Magic Quadrant For Unified Threat Management Protego

With many scholars and analysts questioning the relevance of deterrence as a valid strategic concept, this volume moves beyond Cold War nuclear deterrence to show the many ways in which deterrence is applicable to contemporary security. It examines the possibility of applying deterrence theory and practice to space, to cyberspace, and against non-state actors. It also examines the role of nuclear deterrence in the twenty-first century a reaches surprising conclusions.

Harness new techniques that let you see what is happening on your networks and take decisive action without getting lost in a sea of data.

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 proj deployment level and technical implementation area

During the Cold War, freedom of expression was vaunted as liberal democracy's most cherished possession—but such freedom was put in service of a hidden agenda. In The Cultural Cold War, Frances Stonor Saunders reveals the extraordinary efforts of a secret campaign in which some of the most vocal exponents of intellectual freedom in the West were working for or subsidized by the CIA—whether they knew it or not. Called "the mos comprehensive account yet of the [CIA's] activities between 1947 and 1967" by the New York Times, the book presents shocking evidence of the CIA's undercover program of cultural interventions in Western Europe and at home, drawing together declassified documents and exclusive interviews to expose the CIA's astonishing campaign to deploy the likes of Hannah Arendt, Isaiah Berlin, Leonard Bernstein, Robert Lowell, George Orwell, Jackson Pollock as weapons in the Cold War. Translated into ten languages, this classic work—now with a new preface by the author—is "a real contribution to popular understanding of the postwar period" (The Wall Street Journal), and its story of covert cultural efforts to win hearts and minds continues to be relevant today.

Thinking about Deterrence

Demystifying Impacts of the Fourth Industrial Revolution

Religion, Skepticism, and Literature in Nineteenth-Century America

Penetration Testing

Surprise, Kill, Vanish

A New Framework for Analysis

Microsoft Azure Security Center

In Melville's Wisdom: Religion, Skepticism, Literature in Nineteenth-Century America, Damien B. Schlarb explores the manner in which Herman Melville responds to the spiritual crisis of modernity by using the language of the biblical Old Testament wisdom books to moderate contemporary discourses on religion, skepticism, and literature. Schlarb argues that attending to Melville's engagement with the wisdom books (Job, Proverbs, and Ecclesiastes) can help us understand a paradox at the heart of American modernity: the simultaneous displacement and affirmation of biblical language and religious culture. In wisdom, which addresses questions of theology, radical skepticism, and the nature of evil, Melville finds an ethos of critical inquiry that allows him to embrace modern analytical techniques, such as higher biblical criticism. In the medium of literature, he articulates a new way of accessing the Bible by marrying the moral and spiritual didacticism of its language with the intellectual distance afforded by critical reflection, a hallmark of modern intellectual style. Melville's Wisdom joins other works of post secular literary studies in challenging its own discipline's constitutive secularization narrative by rethinking modern, putatively secular cultural formations in terms of their reciprocity with religious concepts and texts. Schlarb foregrounds Melville's sustained, career-spanning concern with biblical wisdom, its formal properties, and its knowledge-creating potential. By excavating this project from his oeuvre, Melville's Wisdom shows how Melville celebrates intellectually rigorous, critical inquisitiveness, an attitude that we often associate with modernity but which Melville saw augured by the wisdom books. He finds in this attitude the means for avoiding the spiritually corrosive effects of skepticism.

This document brings together a set of latest data points and publicly available information relevant for Digital Customer Experience. We are very excited to share this content and believe that readers will benefit immensely from this periodic publication immensely.

