Product Matrix For 2017 Fortinet

As recognized, adventure as competently as experience roughly lesson, amusement, as capably as union can be gotten by just checking out a book **product matrix for 2017 fortinet** in addition to it is not directly done, you could take even more just about this life, concerning the world.

We have enough money you this proper as with ease as easy exaggeration to get those all. We meet the expense of product matrix for 2017 fortinet and numerous book collections from fictions to scientific research in any way. accompanied by them is this product matrix for 2017 fortinet that can be your partner.

Learn Azure in a Month of Lunches, Second Edition - Iain Foulds 2020-10-06
Learn Azure in a Month of Lunches, Second Edition, is a tutorial on writing, deploying, and running applications in Azure. In it, you'll work through 21 short lessons that give you real-world experience. Each lesson includes a hands-on lab so you can try out and lock in your new skills. Summary You can be incredibly productive with Azure without mastering every feature, function, and service. Learn Azure in a Month of Lunches, Second Edition gets you up and running quickly, teaching you the most important concepts and tasks in 21 practical bite-sized lessons. As you explore the examples, exercises, and labs, you'll pick up valuable skills

immediately and take your first steps to Azure mastery! This fully revised new edition covers core changes to the Azure UI, new Azure features, Azure containers, and the upgraded Azure Kubernetes Service. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology Microsoft Azure is vast and powerful, offering virtual servers, application templates, and prebuilt services for everything from data storage to AI. To navigate it all, you need a trustworthy guide. In this book, Microsoft engineer and Azure trainer Iain Foulds focuses on core skills for creating cloud-based applications. About the book Learn Azure in a Month of Lunches, Second Edition, is a tutorial on writing, deploying, and running applications in Azure. In it, you'll work through 21 short lessons that give you real-world experience. Each lesson includes a hands-on lab so you can try out and lock in your new skills. What's inside Understanding Azure beyond point-and-click Securing applications and data Automating your environment Azure services for machine learning, containers, and more About the reader This book is for readers who can write and deploy simple web or client/server applications. About the author Iain Foulds is an engineer and senior content developer with Microsoft. Table of Contents PART 1 - AZURE CORE SERVICES 1 Before you begin 2 Creating a virtual machine 3 Azure Web Apps 4 Introduction to Azure Storage 5 Azure Networking basics PART 2 - HIGH AVAILABILITY AND SCALE 6 Azure Resource Manager 7 High availability and redundancy 8 Load-balancing applications 9 Applications that scale 10 Global databases with Cosmos DB 11 Managing network traffic and routing 12 Monitoring and troubleshooting PART 3 - SECURE BY DEFAULT 13 Backup, recovery, and replication 14 Data encryption 15 Securing information with Azure Key Vault 16 Azure Security Center and updates PART 4 - THE COOL STUFF 17 Machine learning and artificial intelligence 18 Azure Automation 19 Azure containers 20 Azure and the Internet of Things 21 Serverless computing

Computer Security Handbook - Seymour Bosworth 2014-03-31

xREF: System x Reference - David Watts 2015-05-18

Lenovo System x® and BladeCenter® servers and Lenovo Flex SystemTM compute nodes help to deliver a dynamic infrastructure that provides leadership quality and service that you can trust. This document (simply known as xREF) is a quick reference guide to the specifications of the currently available models of each System x and BladeCenter server. Each page can be used in a stand-alone format and provides a dense and comprehensive summary of the features of that particular server model. Links to the related Product Guide are also provided for more information. An easy-to-remember link you can use to share this guide: http://lenovopress.com/xref Also available is xREF for Products Withdrawn Prior to 2012, a document that contains xREF sheets of System x, BladeCenter, and xSeries servers, and IntelliStation workstations that were withdrawn from marketing prior to 2012. Changes in the May 18 update: Added the Flex System Carrier-Grade Chassis See the Summary of changes in the document for a complete change history.

Trends and Advances in Information Systems and Technologies - Álvaro Rocha 2018-03-23

This book includes a selection of papers from the 2018 World Conference on Information Systems and Technologies (WorldCIST'18), held in Naples, Italy on March27-29, 2018. WorldCIST is a global forum for researchers and practitioners to present and discuss recent results and innovations, current trends, professional experiences and the challenges of modern information systems and technologies research together with their technological development and applications. The main topics covered are:

A) Information and Knowledge Management; B) Organizational Models and Information Systems; C) Software and Systems Modeling; D) Software Systems, Architectures, Applications and Tools; E) Multimedia Systems and Applications; F) Computer Networks, Mobility and Pervasive Systems; G) Intelligent and Decision Support Systems; H) Big Data Analytics and Applications; I) Human–Computer Interaction; J) Ethics, Computers & Security; K) Health Informatics; L) Information Technologies in Education; M) Information Technologies in Radiocommunications; N) Technologies for Biomedical Applications.

