even after applying rational governance hygiene, cybersecurity configuration and software updates are often overlooked when they are most needed to fight cyber-crime and ensure data privacy. Therefore, the threat landscape in the context of enterprises has become wider and far more challenging. There is a clear need for collaborative work throughout the entire value chain of this network. In this context, this book addresses the cybersecurity and cooperate governance challenges associated with enterprises, which will provide a bigger picture of the concepts, intelligent techniques, practices, and open research directions in this area. This book serves as a single source of reference for acquiring the knowledge on the technology, process, and people involved in next-generation privacy and security.
Collective Creativity for Responsible and Sustainable Business Practice Springer Nature
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.
Next-Generation Enterprise Security and Governance IGI Global
Threat actors, be they cyber criminals, terrorists, hacktivists or disgruntled employees, are employing sophisticated attack techniques and anti-forensics tools to cover their attacks and breach attempts. As emerging and hybrid technologies continue to influence daily business decisions, the proactive use of cyber forensics to better assess the risks that the exploitation of these technologies pose to enterprise-wide operations is rapidly becoming a strategic business objective. This book moves beyond the typical, technical approach to discussing cyber forensics processes and procedures. Instead, the authors examine how cyber forensics can be applied to identifying, collecting, and examining evidential data from emerging and hybrid technologies, while taking steps to proactively manage the influence and impact, as well as the policy and governance aspects of these technologies and their effect on business operations. A world-class team of cyber forensics researchers, investigators, practitioners and law enforcement professionals have come together to provide the reader with insights and recommendations into the proactive application of cyber forensic methodologies and procedures to both protect data and to identify digital evidence related to the misuse of these data. This book is an essential guide for both the technical and non-technical executive, manager, attorney, auditor, and general practitioner who is seeking an authoritative source on how cyber forensics may be applied to both evidential data collection and to proactively managing today's and tomorrow's emerging and hybrid technologies. The book will also serve as a primary or supplemental text in both under- and post-graduate academic programs addressing information, operational and emerging technologies, cyber forensics, networks, cloud computing and cybersecurity.
Regulating Cyber Technologies: Privacy Vs Security CRC Press
Strategic Cyber DeterrenceRowman & Littlefield
Cybersecurity Best Practices Springer Nature
Updated and revised edition of the bestselling guide to developing defense strategies against the latest threats to cybersecurity Key FeaturesCovers the latest security threats and defense strategies for 2020Introduces techniques and skillsets required to conduct threat hunting and deal with a system breachProvides new information on Cloud Security Posture Management, Microsoft Azure Threat Protection, Zero Trust Network strategies, Nation State attacks, the use of Azure Sentinel as a cloud-based SIEM for logging and investigation, and much moreBook Description Cybersecurity – Attack and Defense Strategies, Second Edition is a completely revised new edition of the bestselling book, covering the very latest security threats and defense mechanisms including a detailed overview of Cloud Security Posture Management (CSPM) and an assessment of the current threat landscape, with additional focus on new IoT threats and cryptomining. Cybersecurity starts with the basics that organizations need to know to maintain a secure posture against outside threat and design a robust cybersecurity program. It takes you into the mindset of a Threat Actor to help you better understand the motivation and the steps of performing an actual attack – the Cybersecurity kill chain. You will gain hands-on experience in implementing cybersecurity using new techniques in reconnaissance and chasing a user's identity that will enable you to discover how a system is compromised, and identify and then exploit the vulnerabilities in your own system. This book also

focuses on defense strategies to enhance the security of a system. You will also discover in-depth tools, including Azure Sentinel, to ensure there are security controls in each network layer, and how to carry out the recovery process of a compromised system. What you will learnThe importance of having a solid foundation for your security postureUse cyber security kill chain to understand the attack strategyBoost your organization's cyber resilience by improving your security policies, hardening your network, implementing active sensors, and leveraging threat intelligenceUtilize the latest defense tools, including Azure Sentinel and Zero Trust Network strategyIdentify different types of cyberattacks, such as SQL injection, malware and social engineering threats such as phishing emailsPerform an incident investigation using Azure Security Center and Azure SentinelGet an in-depth understanding of the disaster recovery processUnderstand how to consistently monitor security and implement a vulnerability management strategy for on-premises and hybrid cloudLearn how to perform log analysis using the cloud to identify suspicious activities, including logs from Amazon Web Services and AzureWho this book is for For the IT professional venturing into the IT security domain, IT pentesters, security consultants, or those looking to perform ethical hacking. Prior knowledge of penetration testing is beneficial.