In a world of rising tensions between Russia and the United States, the Middle East and Europe, Sunnis and Shiites, Islamism and liberalism, Turkey is at the epicentre. And at the heart of Turkey is its right-wing populist president, Recep Tayyip Erdo?an. Since 2002, Erdo?an has consolidated his hold on domestic politics while using military and diplomatic means to solidify Turkey as a regional power. His crackdown has been brutal and consistent - scores of journalists arrested, academics officially banned from leaving the country, university deans fired and many of the highest-ranking military officers arrested. In some senses, the nefarious and failed 2016 coup has given Erdo?an the licence to make good on his repeated promise to bring order and stability under a 'strongman'. Here, leading Turkish expert Soner Cagaptay will look at Erdo?an's roots in Turkish history, what he believes in and how he has cemented his rule, as well as what this means for the world. The book will also unpick the 'threats' Erdogan has worked to combat - from the liberal Turks to the Gulen movement, from coup plotters to Kurdish nationalists - all of which have culminated in the crisis of modern Turkey.

Enterprise Cybersecurity empowers organizations of all sizes to defend themselves with next-generation cybersecurity programs against the escalating threat of modern targeted cyberattacks. This book presents a comprehensive framework for managing all aspects of an enterprise cybersecurity program. It enables an enterprise to architect, design, implement, and operate a coherent cybersecurity program that is seamlessly coordinated with policy, programmatics, IT life cycle, and assessment. Fail-safe cyberdefense is a pipe dream. Given sufficient time, an intelligent attacker can eventually defeat defensive measures protecting an enterprise's computer systems and IT networks. To prevail, an enterprise cybersecurity program must manage risk by detecting attacks early enough and delaying them long enough that the defenders have time to respond effectively. Enterprise Cybersecurity shows players at all levels of responsibility how to unify their organization's people, budgets, technologies, and processes into a cost-efficient cybersecurity program capable of countering advanced cyberattacks and containing damage in the event of a breach. The authors of Enterprise Cybersecurity explain at both strategic and tactical levels how to accomplish the mission of leading, designing, deploying, operating, managing, and supporting cybersecurity capabilities in an enterprise environment. The authors are recognized experts and thought leaders in this rapidly evolving field, drawing on decades of collective experience in cybersecurity and IT. In capacities ranging from executive strategist to systems architect to cybercombatant, Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, and Abdul Aslam have fought on the front lines of cybersecurity against advanced persistent threats to government, military, and business entities.

Configuration and Troubleshooting Best Practices for the Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Advanced Malware Protection (AMP)

Security

T-Bytes Hybrid Cloud Infrastructure

Overview of patent out-licencing opportunities

History, Art and Science in 101 Designer Puzzles

64 Methods to Reduce Costs and Increase Value with Suppliers

Practical Internet of Things Security

Whether you just wanted to start your Sudoku adventure or add magic to a long-established habit, this book is intended for you. You will find here 101 specially designed puzzles accompanied by mini-essays on a wide variety of entertaining topics. The distinctive puzzles serve as illustrations to the popular articles and, in return, the articles give life back to the objects depicted in the puzzles. Did you know, for example, that Archimedes, unhappy with Apollonius of Perga finding a better approximation to than his 22/7, threw down the mathematical gauntlet in the form of the formidable "Cattle Problem"? And that to ensure that no one, Apollonius included, could solve the riddle, Archimedes so devised the problem that its smallest solution had 206,545 digits? Sudoku Stories will provide you with a unique puzzle-solving experience in the company of James Bond, Harry Houdini, Sherlock Holmes, space explorers, Spanish "Conquistadores," lightning bugs and electrical plugs and the rest of the 101 characters, animals and objects of note. Pocket Edition, Black & White, Trim Size: 5" x 8" A selection of the book's puzzles can be played free on SudokuStories.com.

