Cyber Threat Assessment Fortinet

The New Era of Cybersecurity Breaches
Some Basic Concepts and Issues
Towards a 'Public Criminology'
Architectures, Countermeasures, and Challenges
The Complete Reference
A meta analysis of threats, trends, and responses to cyber attacks
Effective Cybersecurity
Cyber-Physical Threat Intelligence for Critical Infrastructures Security
Guide to Vulnerability Analysis for Computer Networks and Systems
Managing Cyber Risk
Zero Trust Networks
Cybersecurity ??? Attack and Defense Strategies
International Law, International Relations and Diplomacy
High-impact Technology - What You Need to Know
Security and Organization within IoT and Smart Cities
Cyber Security on Azure
Best Practices for Designing, Implementing, and Maintaining Systems
Building Secure and Reliable Systems
Commerce, Justice, Science, and Related Agencies Appropriations for 2013: Statements of

members of Congress and other interested individuals and organizations
Building Secure Systems in Untrusted Networks
Building an Effective Cybersecurity Program, 2nd Edition
Actors, Attacks and Cybersecurity
Network Security Assessment
Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity
Hacking Multifactor Authentication
The Rise of Politically Motivated Cyber Attacks
Peacetime Regime for State Activities in Cyberspace
Assessing Cyber Security
Proactive Cybersecurity Strategies for Today's Leaders
A Guide to Using Best Practices and Standards
At the Nexus of Cybersecurity and Public Policy
Official (ISC)2 Guide to the CISSP CBK
The Active Cyber Defense Option
Strategic Cyber Security
Security Information and Event Management (SIEM) Implementation
An Artificial Intelligence Approach
A Case Study and Lessons Learned
Network Security
Know Your Network

The New Era of Cybersecurity Breaches

Newnes

Strategic Cyber DeterrenceThe Active Cyber Defense OptionRowman & Littlefield

Some Basic Concepts and Issues

Springer

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.

Towards a 'Public Criminology'

John Wiley & Sons

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. McGraw Hill Professional IT-SEC protects the information. SEC-OT protects physical, industrial operations from information, more specifically from attacks embedded in information. When the consequences of compromise are unacceptable ? unscheduled downtime, impaired product quality and damaged equipment ? software-based IT-SEC defences are not enough. Secure Operations Technology (SEC-OT) is a perspective, a methodology, and a set of best practices used at secure industrial sites. SEC-OT demands cyber-physical protections - because all software can be compromised. SEC-OT strictly controls the flow of information ? because all information can encode attacks. SEC-OT uses a

wide range of attack capabilities to determine the strength of security postures - because nothing is secure. This book documents the Secure Operations Technology approach, including physical offline and online protections against cyber attacks and a set of twenty standard cyber-attack patterns to use in risk assessments. *Architectures, Countermeasures, and Challenges* IGI Global This comprehensive book instructs IT managers to adhere to federally mandated compliance requirements. FISMA Compliance Handbook Second Edition explains what the requirements are for FISMA compliance and why FISMA compliance is mandated by federal law. The evolution of Certification and Accreditation is discussed. This book walks the reader through the entire FISMA compliance process and includes guidance on how to manage a FISMA compliance project from start to finish. The book has chapters for all FISMA compliance deliverables and includes information on how to conduct a FISMA compliant security assessment. Various topics discussed in this book include the

NIST Risk Management Framework, how to characterize the sensitivity level of your system, contingency plan, system security plan development, security awareness training, privacy impact assessments, security assessments and more. Readers will learn how to obtain an Authority to Operate for an information system and what actions to take in regards to vulnerabilities and audit findings. FISMA Compliance Handbook Second Edition, also includes all-new coverage of federal cloud computing compliance from author Laura Taylor, the federal government's technical lead for FedRAMP, the government program used to assess and authorize cloud products and services. Includes new information on cloud computing compliance from Laura Taylor, the federal government's technical lead for FedRAMP Includes coverage for both corporate and government IT managers Learn how to prepare for, perform, and document FISMA compliance projects This book is used by various colleges and universities in information security and MBA curriculums

The Complete Reference

BoD – Books on Demand

«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

A meta analysis of threats, trends, and responses to cyber attacks
CRC Press
Enhance your organization’s secure

posture by improving your attack and defense strategies Key Features Gain a clear understanding of the attack methods, and patterns to recognize abnormal behavior within your organization with Blue Team tactics. Learn to unique techniques to gather exploitation intelligence, identify risk and demonstrate impact with Red Team and Blue Team strategies. A practical guide that will give you hands-on experience to mitigate risks and prevent attackers from infiltrating your system. Book Description The book will start talking about the security posture before moving to Red Team tactics, where you will learn the basic syntax for the Windows and Linux tools that are commonly used to perform the necessary operations. You will also gain hands-on experience of using new Red Team techniques with powerful tools such as python and PowerShell, which will enable you to discover vulnerabilities in your system and how to exploit them. Moving on, you will learn how a system is usually compromised by adversaries, and how they hack user's identity, and the various tools used by the Red Team to find vulnerabilities in a system. In the next section, you will learn