Times Business Directory of Singapore Springer

Organizations around the world are in a struggle for survival, racing to transform themselves in a herculean effort to adapt to the digital age, all while protecting themselves from headline-grabbing cybersecurity threats. As organizations succeed or fail, the centrality and importance of cybersecurity and the role of the CISO—Chief Information Security Officer—becomes ever more apparent. It's becoming clear that the CISO, which began as a largely technical role, has become nuanced, strategic, and a cross-functional leadership position. Fight Fire with Fire: Proactive Cybersecurity Strategies for Today's Leaders explores the evolution of the CISO's responsibilities and delivers a blueprint to effectively improve cybersecurity across an organization. Fight Fire with Fire draws on the deep experience of its many all-star contributors. For example: Learn how to talk effectively with the Board from engineer-turned-executive Marianne Bailey, a top spokesperson well-known for global leadership in cyber Discover how to manage complex cyber supply chain risk with Terry Roberts, who addresses this complex area using cutting-edge technology and emerging standards Tame the exploding IoT threat landscape with Sonia Arista, a CISO with decades of experience across sectors, including healthcare where edge devices monitor vital signs and robots perform surgery These are just a few of the global trailblazers in cybersecurity who have banded together to equip today’s leaders to protect their enterprises and inspire tomorrow’s leaders to join them. With fires blazing on the horizon, there is no time for a seminar or boot camp. Cyber leaders need information at their fingertips. Readers will find insight on how to close the diversity and skills gap and become well-versed in modern cyber threats, including attacks coming from organized crime and nation-states. This book highlights a three-pronged approach that encompasses people, process, and technology to empower everyone to protect their organization. From effective risk management to supply chain security and communicating with the board, Fight Fire with Fire presents discussions from industry leaders that cover every critical competency in information security. Perfect for IT and information security professionals seeking perspectives and insights they can’t find in certification exams or standard textbooks, Fight Fire with Fire is an indispensable resource for everyone hoping to improve their understanding of the realities of modern cybersecurity through the eyes of today’s top security leaders.

Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution Rowman & Littlefield

«Журнал сетевых решений / LAN» – издание для специалистов по проектированию, установке, эксплуатации и модернизации информационных систем о компьютерных сетях, системах передачи данных, управления сетями и проектами, средствах связи, системах безопасности разного уровня. Тематика охватывает весь круг вопросов, связанных с корпоративными сетями, их сопряжением с общедоступными сетями, вычислительной и телекоммуникационной инфраструктурой, включая центры данных, СКС, системы бесперебойного питания.В номере:Тема номераЭволюция хостингаИТ-инфраструктураЭволюция методов монетизации программного обеспеченияНовые технологииМашинное обучение в СХД. Балансировка производительностиЗащита информацииБезопасность как возможностьКабельные системыБудут ли кабельные сети вытеснены беспроводными?и многое другое

Fight Fire with Fire Redline Wirtschaft

Das Thema Cybersecurity ist so aktuell wie nie, denn im Cyberspace lassen sich nur schwer Grenzen in Bezug auf den Zugang zu Informationen, Daten und Redefreiheit setzen. Kriminelle nutzen die Lücken oft zu ihrem Vorteil aus. Die Vielzahl der IT-Systeme, ihre unterschiedlichen Nutzungsarten und ihre Innovations- und Lebenszyklen haben zu hohen Sicherheitsrisiken für Unternehmen und staatliche Einrichtungen geführt. Diese Risiken werden sich auch langfristig nicht so einfach aus der Welt schaffen lassen. Daher müssen Institutionen Strategien und Lösungen zu ihrem Selbstschutz entwickeln. Dieses Buch beschreibt Lösungsansätze und Best Practices aus den unterschiedlichsten Bereichen, die nachweislich zu einer höheren Resilienz gegenüber Cyberangriffen führen. Weltweit renommierte IT-Sicherheitsexperten berichten in 40 Beiträgen, wie sich staatliche Institutionen, unter anderem das Militär (Cyber Defence), Behörden, internationale Organisationen und Unternehmen besser gegen Cyberangriffe schützen und nachhaltige Schutzstrategien entwickeln können. Die Autoren widmen sich den Gründen und Zielen, die ihren jeweiligen Strategien zugrunde liegen, sie berichten, wie Unternehmen auf konkrete Cyberattacken reagiert haben und wie einzelne staatliche Institutionen angesichts nationaler Cyberstrategien agieren. In weiteren Kapiteln zeigen Wissenschaftler auf, was bei der Abwehr von Cyber-Attacken bereits heute möglich ist, welche Entwicklungen in Arbeit sind und wie diese in Zukunft eingesetzt werden können, um die Cyber-Sicherheit zu erhöhen. Im letzten Kapitel berichten Hersteller, Anwenderunternehmen und Dienstleister welche Best Practices sie in ihren Unternehmen eingeführt haben und wie andere Unternehmen ihrem Beispiel folgen können. Das Buch richtet sich an IT-Verantwortliche und -Sicherheitsbeauftragte in Unternehmen und anderen Organisationen, aber auch an Studierende in den verschiedenen IT-Studiengängen.