A practical, indispensable security guide that will navigate you through the complex realm of securely building and deploying systems in our IoT-connected world About This Book Learn to design and implement cyber security strategies for your organization Learn to protect cyber-physical systems and utilize forensic data analysis to beat vulnerabilities in your IoT ecosystem Learn best practices to secure your data from device to the cloud Gain insight into privacy-enhancing techniques and technologies Who This Book Is For This book targets IT Security Professionals and Security Engineers (including pentesters, security architects and ethical hackers) who would like to ensure security of their organization's data when connected through the IoT. Business analysts and managers will also find it useful. What You Will Learn Learn how to break down cross-industry barriers by adopting the best practices for IoT deployments Build a rock-solid security program for IoT that is cost-effective and easy to maintain Demystify complex topics such as cryptography, privacy, and penetration testing to improve your security posture See how the selection of individual components can affect the security posture of the entire system Use Systems Security Engineering and Privacy-by-design principles to design a secure IoT ecosystem Get to know how to leverage the burdgening cloud-based systems that will support the IoT into the future. In Detail With the advent of Intenret of Things (IoT), businesses will be faced with defending against new types of threats. The business ecosystem now includes cloud computing infrastructure, mobile and fixed endpoints that open up new attack surfaces, a desire to share information with many stakeholders and a need to take action quickly based on large quantities of collected data. . It therefore becomes critical to ensure that cyber security threats are contained to a minimum when implementing new IoT services and solutions. . The interconnectivity of people, devices, and companies raises stakes to a new level as computing and action become even more mobile, everything becomes connected to the cloud, and infrastructure is strained to securely manage the billions of devices that will connect us all to the IoT. This book shows you how to implement cyber-security solutions, IoT design best practices and risk mitigation methodologies to address device and infrastructure threats to IoT solutions. This book will take readers on a journey that begins with understanding the IoT and how it can be applied in various industries, goes on to describe the security challenges associated with the IoT, and then provides a set of guidelines to architect and deploy a secure IoT in your Enterprise. The book will showcase how the IoT is implemented in early-adopting industries and describe how lessons can be learned and shared across diverse industries to support a secure IoT. Style and approach This book aims to educate readers on key areas in IoT security. It walks readers through engaging with security challenges and then provides answers on how to successfully manage IoT security and build a safe infrastructure for smart devices. After reading this book, you will understand the true potential of tools and solutions in order to build real-time security intelligence on IoT networks.

Love, and war—and dragons! "A sweet standalone romantic fantasy... richly imagined." -- Publisher's Weekly Old Forge is known for its dragons—savage little things, more singe than snarl—and Milo Priddy is known for his way with them. When rumblings of conflict appear on the horizon, the dragons start to disappear. Milo is dragonkin, and knows what he must do. It is an uneasy choice, and one he dares not reveal even to his lover, Ellis. As leader of neighbouring Wellech, Ellis has his own hard choices. His skills are crucial to a secure homeland. More and more, the homeland he and Milo once hoped to share is under threat--not only from outside, but within. For their own people are sowing mistrust of the magic users, seeding a betrayal of not only the dragons, but their kin.

This volume brings together some of the world's leading scholars of market categorization. Together, their contributions depict categorization as both a cognitive and a social process, tightly connected to actors involved, their specific acts, the entity being categorized, and the context and timing which inform these activities.

The New Sultan

Modern Cybersecurity Strategies for Enterprises

First International Conference, TrustBus 2004, Zaragoza, Spain, August 30-September 1, 2004, Proceedings

Global Innovation Index 2020

DICOM Structured Reporting

The Purchasing Chessboard

The CIA and the World of Arts and Letters

Big data, analytics, and artificial intelligence are revolutionizing work, management, and lifestyles and are becoming disruptive technologies for healthcare, e-commerce, and web services. However, many fundamental, technological, and managerial issues for developing and applying intelligent big data analytics in these fields have yet to be addressed. Managerial Perspectives on Intelligent Big Data Analytics is a collection of innovative research that discusses the integration and application of artificial intelligence, business intelligence, digital transformation, and intelligent big data analytics from a perspective of computing, service, and management. While highlighting topics including e-commerce, machine learning, and fuzzy logic, this book is ideally designed for students, government officials, data scientists, managers, consultants, analysts, IT specialists, academicians, researchers, and industry professionals in fields that include big data, artificial intelligence, computing, and commerce.