Tribe of Hackers - Marcus J. Carey 2019-07-23 Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World (9781119643371) was previously published as Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World (9781793464187). While this version features a new cover design and introduction, the remaining content is the same as the prior release and should not be considered a new or updated product. Looking for real-world advice from leading cybersecurity experts? You've found your tribe. Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World is your guide to joining the ranks of hundreds of thousands of cybersecurity professionals around the world. Whether you're just joining the industry, climbing the corporate ladder, or considering consulting, Tribe of Hackers offers the practical know-how, industry perspectives, and technical insight you need to succeed in the rapidly growing information security market. This unique guide includes inspiring interviews from 70 security experts, including Lesley Carhart, Ming Chow, Bruce Potter, Robert M. Lee, and Jayson E. Street. Get the scoop on the biggest cybersecurity myths and misconceptions about security Learn what qualities and credentials you need to advance in the cybersecurity field Uncover which life hacks are worth your while Understand how social media and the Internet of Things has changed cybersecurity Discover what it takes to make the move from the corporate world to your own cybersecurity venture Find your favorite hackers online and continue the conversation Tribe of Hackers is a must-have resource for security professionals who are looking to advance their careers, gain a fresh perspective, and get serious about cybersecurity with thought-provoking insights from the world's most noteworthy hackers and influential security specialists.

Microsoft Azure Sentinel - Yuri Diogenes
2020-02-25

Microsoft Azure Sentinel Plan, deploy, and operate Azure Sentinel, Microsoft's advanced cloud-based SIEM Microsoft's cloud-based Azure Sentinel helps you fully leverage advanced AI to automate threat identification and response – without the complexity and scalability challenges of traditional Security Information and Event Management (SIEM) solutions. Now, three of Microsoft's leading experts review all it can do, and guide you step by step through planning, deployment, and daily operations. Leveraging in-the-trenches experience supporting early customers, they cover everything from configuration to data ingestion, rule development to incident management… even proactive threat hunting to disrupt attacks before you're exploited. Three of Microsoft's leading security operations experts show how to: • Use Azure Sentinel to respond to today's fast-evolving cybersecurity environment, and leverage the benefits of its cloud-native architecture • Review threat intelligence essentials: attacker motivations, potential targets, and tactics, techniques, and procedures • Explore Azure Sentinel components, architecture, design considerations, and initial configuration • Ingest alert log data from services and endpoints you need to monitor • Build and validate rules to analyze ingested data and create cases for investigation • Prevent alert fatigue by projecting how many incidents each rule will generate • Help Security Operation Centers (SOCs) seamlessly manage each incident’s lifecycle • Move towards proactive threat hunting: identify sophisticated threat behaviors and disrupt cyber kill chains before you’re exploited • Do more with data: use programmable Jupyter notebooks and their libraries for machine learning, visualization, and data analysis • Use Playbooks to perform Security Orchestration, Automation and Response (SOAR) • Save resources by automating responses to low-level events • Create visualizations to spot trends, identify or clarify relationships, and speed decisions • Integrate with partners and other third-parties, including Fortinet, AWS, and Palo Alto

CAPS LOCK: How Capitalism Took Hold of Graphic Design, and How to Escape from It - Ruben Pater 2021-09-21

Capitalism could not exist without the coins, banknotes, documents, information graphics, interfaces, branding, and advertisements made by graphic designers. Even anti-consumerist strategies such as social design and speculative design are appropriated to serve economic growth. It seems design is locked in a cycle of exploitation and extraction, furthering inequality and environmental collapse. CAPS LOCK uses clear language and visual examples to show how graphic design and capitalism are inextricably linked. The book features designed objects and also examines how the study, work, and professional practice of designers support the market economy. Six radical design cooperatives are featured that resist capitalist thinking in their own way, hoping to inspire a more socially aware graphic design.

Towards new e-Infrastructure and e-Services for Developing Countries - Rafik Zitouni 2021-03-04

This book constitutes the thoroughly refereed proceedings of the 12th International Conference on e-Infrastructure and e-Services for Developing Countries, AFRICOMM 2020, held in Ebène City, Mauritius, in December 2020. Due to COVID-19 pandemic the conference was held virtually. The 20 full papers were carefully selected from 90 submissions. The papers are organized in four thematic sections on dynamic spectrum access and mesh networks; wireless sensing and 5G networks; software-defined networking; Internet of Things; e-services and big data; DNS resilience and performance.

Clarity for Learning - John Almarode 2018-10-24 An essential resource for student and teacher clarity With the ever-changing landscape of education, teachers and leaders often find themselves searching for clarity in a sea of standards, curriculum resources, and competing priorities. Clarity for Learning offers a simple and doable approach to developing clarity and sharing it with students through five essential components: crafting learning intentions and success criteria co-constructing learning intentions and success criteria with learners creating opportunities for students to respond effective feedback on and for learning students and teachers sharing learning and progress The book is full of examples from teachers and leaders who have shared their journey, struggles, and successes for readers to use to propel their own work forward.