Code und andere Gesetze des Cyberspace CRC Press

This book responds to the claim that criminology is becoming socially and politically irrelevant despite its exponential expansion as an academic sub-discipline. It does so by addressing the question 'what is to be done' in relation to a number of major issues associated with crime and

punishment. The original contributions to this volume are provided by leading international experts in a wide range of issues. They address imprisonment, drugs, gangs, cybercrime, prostitution, domestic violence, crime control, as well as white collar and corporate crime. Written in an accessible style, this collection aims to contribute to the development of a more public criminology and encourages students and researchers at all levels to engage in a form of criminology that is more socially relevant and more useful.

Assessing Cyber Security Routledge

Web application security is a branch of information security that deals specifically with security of websites and web applications. At a high level, Web application security draws on the principles of application security but applies them specifically to Internet and Web systems. Typically web applications are developed using programming languages such as PHP, Java EE, Java, Python, Ruby, ASP.NET, C#, VB.NET or Classic ASP. This book is your ultimate resource for Web Application Security. Here you will find the most up-to-date information, analysis, background and everything you need to know. In easy to read chapters, with extensive references and links to get you to know all there is to know about Web Application Security right away, covering: Web application security, Network security, Administrative domain, AEGIS SecureConnect, Aladdin Knowledge Systems, Alert Logic, Anomaly-based intrusion detection system, Anti-pharming, Anti-phishing software, Anti-worm, Application-level gateway, ARP spoofing, Asprox botnet, Attack (computer), Attack tree, Authentication server, Avaya Secure Network Access, Avaya VPN Router, Bagle (computer worm), Barracuda Networks, Bastion host, Black hole (networking), BLACKER, Blue Cube Security, BNC (software), Botnet, BredoLab botnet, Bro (software), Byzantine Foothold, Captive portal, Capture the flag, Check Point, Check Point Abra, Check Point VPN-1, Christmas tree packet, Cisco ASA, Cisco Global Exploiter, Cisco PIX, Cisco Security Agent, Cisco Systems VPN Client, Clarified Networks, Clear Channel Assessment attack, Client Puzzle Protocol, Cloudvpn, Codenomicon, Columbitech, Computer security, Context-based access control, ContraVirus, Core Impact, Core Security, Countermeasure (computer), Cryptek, Cutwail botnet, CVSS, CyberCIEGE, Dark Internet, Data breach, Deep packet inspection, Defense in depth (computing), Denial-of-service attack, Device fingerprint, DHIPDS, Differentiated security, Digital Postmarks, Digital security, Distributed firewall, DMZ (computing), DNS hijacking, Donbot botnet, Dual-homed, Egress filtering, Entrust, Evil bit, Extensible Threat Management (XTM), Extranet, Fail2ban, Fake AP, Finjan, Firewalk (computing), Firewall (computing), Firewall pinhole, Firewalls and Internet Security, Fortinet, Forward-confirmed reverse DNS, General Dynamics C4 Systems, Generalized TTL security mechanism, Global Internet Freedom Consortium, Greynet, Grum botnet, Guided tour puzzle protocol, Gumblar, Hole punching, Honeyd, HoneyMonkey, Honeynet Project, Honeypot (computing), Honeytoken, Host Identity Protocol, ICMP hole punching, Identity driven networking, IEC 62351, IEEE 802.1X, IF-MAP, Ingress filtering, Institute for Applied Network Security, Integrated Windows Authentication, Inter-protocol communication, Inter-protocol exploitation, Internet censorship, Internet security, Internet Storm Center, IntruShield, Network intrusion detection system, Intrusion prevention system, IP address spoofing, IP blocking, IP fragmentation attacks, Kaspersky Anti-Virus, Kerberos (protocol), Kerio Control, Key distribution center, Knowledge-based authentication, Kraken botnet, Lethic botnet, List of cyber attack threat trends, Lock-Keeper, Lorcon, Lumeta Corporation, MAC flooding, Managed security service, Managed VoIP Service, Mariposa botnet, Mega-D botnet, Messaging Security, Metasploit Project, Middlebox, Miredo, Mobile virtual private network, Monoculture (computer science), Mu Dynamics, MySecureCyberspace, NAT traversal, NeoAccel, NetBox Blue, Network Access Control, Network Admission Control, Network Based Application Recognition, Network encryption cracking...and much more This book explains in-depth the real drivers and workings of Web Application Security. It reduces the risk of your technology, time and resources investment decisions by enabling you to compare your understanding of Web Application Security with the objectivity of experienced professionals.