The biggest online threat to businesses and consumers today is ransomware, a category of malware that can encrypt your computer files until you pay a ransom to unlock them. With this practical book, you'll learn how easily ransomware infects your system and what steps you can take to stop the attack before it sets foot in the network. Security experts Allan Liska and Timothy Gallo explain how the success of these attacks has spawned not only several variants of ransomware, but also a litany of ever-changing ways they're delivered to targets. You'll learn pragmatic methods for responding quickly to a ransomware attack, as well as how to protect yourself from becoming infected in the first place. Learn how ransomware enters your system and encrypts your files Understand why ransomware use has grown, especially in recent years Examine the organizations behind ransomware and the victims they target Learn how wannabe hackers use Ransomware as a Service (RaaS) to launch campaigns Understand how ransom is paid—and the pros and cons of paying Use methods to protect your organization's workstations and servers

Based on an innovative blend of Kabbalah and magic, a step-by-step program toward spiritual attainment guides readers through each level of the the Golden Dawn system of ritual magic and its corresponding sphere in the Kabbalah Tree of Life. Original. 10,000 first printing.

This Festschrift volume, published in honor of Nissim Francez on the occasion of his 65th birthday, contains 15 papers, written by friends and colleagues, many of whom congregated at a celebratory symposium held on May 2009, in Haifa, Israel.

Systems Analysis and Design in a Changing World

Cyber-Physical Threat Intelligence for Critical Infrastructures Security

A Beginner's Guide to Protecting and Recovering from Ransomware Attacks

Security Information and Event Management (SIEM) Implementation

A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures

T-Byte Digital Customer Experience

Essays Dedicated to Nissim Francez on the Occasion of His 65th Birthday

Network security is not simply about building impenetrable walls—determined attackers will eventually overcome traditional defenses. The most effective computer security strategies integrate network security monitoring (NSM): the collection and analysis of data to help you detect and respond to intrusions. In The Practice of Network Security Monitoring, Mandiant CSO Richard Bejtlich shows you how to use NSM to add a robust layer of protection around your networks—no prior experience required. To help you avoid costly and inflexible solutions, he teaches you how to deploy, build, and run an NSM operation using open source software and vendor-neutral tools. You'll learn how to: –Determine where to deploy NSM platforms, and size them for the monitored networks –Deploy stand-alone or distributed NSM installations –Use command line and graphical packet analysis tools, and NSM consoles –Interpret network evidence from server-side and client-side intrusions –Integrate threat intelligence into NSM software to identify sophisticated adversaries There's no foolproof way to keep attackers out of your network. But when they get in, you'll be prepared. The Practice of Network Security Monitoring will show you how to build a security net to detect, contain, and control them. Attacks are inevitable, but losing sensitive data shouldn't be.

This dynamic and beautifully written textbook takes a modern and innovative approach to strategy by placing technology at its heart, bridging the gap between general strategy texts and specialist technology and innovation literature. It addresses the challenges and opportunities presented to organisations by disruptive technological change and takes into account the navigation of uncertain business environments. In addition to examining more established concepts and theories, the text also explores new disruptive business models and non-traditional approaches to strategy development such as effectuation, the Business Model Canvas and prediction logic. This comprehensive and critical approach is supported by a rich assortment of practical examples and cases drawn from different sectors and a range of exciting companies from all over the world, helping students and practitioners to apply theory to practice. This will be an essential core text for modules on technology strategy and innovation at upper undergraduate, postgraduate and MBA levels, and invaluable reading for senior executives and aspiring managers who seek to understand how to implement strategy in a volatile disruptive environment.