Cracking the Code Dan Callahan 2007 Cracking the Code: A Professional Salesperson's Guide to Penetrating the Intelligence Community was written with two goals in mind: 1) to demystify the often confusing and always secretive intelligence community from a sales person's perspective, and 2) to provide a first-level road map to penetrating this multibillion dollar market with a product or service. This book will give you no-nonsense answers to the following questions: Who comprises the intelligence community? Who is really in charge when it comes to making buying decisions? Exactly where and how should you begin your sales efforts? Without a security clearance, shall I even bother? How are IC agencies similar yet different than other federal agencies? What tactical steps can a sales person take to "break into" the IC? Where does the sales opportunity really exist? How should a person prepare for sales meetings? Do I really need to worry about things like a GSA Schedule, a secure vault, and a polygraph? Who can help me in my effort to penetrate the intelligence community? What is the best source of information to learn about my target clients? These and many other questions will be answered in this informative book. This is the first resource that helps the reader make money by persuasive selling, targeting intelligence community individuals who have one of the most complex jobs in our nation's history-protecting the American citizen against state sponsored crimes and the intricacies of the modern global war on terror (GWOT). Learn from someone who has been in the trenches of federal sales, yet views his role as helping our nation "be all it can be". This book will guide you on the 'road to revenue' in a candid view of person-to-person selling into the most secretive market in the world!

Cisco Firewalls-Alexandre M.S.P. Moraes 2011-06-06

Cisco Firewalls Concepts, design and deployment for Cisco Stateful Firewall solutions ¿ " In this book, Alexandre proposes a totally different approach to the important subject of firewalls: Instead of just presenting configuration models, he uses a set of carefully crafted examples to illustrate the theory in action.¿A must read!" —Luc Billot, Security Consulting Engineer at Cisco ¿ Cisco Firewalls thoroughly explains each of the leading Cisco firewall products, features, and solutions, and shows how they can add value to any network security design or operation. The author tightly links theory with practice, demonstrating how to integrate Cisco firewalls into highly secure, self-defending networks. Cisco Firewalls shows you how to deploy Cisco firewalls as an essential component of every network infrastructure. The book takes the unique approach of illustrating complex configuration concepts through step-by-step examples that demonstrate the theory in action. This is the first book with detailed coverage of firewalling Unified Communications systems, network virtualization architectures, and environments that include virtual machines. The author also presents indispensable information about integrating firewalls with other security elements such as IPS, VPNs, and load balancers; as well as a complete introduction to firewalling IPv6 networks. Cisco Firewalls will be an indispensable resource for engineers and architects designing and implementing firewalls; security administrators, operators, and support professionals; and anyone preparing for the CCNA Security, CCNP Security, or CCIE Security certification exams. ¿ Alexandre Matos da Silva Pires de Moraes, CCIE No. 6063, has worked as a Systems Engineer for Cisco Brazil since 1998 in projects that involve not only Security and VPN technologies but also Routing Protocol and Campus Design, IP Multicast Routing, and MPLS Networks Design. He coordinated a team of Security engineers in Brazil and holds the CISSP, CCSP, and three CCIE certifications (Routing/Switching, Security, and Service Provider). A frequent speaker at Cisco Live, he holds a degree in electronic engineering from the Instituto Tecnológico de Aeronáutica (ITA – Brazil). ¿ ·¿¿¿¿¿¿¿ Create advanced security designs utilizing the entire Cisco firewall product family ·¿¿¿¿¿¿¿ Choose the right firewalls based on your performance requirements ·¿¿¿¿¿¿¿ Learn firewall¿ configuration fundamentals and master the tools that provide insight about firewall operations ·¿¿¿¿¿¿¿ Properly insert firewalls in your network’s topology using Layer 3 or Layer 2 connectivity ·¿¿¿¿¿¿¿ Use Cisco firewalls as part of a robust, secure virtualization architecture ·¿¿¿¿¿¿¿ Deploy Cisco ASA firewalls with or without NAT ·¿¿¿¿¿¿¿ Take full advantage of the classic IOS firewall feature set (CBAC) ·¿¿¿¿¿¿¿ Implement flexible security policies with the Zone Policy Firewall (ZPF) ·¿¿¿¿¿¿¿ Strengthen stateful inspection with antispoofing, TCP normalization, connection limiting, and IP fragmentation handling ·¿¿¿¿¿¿¿ Use application-layer inspection capabilities built into Cisco firewalls ·¿¿¿¿¿¿¿ Inspect IP voice protocols, including SCCP, H.323, SIP, and MGCP ·¿¿¿¿¿¿¿ Utilize identity to provide user-based stateful functionality ·¿¿¿¿¿¿¿ Understand how multicast traffic is handled through firewalls ·¿¿¿¿¿¿¿ Use firewalls to protect your IPv6 deployments ¿ This security book is part of the Cisco Press Networking Technology Series. Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end, self-defending networks.

RIoT Control - Tyson Macaulay 2016-09-16 RIoT Control: Understanding and Managing Risks and the Internet of Things explains IoT risk in terms of project requirements, business needs, and system designs. Learn how the Internet of Things (IoT) is different from “Regular Enterprise security, more intricate and more complex to understand and manage. Billions of internet-connected devices make for a chaotic system, prone to unexpected behaviors. Industries considering IoT technologies need guidance on IoT-ready security and risk management practices to ensure key management objectives like Financial and Market success, and Regulatory compliance. Understand the threats and vulnerabilities of the IoT, including endpoints, newly emerged forms of gateway, network connectivity, and cloud-based data centers. Gain insights as to which emerging techniques are best according to your specific IoT system, its risks, and organizational needs. After a thorough introduction to the Iot, Riot Control explores dozens of IoT-specific risk management requirements, examines IoT-specific threats and finally provides risk management recommendations which are intended as applicable to a wide range of use-cases. Explains sources of risk across IoT architectures and performance metrics at the enterprise level Understands risk and security concerns in the next-generation of connected devices beyond computers and mobile consumer devices to everyday objects, tools, and devices Offers insight from industry insiders about emerging tools and techniques for real-world IoT systems