Security and Organization within IoT and Smart Cities MITP-Verlags GmbH & Co. KG

Cyber risk is the second highest perceived business risk according to U.S. risk managers and corporate insurance experts. Digital assets now represent over 85% of an organization’s value. In a survey of Fortune 1000 organizations, 83% surveyed described cyber risk as an organizationally complex topic, with most using only qualitative metrics that provide little, if any insight into an effective cyber strategy. Written by one of the foremost cyber risk experts in the world and with contributions from other senior professionals in the field, Managing Cyber Risk provides corporate cyber stakeholders – managers, executives, and directors – with context and tools to accomplish several strategic objectives. These include enabling managers to understand and have proper governance oversight of this crucial area and ensuring improved cyber resilience. Managing Cyber Risk helps businesses to understand cyber risk quantification in business terms that lead risk owners to determine how much cyber insurance they should buy based on the size and the scope of policy, the cyber budget required, and how to prioritize risk remediation based on reputational, operational, legal, and financial impacts. Directors are held to standards of fiduciary duty, loyalty, and care. These insights provide the ability to demonstrate that directors have appropriately discharged their duties, which often dictates the ability to successfully rebut claims made against such individuals. Cyber is a strategic business issue that requires quantitative metrics to ensure cyber resiliency. This handbook acts as a roadmap for executives to understand how to increase cyber resiliency and is unique since it quantifies exposures at the digital asset level.

Cyber-Sicherheit John Wiley & Sons

This nine-volume set LNCS 14104 – 14112 constitutes the refereed workshop proceedings of the 23rd International Conference on Computational Science and Its Applications, ICCSA 2023, held at Athens, Greece, during July 3–6, 2023. The 350 full papers and 29 short papers and 2 PHD showcase papers included in this volume were carefully reviewed and selected from a total of 876 submissions. These nine-volumes includes the proceedings of the following workshops: Advances in Artificial Intelligence Learning Technologies: Blended Learning, STEM, Computational Thinking and Coding (AAILT 2023); Advanced Processes of Mathematics and Computing Models in Complex Computational Systems (ACMC 2023); Artificial Intelligence supported Medical data examination (AIM 2023); Advanced and Innovative web Apps (AIWA 2023); Assessing Urban Sustainability (ASUS 2023); Advanced Data Science Techniques with applications in Industry and Environmental Sustainability (ATELIERS 2023); Advances in Web Based Learning (AWBL 2023); Blockchain and Distributed Ledgers: Technologies and Applications (BDLTA 2023); Bio and Neuro inspired Computing and Applications (BIONCA 2023); Choices and Actions for Human Scale Cities: Decision

Support Systems (CAHSC-DSS 2023); and Computational and Applied Mathematics (CAM 2023).