UTM Security with FortinetMastering FortiOSNewnes

Is my enterprise really prepared for future business? What can I do to become more competitive? Ulf Pillkahn's book is directed at all of those seeking answers to these questions: executives in strategic positions, business analysts, consultants, trend scouts, marketing and product managers and research engineers. The book presents the two most powerful tools for future planning: environmental analysis, based on the use of trends, as well as the development of visions of the future through the use of scenarios. While scenarios are generally regarded as a classical management tool, it is expected that the importance of trends will gain tremendously in the coming years. Pillkahn demonstrates how to build robust strategies by aligning the results of environmental and enterprise scenarios, thereby offering entirely new insights. "Using Trends and Scenarios as Tools for Strategy Development" convincingly illustrates why efficient observation of the environment of an enterprise is an absolutely essential factor for strategy development, and why strategy development only works if it is institutionalized as a permanent enterprise process. It also addresses the issue of what information is needed to keep both processes running. The book further describes how trends can be categorized, and offers advice on how to glean the essential information from the vast variety of trends. Information is provided on how scenarios are used as a holistic instrument for creating visions and pictures of the future, and how the results of trend research and scenario techniques find their way into entrepreneurial strategy development. An optimized strategy development process is also outlined. Practical examples and real-life pictures of the future round off Pillkahn's insightful discussion of future business planning.

Cisco Firepower Threat Defense (FTD)

Using Trends and Scenarios as Tools for Strategy Development

Protect and Secure Your Enterprise Networks, Digital Business Assets, and Endpoint Security with Tested and Proven Methods (English Edition)

System Engineering Analysis, Design, and Development

Ransomware

Ransomware Revealed

Kabbalah, Magic, and the Great Work of Self-transformation

Many network security threats today are spread over the internet, making it imperative to monitor and prevent unauthorized access, misuse, modification, or denial of a computer network and other network-accessible resources. Many businesses have been securing themselves over the internet through firewalls and encryption mechanisms; however network security is now undergoing a transformational stage with the advent of cloud computing and rapid penetration of mobile devices. In this report, we have analyzed the technological landscape of this impactful technology from the perspective of Intellectual Property (Patents).

As one of the first books to distill the economics of information and networks into practical business strategies, this is a guide to the winning moves that can help business leaders--from writers, lawyers and finance professional to executives in the entertainment, publishing and hardware and software industries-- navigate successfully through the information economy.

This document brings together a set of latest data points and publicly available information relevant for Hybrid Cloud Infrastructure Industry. We are very excited to share this content and believe that readers will benefit from this periodic publication immensely.

Sincerely welcome to proceedings of the 1st International Conference on Trust and Privacy in Digital Business, Zaragoza, Spain, held from August 30th to September 1st, 2004. This conference was an outgrowth of the two successful TrustBus inter- tional workshops, held in 2002 and 2003 in conjunction with the DEXA conferences in Aix-en-Provence and in Prague. Being the first of a planned series of successful conferences it was our goal that this event would initiate a forum to bring together researchers from academia and commercial developers from industry to discuss the state of the art of technology for establishing trust and privacy in digital business. We thank you all the attendees for coming to Zaragoza to participate and debate the new emerging advances in this area. The conference program consisted of one invited talk and nine regular technical papers sessions. The invited talk and keynote speech was delivered by Ahmed Patel from the Computer Networks and Distributed Systems Research Group, University College Dublin, Ireland on "Developing Secure, Trusted and Auditable Services for E-Business: An Autonomic Computing Approach". A paper covering his talk is also contained in this book. The regular paper sessions covered a broad range of topics, from access control - sues to electronic voting, from trust and protocols to digital rights management. The conference attracted close to 100 submissions of which the program committee - cepted 29 papers for presentation and inclusion in the conference proceedings.

How to Build a Successful Cyberdefense Program Against Advanced Threats

Melville's Wisdom

A Hands-On Introduction to Hacking

Languages: From Formal to Natural

The Secret History of CIA Paramilitary Armies, Operators, and Assassins

Mastering FortiOS

Two schools of thought now exist in security studies: traditionalists want to restrict the subject to politico-military issues; while wideners want to extend it to the economic, societal and environmental sectors. This book sets out a comprehensive statement of the new security studies, establishing the case for the broader agenda.