Effective Cybersecurity - William Stallings 2018-07-20

The Practical, Comprehensive Guide to Applying Cybersecurity Best Practices and Standards in Real Environments In Effective Cybersecurity, William Stallings introduces the technology, operational procedures, and management practices needed for successful cybersecurity. Stallings makes extensive use of standards and best practices documents that are often used to guide or mandate cybersecurity implementation. Going beyond these, he offers in-depth tutorials on the “how” of implementation, integrated into a unified framework and realistic plan of action. Each chapter contains a clear technical overview, as well as a detailed discussion of action items and appropriate policies. Stallings offers many pedagogical features designed to help readers master the material: clear learning objectives, keyword lists, review questions, and QR codes linking to relevant standards documents and web resources. Effective Cybersecurity aligns with the comprehensive Information Security Forum document “The Standard of Good Practice for Information Security,” extending ISF’s work with extensive insights from ISO, NIST, COBIT, other official standards and guidelines, and modern professional, academic, and industry literature. • Understand the cybersecurity discipline and the role of standards and best practices • Define security governance, assess risks, and manage strategy and tactics • Safeguard information and privacy, and ensure GDPR compliance • Harden systems across the system development life cycle (SDLC) • Protect servers, virtualized systems, and storage • Secure networks and electronic communications, from email to VoIP • Apply the most appropriate methods for user authentication • Mitigate security risks in supply chains and cloud environments This knowledge is indispensable to every cybersecurity professional. Stallings presents it systematically and coherently, making it practical and actionable.

Network Security Assessment - Chris McNab 2004

A practical handbook for network adminstrators who need to develop and implement security assessment programs, exploring a variety of offensive technologies, explaining how to design and deploy networks that are immune to offensive tools and scripts, and detailing an efficient testing model. Original. (Intermediate)

Entrepreneur Journeys - Sramana Mitra 2009-04-16

Captures the stories of established entrepreneurs to help those who want to learn.

Digital Transformation in a Post-Covid World - Adrian T. H. Kuah 2021-10-04

This book explores the innovations, disruptions and changes that are required to adapt in a fast-evolving landscape due to the extraordinary circumstances triggered by the COVID-19 pandemic. Recognized experts from around the world share their research and professional experience on how the working environment, as well as the world around them, have changed due to the pandemic. Chapters consider how different fields across technology and business have been affected by this new, dramatic scenario and the drastic consequences that the pandemic had on them. With diverse contributions stemming from public health, technology strategies, urban planning and sociology to sustainable management, this volume is articulated into four distinct but complementary sections of People, Process, Planet, and Prosperity influencing the post-COVID world. This book will be of great interest to those in the fields of computer science and information technology, as well as those studying the impact and effects that COVID-19 is having on society.

Forward Resilience - Daniel S. Hamilton 2017-02-07

The notion of 'resilience' is gaining currency in European and transatlantic security policy discussions. The EU and NATO are each building the capacity of their member states to anticipate, preempt and resolve disruptive challenges to vital societal functions. The EU and NATO are also exploring ways to work more effectively together in this area. But is resilience enough to deal with disruptive threats in a deeply interconnected world? In this new study, authors and experts argue that while state-by-state approaches to resilience are important, they are likely to be insufficient in a world where few critical infrastructures are limited to national borders, and where robust resilience efforts by one country may mean little if its neighbor's systems are weak. They argue not only that resilience must be shared, it must be projected forward, and that traditional notions of territorial security must be supplemented with actions to address flow security - protecting critical links that bind societies to one another.

The Illustrated Network - Walter Goralski 2009-10-01

In 1994, W. Richard Stevens and Addison-Wesley published a networking classic: TCP/IP Illustrated. The model for that book was a brilliant, unfettered approach to networking concepts that has proven itself over time to be popular with readers of beginning to intermediate networking knowledge. The Illustrated Network takes this time-honored approach and modernizes it by creating not only a much larger and more complicated network, but also by incorporating all the networking advancements that have taken place since the mid-1990s, which are many. This book takes the popular Stevens approach and modernizes it, employing 2008 equipment, operating systems, and router vendors. It presents an ?illustrated? explanation of how TCP/IP works with consistent examples from a real, working network configuration that includes servers, routers, and workstations. Diagnostic traces allow the reader to follow the discussion with unprecedented clarity and precision. True to the title of the book, there are 330+ diagrams and screen shots, as well as topology diagrams and a unique repeating chapter opening diagram. Illustrations are also used as end-of-chapter questions. A complete and modern network was assembled to write this book, with all the material coming from real objects connected and running on the network, not assumptions. Presents a real world networking scenario the way the reader sees them in a device-agnostic world. Doesn't preach one platform or the other. Here are ten key differences between the two: Stevens Goralski's Older operating systems (AIX,svr4,etc.) Newer OSs (XP, Linux, FreeBSD, etc.) Two routers (Cisco, Telebit (obsolete)) Two routers (M-series, J-series) Slow Ethernet and SLIP link Fast Ethernet, Gigabit Ethernet, and SONET/SDH links (modern) Tcpdump for traces Newer, better utility to capture traces (Ethereal, now has a new name!) No IPSec IPSec No multicast Multicast No router security discussed Firewall routers detailed No Web Full Web browser HTML consideration No IPv6 IPv6 overview Few configuration details More configuration details (ie, SSH, SSL, MPLS, ATM/FR consideration, wireless LANS, OSPF and BGP routing protocols New Modern Approach to Popular Topic Adopts the popular Stevens approach and modernizes it, giving the reader insights into the most up-to-date network equipment, operating systems, and router vendors. Shows and Tells Presents an illustrated explanation of how TCP/IP works with consistent examples from a real, working network configuration that includes servers, routers, and workstations, allowing the reader to follow the discussion with unprecedented clarity and precision. Over 330 Illustrations True to the title, there are 330 diagrams, screen shots, topology diagrams, and a unique repeating chapter opening diagram to reinforce concepts Based on Actual Networks A complete and modern network was assembled to write this book, with all the material coming from real objects connected and running on the network, bringing the real world, not theory, into sharp focus.