Network Access Control Packt Publishing Ltd

Inside the Dark Web provides a broad overview of emerging digital threats and computer crimes, with an emphasis on cyberstalking, hacktivism, fraud and identity theft, and attacks on critical infrastructure. The book also analyzes the online underground economy and digital currencies and cybercrime on the dark web. The book further explores how dark web crimes are conducted on the surface web in new mediums, such as the Internet of Things (IoT) and peer-to-peer file sharing systems as well as dark web forensics and mitigating techniques. This book starts with the fundamentals of the dark web along with explaining its threat landscape. The book then introduces the Tor browser, which is used to access the dark web ecosystem. The book continues to take a deep dive into cybersecurity criminal activities in the dark net and analyzes the malpractices used to secure your system. Furthermore, the book digs deeper into the forensics of dark web, web content analysis, threat intelligence, IoT, crypto market, and cryptocurrencies. This book is a comprehensive guide for those who want to understand the dark web quickly. After reading Inside the Dark Web, you'll understand The core concepts of the dark web. The different theoretical and cross-disciplinary approaches of the dark web and its evolution in the context of emerging crime threats. The forms of cybercriminal activity through the dark web and the technological and "social engineering" methods used to undertake such crimes. The behavior and role of offenders and victims in the dark web and analyze and assess the impact of cybercrime and the effectiveness of their mitigating techniques on the various domains. How to mitigate cyberattacks happening through the dark web. The dark web ecosystem with cutting edge areas like IoT, forensics, and threat intelligence and so on. The dark web-related research and applications and up-to-date on the latest technologies and research findings in this area. For all present and aspiring cybersecurity professionals who want to upgrade their skills by understanding the concepts of the dark web, Inside the Dark Web is their one-stop guide to understanding the dark web and building a cybersecurity plan.

Managing Cyber Risk goWare & Edizioni Guerini e associati

HauptbeschreibungDurch die zunehmende Vernetzung von privatwirtschaftlichen Unternehmen und öffentlichen Einrichtungen mit ihren jeweiligen Zulieferern und Kunden sind heute deren Geschäftstätigkeiten ohne IT-Systeme nicht mehr darstellbar. Auch Privatpersonen wickeln in steigendem Umfang Angelegenheiten des täglichen Lebens unter Einsatz von IT-Systemen ab. Der damit verbundenen IT-geschützten Speicherung und Verarbeitung von Unternehmensdaten und personenbezogenen Daten steht eine Flut von Gefährdungen der IT-Systeme und der Daten gegenüber. Welchen Anforderungen zur Sicherheit der IT-System.

Building an Effective Cybersecurity Program, 2nd Edition Litres

Over the years, a plethora of reports has emerged that assess the causes, dynamics, and effects of cyber threats. This proliferation of reports is an important sign of the increasing prominence of cyber attacks for organizations, both public and private, and citizens all over the world. In addition, cyber attacks are drawing more and more attention in the media. Such efforts can help to better awareness and understanding of cyber threats and pave the way to improved prevention, mitigation, and resilience. This report aims to help in this task by assessing what we know about cyber security threats based on a review of 70 studies published by public authorities, companies, and research organizations from about 15 countries over the last few years. It answers the following questions: what do we know about the number, origin, and impact of cyber attacks? What are the current and emerging cyber security trends? And how well are we prepared to face these threats?

Strategic Cyber Deterrence IGI Global

This book aims to provide the latest research developments and results in the domain of AI techniques for smart cyber ecosystems. It presents a holistic insight into AI-enabled theoretic approaches and methodology in IoT networking, security analytics using AI tools and network automation, which ultimately enable intelligent cyber space. This book will be a valuable resource for students, researchers, engineers and policy makers working in various areas related to cybersecurity and privacy for Smart Cities. This book includes chapters titled "An Overview of the Artificial Intelligence Evolution and Its Fundamental Concepts, and Their Relationship with IoT Security", "Smart City: Evolution and Fundamental Concepts", "Advances in AI-Based Security for Internet of Things in Wireless Virtualization Environment", "A Conceptual Model for Optimal Resource Sharing of Networked Microgrids Focusing Uncertainty: Paving Path to Eco-friendly Smart Cities", "A Novel Framework for a Cyber Secure Smart City", "Contemplating Security Challenges and Threats for Smart Cities", "Self-Monitoring Obfuscated IoT Network", "Introduction to Side Channel Attacks and Investigation of Power Analysis and Fault Injection Attack Techniques", "Collaborative Digital Forensic Investigations Model for Law Enforcement: Oman as a Case Study", "Understanding Security Requirements and Challenges in the Industrial Internet of Things: A Review", "5G Security and the Internet of Things", "The Problem of Deepfake Videos and How to Counteract Them in Smart Cities", "The Rise of Ransomware Aided by Vulnerable IoT Devices", "Security Issues in Self-Driving Cars within Smart Cities", and "Trust-Aware Crowd Associated Network-Based Approach for Optimal Waste Management in Smart Cities". This book provides state-of-the-art research results and discusses current issues, challenges, solutions and recent trends related to security and organization within IoT and Smart Cities. We expect this book to be of significant importance not only to researchers and practitioners in academia, government agencies and industries, but also for policy makers and system managers. We anticipate this book to be a valuable resource for all those working in this new and exciting area, and a "must have" for all university libraries.