Refined and streamlined, SYSTEMS ANALYSIS AND DESIGN IN A CHANGING WORLD, 7E helps students develop the conceptual, technical, and managerial foundations for systems analysis design and implementation as well as project management principles for systems development. Using case driven techniques, the succinct 14-chapter text focuses on content that is key for success in today's market. The authors' highly effective presentation teaches both traditional (structured) and object-oriented (OO) approaches to systems analysis and design. The book highlights use cases, use diagrams, and use case descriptions required for a modeling approach, while demonstrating their application to traditional, web development, object-oriented, and service-oriented architecture approaches. The Seventh Edition's refined sequence of topics makes it easier to read and understand than ever. Regrouped analysis and design chapters provide more flexibility in course organization. Additionally, the text's running cases have been completely updated and now include a stronger focus on connectivity in applications. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Praise for the first edition: "This excellent text will be useful to everysystem engineer (SE) regardless of the domain. It covers ALLrelevant SE material and does so in a very clear, methodicalfashion. The breadth and depth of the author's presentation ofSE principles and practices is outstanding." –Philip Allen This textbook presents a comprehensive, step-by-step guide toSystem Engineering analysis, design, and development via anintegrated set of concepts, principles, practices, andmethodologies. The methods presented in this text apply to any typeof human system -- small, medium, and large organizational systemsand system development projects delivering engineered systems orservices across multiple business sectors such as medical,transportation, financial, educational, governmental, aerospace anddefense, utilities, political, and charity, among others. Provides a common focal point for "bridgingthe gap" between and unifying System Users, System Acquirers,multi-discipline System Engineering, and Project, Functional, andExecutive Management education, knowledge, and decision-making fordeveloping systems, products, or services Each chapter provides definitions of key terms,guiding principles, examples, author's notes, real-worldexamples, and exercises, which highlight and reinforce key SE&Dconcepts and practices Addresses concepts employed in Model-BasedSystems Engineering (MBSE), Model-Driven Design (MDD), UnifiedModeling Language (UMLTM) / Systems Modeling Language(SysMLTM), and Agile/Spiral/V-Model Development such asuser needs, stories, and use cases analysis; specificationdevelopment; system architecture development; User-Centric SystemDesign (UCSD); interface definition & control; systemintegration & test; and Verification & Validation(V&V) Highlights/introduces a new 21st Century SystemsEngineering & Development (SE&D) paradigm that is easy tounderstand and implement. Provides practices that are critical stagingpoints for technical decision making such as Technical StrategyDevelopment; Life Cycle requirements; Phases, Modes, & States;SE Process; Requirements Derivation; System ArchitectureDevelopment, User-Centric System Design (UCSD); EngineeringStandards, Coordinate Systems, and Conventions; et al. Thoroughly illustrated, with end-of-chapter exercises andnumerous case studies and examples, Systems EngineeringAnalysis, Design, and Development, Second Edition is a primarytextbook for multi-discipline, engineering, system analysis, andproject management undergraduate/graduate level students and avaluable reference for professionals.