Cybersecurity ??? Attack and Defense Strategies - Yuri Diogenes 2018-01-30

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.

Zero Trust Networks Evan Gilman 2017-06-19 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 Days, Thousands of Nights - Lillian Ablon 2017-03-09

Zero-day vulnerabilities—software vulnerabilities for which no patch or fix has been publicly released—and their exploits are useful in cyber operations, as well as in defensive and academic settings. This report provides findings from real-world zero-day vulnerability and exploit data that can inform ongoing policy debates regarding stockpiling (i.e., keeping zero-day vulnerabilities private) versus disclosing them to the public.

Nanofibers and Nanotechnology in Textiles - P. Brown 2007-10-17

Nanotechnology is revolutionising the world of materials. This important book reviews its impact in developing a new generation of textile fibers with enhanced functionality and a wide range of applications. The first part of the book reviews nanofiber production, discussing how different fiber types can be produced using electrospinning techniques. Part two analyses the production and properties of carbon nanotubes and polymer nanocomposites and their applications in such areas as aerospace engineering. The third part of the book considers ways of using nanotechnology to improve polymer properties such as thermal stability and dyeability. The final part of the book reviews the use of nanotechnology to modify textile surfaces, including the use of coatings and films, in order to improve hydrophobic, filtration and other properties.

Nanofibers and nanotechnology in textiles is a valuable reference in assessing and using a new generation of textile fibers in applications as diverse as tissue and aerospace engineering. Nanotechnology is revolutionising the world of materials Learn about a new generation of textile fibers that have a wide range of applications Examines how to improve polymer properties

Computer Security - Robert C Newman 2009-02-19

Today, society is faced with numerous internet schemes, fraudulent scams, and means of identity theft that threaten our safety and our peace of mind. Computer Security: Protecting Digital Resources provides a broad approach to computer-related crime, electronic commerce, corporate networking, and Internet security, topics that have become increasingly important as more and more threats are made on our internet environment. This book is oriented toward the average computer user, business professional, government worker, and those within the education community, with the expectation that readers can learn to use the network with some degree of safety and security. The author places emphasis on the numerous vulnerabilities and threats that are inherent in the Internet environment. Efforts are made to present techniques and suggestions to avoid identity theft and fraud. Readers will gain a clear insight into the many security issues facing the e-commerce, networking, web, and internet environments, as well as what can be done to keep personal and business information secure.

Computer Security -- ESORICS 2019 - Kazue Sako (Innovation Producer) 2019

The two volume set, LNCS 11735 and 11736, constitutes the proceedings of the 24th European Symposium on Research in Computer Security, ESORIC 2019, held in Luxembourg, in September 2019. The total of 67 full papers included in these proceedings was carefully reviewed and selected from 344 submissions. The papers were organized in topical sections named as follows: Part I: machine learning; information leakage; signatures and re-encryption; side channels; formal modelling and verification; attacks; secure protocols; useful tools; blockchain and smart contracts. Part II: software security; cryptographic protocols; security models; searchable encryption; privacy; key exchange protocols; and web security. --

Managing the Mail - United States. National Archives and Records Service. Office of Records Management 1971

Guide to Ipsec Vpns - Sheila Frankel 2005-12-31

This publication seeks to assist organizations in mitigating the risks associated with the transmission of sensitive information across networks by providing practical guidance on implementing security services based on Internet Protocol Security (IPsec).