about the defense strategies followed by the Blue Team to enhance the overall security of a system. You will also learn about an in-depth strategy to ensure that there are security controls in each network layer, and how you can carry out the recovery process of a compromised system. Finally, you will learn how to create a vulnerability management strategy and the different techniques for manual log analysis. By the end of this book, you will be well-versed with Red Team and Blue Team techniques and will have learned the techniques used nowadays to attack and defend systems. What you will learn Learn the importance of having a solid foundation for your security posture Understand the attack strategy using cyber security kill chain Learn how to enhance your defense strategy by improving your security policies, hardening your network, implementing active sensors, and leveraging threat intelligence Learn how to perform an incident investigation Get an in-depth understanding of the recovery process Understand continuous security monitoring and how to implement a vulnerability management strategy Learn how to

perform log analysis to identify suspicious activities Who this book is for This book aims at IT professional who want to venture the IT security domain. IT pentester, Security consultants, and ethical hackers will also find this course useful. Prior knowledge of penetration testing would be beneficial.

Effective Cybersecurity O'Reilly Media

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.

Cyber-Physical Threat Intelligence for Critical Infrastructures Security

"O'Reilly Media, Inc." Network Access Control (NAC) is an approach to computer network security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement. This book is your ultimate resource for Network Access Control (NAC). 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 Network Access Control (NAC) right away, covering: Network Access Control, 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 Secure Integrated Software, Cisco Security Agent, Cisco Systems VPN Client, 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, Golden Frog Inc, 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 Admission Control, Network Based Application Recognition, Network encryption cracking, Network intelligence, Network security policy, Network Security Toolkit, Nfront security, NIST RBAC model, NTLM, Null session, OCML...and much more This book explains in-depth the real drivers and workings of Network Access Control (NAC). It reduces the risk of your technology, time and resources investment decisions by

enabling you to compare your understanding of Network Access Control (NAC) with the objectivity of experienced professionals. **Guide to Vulnerability Analysis for Computer Networks and Systems** Rowman & Littlefield Prevent destructive attacks to your Azure public cloud infrastructure, remove vulnerabilities, and instantly report cloud security readiness. This book provides comprehensive guidance from a security insider's perspective. Cyber Security on Azure explains how this 'security as a service' (SECaaS) business solution can help you better manage security risk and enable data security control using encryption options such as Advanced Encryption Standard (AES) cryptography. Discover best practices to support network security groups, web application firewalls, and database auditing for threat protection. Configure custom security notifications of potential cyberattack vectors to prevent unauthorized access by hackers, hacktivists, and industrial spies. What You'll Learn This book provides step-by-step guidance on how to: Support enterprise security policies

Improve cloud security Configure intrusion detection Identify potential vulnerabilities Prevent enterprise security failures Who This Book Is For IT, cloud, and security administrators ; CEOs, CIOs, and other business professionals

Managing Cyber Risk Springer Nature

The perimeter defenses guarding your network perhaps are not as secure as you think. Hosts behind the firewall have no defenses of their own, so when a host in the "trusted" zone is breached, access to your data center is not far behind. That's an all-too-familiar scenario today. With this practical book, you'll learn the principles behind zero trust architecture, along with details necessary to implement it. The Zero Trust Model treats all hosts as if they're internet-facing, and considers the entire network to be compromised and hostile. By taking this approach, you'll focus on building strong authentication , authorization, and encryption throughout, while providing compartmentalized access and better operational agility. Understand how perimeter-based defenses have evolved to become the broken model we use today

Explore two case studies of zero trust in production networks on the client side (Google) and on the server side (PagerDuty) Get example configuration for open source tools that you can use to build a zero trust network Learn how to migrate from a perimeter-based network to a zero trust network in production

Zero Trust Networks

CRC Press

We depend on information and information technology (IT) to make many of our day-to-day tasks easier and more convenient. Computers play key roles in transportation , health care, banking, and energy. Businesses use IT for payroll and accounting, inventory and sales, and research and development. Modern military forces use weapons that are increasingly coordinated through computer-based networks. Cybersecurity is vital to protecting all of these functions. Cyberspace is vulnerable to a broad spectrum of hackers, criminals, terrorists, and state actors. Working in cyberspace, these malevolent actors can steal money, intellectual property, or classified information; impersonate law-abiding parties for their own purposes; damage important data; or deny the availability

of normally accessible services. Cybersecurity issues arise because of three factors taken together - the presence of malevolent actors in cyberspace, societal reliance on IT for many important functions, and the presence of vulnerabilities in IT systems. What steps can policy makers take to protect our government, businesses, and the public from those would take advantage of system vulnerabilities ? At the Nexus of Cybersecurity and Public Policy offers a wealth of information on practical measures, technical and nontechnical challenges, and potential policy responses. According to this report, cybersecurity is a never-ending battle; threats will evolve as adversaries adopt new tools and techniques to compromise security. Cybersecurity is therefore an ongoing process that needs to evolve as new threats are identified. At the Nexus of Cybersecurity and Public Policy is a call for action to make cybersecurity a public safety priority. For a number of years, the cybersecurity issue has received increasing public attention; however, most policy focus has been on the short-term costs of improving systems. In its explanation of the

fundamentals of cybersecurity and the discussion of potential policy responses, this book will be a resource for policy makers, cybersecurity and IT professionals, and anyone who wants to understand threats to cyberspace.