The Rise of Politically Motivated Cyber Attacks CRC Press

This book outlines the complexity in understanding different forms of cyber attacks, the actors involved, and their motivations. It explores the key challenges in investigating and prosecuting politically motivated cyber attacks, the lack of consistency within regulatory frameworks, and the grey zone that this creates, for cybercriminals to operate within. Connecting diverse literatures on cyberwarfare, cyberterrorism, and cyberprotests, and categorising the different actors involved – state-sponsored/supported groups, hacktivists, online protestors – this book compares the means and methods used in attacks, the various attackers, and the current strategies employed by cybersecurity agencies. It examines the current legislative framework and proposes ways in which it could be reconstructed, moving beyond the traditional and fragmented definitions used to manage offline violence. This book is an important contribution to the study of cyber attacks within the areas of criminology, criminal justice, law, and policy. It is a compelling reading for all those engaged in cybercrime, cybersecurity, and digital forensics.

Click Here to Kill Everybody World Scientific
The prominence and growing dependency on information communication technologies in nearly every aspect of life has opened the door to threats in cyberspace. Criminal elements inside and outside organizations gain access to information that can cause financial and reputational damage. Criminals also target individuals daily with personal devices like smartphones and home security systems who are often unaware of the dangers and the privacy threats around them. The Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution is a critical scholarly resource that creates awareness of the severity of cyber information threats on personal, business, governmental, and societal levels. The book explores topics such as social engineering in information security, threats to cloud computing, and cybersecurity resilience during the time of the Fourth Industrial Revolution. As a source that builds on available literature and expertise in the field of information technology and security, this publication proves useful for academicians, educationalists, policy makers, government officials, students, researchers, and business leaders and managers.
Web Application Security Springer Nature
This book provides solid, state-of-the-art contributions from both scientists and practitioners working on botnet detection and analysis, including botnet economics. It presents original theoretical and empirical chapters dealing with both offensive and defensive aspects in this field. Chapters address fundamental theory, current trends and techniques for evading detection, as well as practical experiences concerning detection and defensive strategies for the botnet ecosystem, and include surveys, simulations, practical results, and case studies.
Botnets Tebbo
Become a network specialist by developing your skills in network implementation, operations and security while covering all the exam topics for CompTIA Network+ N10-008 certification in an easy-to-follow guide. Purchase of the print or Kindle book includes a free eBook in the PDF format. Key FeaturesA step-by-step guide to gaining a clear understanding of the Network+ certificationLearn about network architecture, protocols, security, and network troubleshootingConfidently ace the N10-008 exam with the help of 200+ practice test questions and answersBook Description This book helps you to easily understand core networking concepts without the need of prior industry experience or knowledge within this fi eld of study. This updated second edition of the CompTIA Network+ N10-008 Certification Guide begins by introducing you to the core fundamentals of networking technologies and concepts, before progressing to intermediate and advanced topics using a student-centric approach. You'll explore best practices for designing and implementing a resilient and scalable network infrastructure to support modern applications and services. Additionally, you'll learn network security concepts and technologies to effectively secure organizations from cyber attacks and threats. The book also shows you how to efficiently discover and resolve networking issues using common troubleshooting techniques. By the end of this book, you'll have gained sufficient knowledge to efficiently design, implement, and maintain a network infrastructure as a successful network professional within the industry. You'll also have gained knowledge of all the official CompTIA Network+ N10-008 exam objectives, networking technologies, and how to apply your skills in the real world. What you will learnExplore common networking concepts, services, and architectureIdentify common cloud architecture and virtualization conceptsDiscover routing and switching technologiesImplement wireless technologies and solutionsUnderstand network security concepts to mitigate cyber attacksExplore best practices to harden networks from threatsUse best practices to discover and resolve common networking issuesWho this book is for This book is for students, network administrators, network engineers, NOC engineers, systems administrators, cybersecurity professionals, and enthusiasts. No prior knowledge in networking is required to get started with this book.

Related with Cyber Threat Assessment Fortinet:
© Cyber Threat Assessment Fortinet Lightyear Imdb Parents Guide
© Cyber Threat Assessment Fortinet Linear Algebra 5th Edition Solutions
© Cyber Threat Assessment Fortinet Lindsay Dole The Practice