Blue Prism MasterClass: Developer & Professional Developer - Prasanna Kumar Ballepalli 2019-11-10

A course in a book for passing Blue Prism certification exams ! Blue Prism certification exams are quite intensive and require advanced knowledge of Blue Prism concepts. This edition includes scenario-based questions, which comprise many of the questions found on the exam as well as some challenging shorter questions. This edition includes hundreds of sample questions and critical time saving tips from each of knowledge areas presented in the Blue Prism exam syllabus for developer and professional developer certifications. These references provide an understanding of the types of exam questions that fall within each of the Blue Prism concepts. It also includes questions specifically related to knowledge areas and the various inputs, tools and techniques, and outputs. An essential self-study resource that can help to increase your chances of passing the

Blue Prism certification exam the first time.This book helps you to: Ensure you pass the exam on your FIRST attempt Focus on exam preparation Acquire valuable tools and techniques for development Decrease your study time by hundreds of hours

The Art of Deception - Kevin D. Mitnick 2011-08-04

The world's most infamous hacker offers an insider's view of the low-tech threats to high-tech security Kevin Mitnick's exploits as a cyber-desperado and fugitive form one of the most exhaustive FBI manhunts in history and have spawned dozens of articles, books, films, and documentaries. Since his release from federal prison, in 1998, Mitnick has turned his life around and established himself as one of the most sought-after computer security experts worldwide. Now, in The Art of Deception, the world's most notorious hacker gives new meaning to the old adage, "It takes a thief to catch a thief." Focusing on the human factors involved with information security, Mitnick explains why all the firewalls and encryption protocols in the world will never be enough to stop a savvy grifter intent on rifling a corporate database or an irate employee determined to crash a system. With the help of many fascinating true stories of successful attacks on business and government, he illustrates just how susceptible even the most locked-down information systems are to a slick con artist impersonating an IRS agent. Narrating from the points of view of both the attacker and the victims, he explains why each attack was so successful and how it could have been prevented in an engaging and highly readable style reminiscent of a true-crime novel. And, perhaps most importantly, Mitnick offers advice for preventing these types of social engineering hacks through security protocols, training programs, and manuals that address the human element of security.

Cyber Defence in the Age of AI, Smart

Societies and Augmented Humanity - Hamid Jahankhani 2020-04-06

This publication highlights the fast-moving technological advancement and infiltration of Artificial Intelligence into society. Concepts of evolution of society through interconnectivity are explored, together with how the fusion of human and technological interaction leading to Augmented Humanity is fast becoming more than just an endemic phase, but a cultural phase shift to digital societies. It aims to balance both the positive progressive outlooks such developments bring with potential issues that may stem from innovation of this kind, such as the invasive procedures of bio hacking or ethical connotations concerning the usage of digital twins. This publication will also give the reader a good level of understanding on fundamental cyber defence principles, interactions with Critical National Infrastructure (CNI) and the Command, Control, Communications and Intelligence (C3I) decision-making framework. A detailed view of the cyber-attack landscape will be garnered; touching on the tactics, techniques and procedures used, red and blue teaming initiatives, cyber resilience and the protection of larger scale systems. The integration of AI, smart societies, the human-centric approach and Augmented Humanity is discernible in the exponential growth, collection and use of [big] data; concepts woven throughout the diversity of topics covered in this publication; which also discusses the privacy and transparency of data ownership, and the potential dangers of exploitation through social media. As humans are become ever more interconnected, with the prolificacy of smart wearable devices and wearable body area networks, the availability of and abundance of user data and metadata derived from individuals has grown exponentially. The notion of data ownership, privacy and situational awareness are now at the forefront in this new age.

Scaling Networks v6 Companion Guide Cisco

Networking Academy 2017-08-17
Scaling Networks v6 Companion Guide is the official supplemental textbook for the Scaling Networks v6 course in the Cisco Networking Academy CCNA Routing and Switching curriculum. The Companion Guide is designed as a portable desk reference to use anytime, anywhere to reinforce the material from the course and organize your time. The book's features help you focus on important concepts to succeed in this course: · Chapter objectives–Review core concepts by answering the focus questions listed at the beginning of each chapter. · Key terms–Refer to the lists of networking vocabulary introduced and highlighted in context in each chapter. · Glossary–Consult the comprehensive Glossary with more than 250 terms. · Summary of Activities and Labs–Maximize your study time with this complete list of all associated practice exercises at the end of each chapter. · Check Your Understanding–Evaluate your readiness with the end-of-chapter questions that match the style of questions you see in the online course quizzes. The answer key explains each answer. How To–Look for this icon to study the steps you need to learn to perform certain tasks. Interactive Activities–Reinforce your understanding of topics with dozens of exercises from the online course identified throughout the book with this icon. Videos–Watch the videos embedded within the online course. Packet Tracer Activities–Explore and visualize networking concepts using Packet Tracer exercises interspersed throughout the chapters and provided in the accompanying Labs & Study Guide book. Hands-on Labs–Work through all the course labs and additional Class Activities that are included in the course and published in the separate Labs & Study Guide.

VMware NSX Micro-Segmentation ? Day 1 - Wade Holmes 2017-01-31
Micro-segmentation - Day 1 brings together the knowledge and guidance for planning,

designing, and implementing a modern security architecture for the software-defined data center based on micro-segmentation. VMware NSX makes network micro-segmentation feasible for the first time. It enables granular firewalling and security policy enforcement for every workload in the data center, independent of the network topology and complexity. Micro-segmentation with NSX already helped over a thousand organizations improve the security posture of their software-defined data center by fundamentally changing the way they approach security architecture. Micro-segmentation - Day 1 is your roadmap to simplify and enhance security within software-defined data centers running NSX. You will find insights and recommendations proven in the field for moving your organization from a perimeter-centric security posture to a micro-segmented architecture that provides enhanced security and visibility within your data center.