Cybersecurity ??? Attack and Defense Strategies

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. *International Law, International Relations and Diplomacy* IGI Global Teaches end-to-end network security concepts and techniques. Includes comprehensive information on how to design a comprehensive security defense model. Plus, discloses how to develop and deploy computer, personnel, and physical security policies, how to design and manage authentication and authorization methods, and much more. **High-impact Technology - What You Need to Know** John Wiley & Sons 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?

Security and Organization within IoT and Smart Cities

National Academies Press

As a result of a rigorous, methodical process that (ISC) follows to routinely update its credential exams, it has announced that enhancements will be made to both the Certified Information Systems Security Professional (CISSP) credential, beginning April 15, 2015. (ISC) conducts this process on a regular basis to ensure that the examinations and

Cyber Security on Azure

McGraw Hill

Professional Over the years, irresponsible business practices have resulted in industrial waste, which is negatively impacting the environment. As a result, it is imperative to develop new solutions to reverse the damage. Collective Creativity for Responsible and Sustainable Business Practice is an authoritative reference source for the latest scholarly research on the elimination of environmental degradation through new discoveries and opportunities provided by collective creativity. Featuring extensive coverage across a range of relevant perspective and topics, such as sustainable business model innovation, social marketing, and education and business co-operatives, this comprehensive and timely publication is an essential reference source for business leaders, managers, academics, and community leaders seeking current research on sustainable management practices.

Best Practices for Designing, Implementing, and Maintaining Systems

Routledge

BUILD YOUR CYBERSECURITY PROGRAM WITH THIS COMPLETELY UPDATED GUIDE

Security practitioners now have a

comprehensive blueprint to build their cybersecurity programs. Building an Effective Cybersecurity Program (2nd Edition) instructs security architects, security managers, and security engineers how to properly construct effective cybersecurity programs using contemporary architectures, frameworks, and models. This comprehensive book is the result of the author's professional experience and involvement in designing and deploying hundreds of cybersecurity programs. The extensive content includes: Recommended design approaches, Program structure, Cybersecurity technologies, Governance Policies, Vulnerability, Threat and intelligence capabilities, Risk management, Defense-in-depth, DevSecOps, Service management, ...and much more! The book is presented as a practical roadmap detailing each step required for you to build your effective cybersecurity program. It also provides many design templates to assist in program builds and all chapters include self-study questions to gauge your progress. With this new 2nd edition of this handbook, you can move forward confidently, trusting that Schrei-

der is recommending the best components of a cybersecurity program for you. In addition, the book provides hundreds of citations and references allow you to dig deeper as you explore specific topics relevant to your organization or your studies.
Whether you are a new manager or current manager involved in your organization's cybersecurity program, this book will answer many questions you have on what is involved in building a program. You will be able to get up to speed quickly on program development practices and have a roadmap to follow in building or improving your organization's cybersecurity program. If you are a manager already involved in your organization's cybersecurity program, you have much to gain from reading this book. This book will become your go to field manual guiding or affirming your program decisions.

Building Secure and Reliable Systems
Tebbo
This book on computer security threats explores the computer security threats and

includes a broad set of solutions to defend the computer systems from these threats. The book is triggered by the understanding that digitalization and growing dependence on the Internet poses an increased risk of computer security threats in the modern world. The chapters discuss different research frontiers in computer security with algorithms and implementation details for use in the real world. Researchers and practitioners in areas such as statistics, pattern recognition, machine learning, artificial intelligence, deep learning, data mining, data analytics and visualization are contributing to the field of computer security. The intended audience of this book will mainly consist of researchers, research students, practitioners, data analysts, and business professionals who seek information on computer security threats and its defensive measures. **Commerce, Justice, Science, and Related Agencies Appropriations for 2013: Statements of members of Congress and other interested individuals and organizations** Springer 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, 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 Cyber Secure Smart City", “Contemplate Security Challenges & Threats for Smart Cities”, “Self-Monitoring Obfuscated IoT Network”, “Introduction to Side Channel Attacks and

Investigation of Power Analysis & Fault Injection Attack Techniques", "Collaborative Digital Forensic Investigations Model for Law Enforcement: Oman as a Case Study", "Internet of Things Security and Privacy in Smart Cities: Status and Challenges", "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", and "Security Issues in Self-Driving Cars within Smart Cities", "PhishFree: A Honeybee Inspired System for Smart City Free of Phishing Attacks", "Trust Aware Crowd Associated Network-based Approach for Optimal Waste Management in Smart Cities" This book provides state-of-the-art of 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.

Related with Cyber Threat Assessment Fortinet:
• New York February 2023 Bar Exam Results : click here