Program Evaluation Guide - United States. Patent and Trademark Office. Office of Planning and Evaluation 1996

Managing Democracy in the Digital Age - Julia Schwanholz 2017-09-22

In light of the increased utilization of information technologies, such as social media and the ‘Internet of Things,’ this book investigates how this digital transformation process creates new challenges and opportunities for political participation, political election campaigns and political regulation of the Internet. Within the context of Western democracies and China, the contributors analyze these challenges and opportunities from three perspectives: the regulatory state, the political use of social media, and through the lens of the public sphere. The first part of the book discusses key challenges for Internet regulation, such as data protection and censorship, while the second addresses the use of social media in political communication and political elections.

In turn, the third and last part highlights various opportunities offered by digital media for online civic engagement and protest in the public sphere. Drawing on different academic fields, including political science, communication science, and journalism studies, the contributors raise a number of innovative research questions and provide fascinating theoretical and empirical insights into the topic of digital transformation.

Cyber-Physical Threat Intelligence for Critical Infrastructures Security - John Soldatos 2020-06-30

Modern critical infrastructures comprise of many interconnected cyber and physical assets, and as such are large scale cyber-physical systems. Hence, the conventional approach of securing these infrastructures by addressing cyber security and physical security separately is no longer effective. Rather more integrated approaches that address the security of cyber and physical assets at the same time are required. This book presents integrated (i.e. cyber and physical) security approaches and technologies for the critical infrastructures that underpin our societies. Specifically, it introduces advanced techniques for threat detection, risk assessment and security information sharing, based on leading edge technologies like machine learning, security knowledge modelling, IoT security and distributed ledger infrastructures. Likewise, it presets how established security technologies like Security Information and Event Management (SIEM), pen-testing, vulnerability assessment and security data analytics can be used in the context of integrated Critical Infrastructure Protection. The novel methods and techniques of the book are exemplified in case studies involving critical infrastructures in four industrial sectors, namely finance, healthcare, energy and communications. The peculiarities of critical infrastructure protection in each one of these sectors is discussed and addressed based on sector-specific solutions.

The advent of the fourth industrial revolution (Industry 4.0) is expected to increase the cyber-physical nature of critical infrastructures as well as their interconnection in the scope of sectorial and cross-sector value chains. Therefore, the demand for solutions that foster the interplay between cyber and physical security, and enable Cyber-Physical Threat Intelligence is likely to explode. In this book, we have shed light on the structure of such integrated security systems, as well as on the technologies that will underpin their operation. We hope that Security and Critical Infrastructure Protection stakeholders will find the book useful when planning their future security strategies.

Cracking the Tech Career - Gayle Laakmann McDowell 2014-09-15

Become the applicant Google can't turn down Cracking the Tech Career is the job seeker's guide to landing a coveted position at one of the top tech firms. A follow-up to The Google Resume, this book provides new information on what these companies want, and how to show them you have what it takes to succeed in the role. Early planners will learn what to study, and established professionals will discover how to make their skillset and experience set them apart from the crowd. Author Gayle Laakmann McDowell worked in engineering at Google, and interviewed over 120 candidates as a member of the hiring committee – in this book, she shares her perspectives on what works and what doesn't, what makes you desirable, and what gets your resume saved or deleted. Apple, Microsoft, and Google are the coveted companies in the current job market. They field hundreds of resumes every day, and have their pick of the cream of the crop when it comes to selecting new hires. If you think the right alma mater is all it takes, you need to update your thinking. Top companies, especially in the tech sector, are looking for more. This book is the complete guide to becoming the candidate they just cannot turn away. Discover the career paths that run through the top tech firms Learn how to craft the prefect resume and prepare for the interview Find ways to make yourself stand out from the hordes of other applicants Understand what the top companies are looking for, and how to demonstrate that you're it These companies need certain skillsets, but they also want a great culture fit. Grades aren't everything, experience matters, and a certain type of applicant tends to succeed. Cracking the Tech Career reveals what the hiring committee wants, and shows you how to get it.

UTM Security with Fortinet - Kenneth Tam 2012-12-31

Traditionally, network security (firewalls to block unauthorized users, Intrusion Prevention Systems (IPS) to keep attackers out, Web filters to avoid misuse of Internet browsing, and antivirus software to block malicious programs) required separate boxes with increased cost and complexity. Unified Threat Management (UTM) makes network security less complex, cheaper, and more effective by consolidating all these components. This book explains the advantages of using UTM and how it works, presents best practices on deployment, and is a hands-on, step-by-step guide to deploying Fortinet's FortiGate in the enterprise. Provides tips, tricks, and proven suggestions and guidelines to set up FortiGate implementations Presents topics that are not covered (or are not covered in detail) by Fortinet's documentation Discusses hands-on troubleshooting techniques at both the project deployment level and technical implementation area

Whistleblowing for Change - Tatiana Bazzichelli 2021-11-30

The courageous acts of whistleblowing that inspired the world over the past few years have changed our perception of surveillance and control in today's information society. But what are the wider effects of whistleblowing as an act of dissent on politics, society, and the arts? How does it contribute to new courses of action, digital tools, and contents? This urgent intervention based on the work of Berlin's Disruption Network Lab examines this growing phenomenon, offering interdisciplinary pathways to empower the public by investigating whistleblowing as a developing political practice that has the ability to provoke change from within.

Chinese Investment in the United States - U S - China Economic and Security Review 2017-04-29

China's economic activities are having a clear and direct impact on the lives of average Americans. This impact is evident in the rise of Chinese investment in advanced sectors of the U.S. economy, including semiconductors and biotech, even as the Chinese government continues to restrict the ability of U.S. companies to invest in the same sectors, raising serious concerns for U.S. economic interests and national security. As the Trump administration prepares to formulate policy towards China, it is important to separate fact from fiction in the discussion of the key drivers and impacts of China's economic activities in the United States. According to data from the Rhodium Group, Chinese investment flows to the United States have grown steadily in recent years, reaching nearly $46 billion in 2016, a threefold increase from 2015. The speed of this investment flow growth coupled with a lack of reliable government data, both in China and the United States, has hindered efforts to accurately analyze trends in Chinese investment while also masking some of the risks and benefits these investments present to the United States. Even with limited official information, however, it is clear that Chinese investment is targeting sectors of strategic importance to the United States economy.

Nokia Firewall, VPN, and IPSO Configuration Guide - Andrew Hay 2009-02-07

"While Nokia is perhaps most recognized for its leadership in the mobile phone market, they have successfully demonstrated their knowledge of the Internet security appliance market and its customers requirements." --Chris Christiansen, Vice President, Internet Infrastructure and Security Software, IDC. Syngress has a long history of publishing market-leading books for system administrators and security professionals on commercial security products, particularly Firewall and Virtual Private Network (VPN) appliances from Cisco, Check Point, Juniper, SonicWall, and Nokia (see related titles for sales histories). The Nokia Firewall, VPN, and IPSO Configuration Guide will be the only book on the market covering the all-new Nokia Firewall/VPN Appliance suite. Nokia Firewall/VPN appliances are designed to protect and extend the network perimeter. According to IDC research, Nokia Firewall/VPN Appliances hold the #3 worldwide market-share position in this space behind Cisco and Juniper/NetScreen. IDC estimated the total Firewall/VPN market at $6 billion in 2007, and Nokia owns 6.6% of this market. Nokia's primary customers for security appliances are Mid-size to Large enterprises who need site-to-site connectivity and Mid-size to Large enterprises who need remote access connectivity through enterprise-deployed mobile devices. Nokia appliances for this market are priced form $1,000 for the simplest devices (Nokia IP60) up to $60,0000 for large enterprise- and service-provider class devices (like the Nokia IP2450 released in Q4 2007). While the feature set of such a broad product range obviously varies greatly, all of the appliances run on the same operating system: Nokia IPSO (IPSO refers to Ipsilon Networks, a company specializing in IP switching acquired by Nokia in 1997. The definition of the acronym has little to no meaning for customers.) As a result of this common operating system across the product line, The Nokia Firewall, VPN, and IPSO Configuration Guide will be an essential reference to users of any of these products. Users manage the Nokia IPSO (which is a Linux variant, specifically designed for these appliances) through a Web interface called Nokia Network Voyager or via a powerful Command Line Interface (CLI). Coverage within the book becomes increasingly complex relative to the product line. The Nokia Firewall, VPN, and IPSO Configuration Guide and companion Web site will provide seasoned network administrators and security professionals with the in-depth coverage and step-by-step walkthroughs they require to properly secure their network perimeters and ensure safe connectivity for remote users. The book contains special chapters devoted to mastering the complex Nokia IPSO command line, as well as tips and tricks for taking advantage of the new "ease of use" features in the Nokia Network Voyager Web interface. In addition, the companion Web site offers downloadable video walkthroughs on various installation and troubleshooting tips from the authors. * Only book on the market covering Nokia Firewall/VPN appliances, which hold 6.6% of a $6 billion market * Companion website offers video walkthroughs on various installation and troubleshooting tips from the authors * Special chapters detail mastering the complex Nokia IPSO command line, as well as tips and tricks for taking advantage of the new "ease of use" features in the Nokia Network Voyager Web interface

Security Information and Event Management (SIEM) Implementation - David Miller 2010-11-05

Implement a robust SIEM system Effectively manage the security information and events produced by your network with help from this authoritative guide. Written by IT security experts, Security Information and Event Management (SIEM) Implementation shows you how to deploy SIEM technologies to monitor, identify, document, and respond to security threats and reduce false-positive alerts. The book explains how to implement SIEM products from different vendors, and discusses the strengths, weaknesses, and advanced tuning of these systems. You'll also learn how to use SIEM capabilities for business intelligence. Real-world case studies are included in this comprehensive resource. Assess your organization's business models, threat models, and regulatory compliance requirements Determine the necessary SIEM components for small- and medium-size businesses Understand SIEM anatomy—source device, log collection, parsing/normalization of logs, rule engine, log storage, and event monitoring Develop an effective incident response program Use the inherent capabilities of your SIEM system for business intelligence Develop filters and correlated event rules to reduce false-positive alerts Implement AlienVault's Open Source Security Information Management (OSSIM) Deploy the Cisco Monitoring Analysis and Response System (MARS) Configure and use the Q1 Labs QRadar SIEM system Implement ArcSight Enterprise Security Management (ESM) v4.5 Develop your SIEM security analyst skills