Security is a shared responsibility, and we must all own it KEY FEATURES ● Expert-led instructions on the pillars of a secure corporate infrastructure and identifying critical components. ● Provides Cybersecurity strategy templates, best practices, and recommendations presented with diagrams. ● Adopts a perspective of developing a Cybersecurity strategy that aligns with business goals. DESCRIPTION Once a business is connected to the Internet, it is vulnerable to cyberattacks, threats, and vulnerabilities. These vulnerabilities now take several forms, including Phishing, Trojans, Botnets, Ransomware, Distributed Denial of Service (DDoS), Wiper Attacks, Intellectual Property thefts, and others. This book will help and guide the readers through the process of creating and integrating a secure cyber ecosystem into their digital business operations. In addition, it will help readers safeguard and defend the IT security infrastructure by implementing the numerous tried-and-tested procedures outlined in this book. The tactics covered in this book provide a moderate introduction to defensive and offensive strategies, and they are supported by recent and popular use-cases on cyberattacks. The book provides a well-illustrated introduction to a set of methods for protecting the system from vulnerabilities and expert-led measures for initiating various urgent steps after an attack has been detected. The ultimate goal is for the IT team to build a secure IT infrastructure so that their enterprise systems, applications, services, and business processes can operate in a safe environment that is protected by a powerful shield. This book will also walk us through several recommendations and best practices to improve our security posture. It will also provide guidelines on measuring and monitoring the security plan's efficacy. WHAT YOU WILL LEARN ● Adopt MITRE ATT&CK and MITRE framework and examine NIST, ITIL, and ISMS recommendations. ● Understand all forms of vulnerabilities, application security mechanisms, and deployment strategies. ● Know-how of Cloud Security Posture Management (CSPM), Threat Intelligence, and modern SIEM systems. ● Learn security gap analysis, Cybersecurity planning, and strategy monitoring. ● Investigate zero-trust networks, data forensics, and the role of AI in Cybersecurity. ● Comprehensive understanding of Risk Management and Risk Assessment Frameworks. WHO THIS BOOK IS FOR Professionals in IT security, Cybersecurity, and other related fields working to improve the organization's overall security will find this book a valuable resource and companion. This book will guide young professionals who are planning to enter Cybersecurity with the right set of skills and knowledge. TABLE OF CONTENTS Section - I: Overview and Need for Cybersecurity 1. Overview of Information Security and Cybersecurity 2. Aligning Security with Business Objectives and Defining CISO Role Section - II: Building Blocks for a Secured Ecosystem and Identification of Critical Components 3. Next-generation Perimeter Solutions 4. Next-generation Endpoint Security 5. Security Incident Response (IR) Methodology 6. Cloud Security & Identity Management 7. Vulnerability Management and Application Security 8. Critical Infrastructure Component of Cloud and Data Classification Section - III: Assurance Framework (the RUN Mode) and Adoption of Regulatory Standards 9. Importance of Regulatory Requirements and Business Continuity 10. Risk management- Life Cycle 11. People, Process, and Awareness 12. Threat Intelligence & Next-generation SIEM Solution 13. Cloud Security Posture Management (CSPM) Section - IV: Cybersecurity Strategy Guidelines, Templates, and Recommendations 14. Implementation of Guidelines & Templates 15. Best Practices and Recommendations

A Complete Course

The Practice of Network Security Monitoring

The Cultural Cold War

Understanding Incident Detection and Response

Information Rules

From Categories to Categorization

The Digital Transformation of Logistics

The authoritative visual guide to Cisco Firepower Threat Defense (FTD) This is the definitive guide to best practices and advanced troubleshooting techniques for the Cisco flagship Firepower Threat Defense (FTD) system running on Cisco ASA platforms, Cisco Firepower security appliances, Firepower eXtensible Operating System (FXOS), and VMware virtual appliances. Senior Cisco engineer Nazmul Rajib draws on unsurpassed experience supporting and training Cisco Firepower engineers worldwide, and presenting detailed knowledge of Cisco Firepower deployment, tuning, and troubleshooting. Writing for cybersecurity consultants, service providers, channel partners, and enterprise or government security professionals, he shows how to deploy the Cisco Firepower next-generation security technologies to protect your network from potential cyber threats, and how to use Firepower's robust command-line tools to investigate a wide variety of technical issues. Each consistently organized chapter contains definitions of keywords, operational flowcharts, architectural diagrams, best practices, configuration steps (with detailed screenshots), verification tools, troubleshooting techniques, and FAQs drawn directly from issues raised by Cisco customers at the Global Technical Assistance Center (TAC). Covering key Firepower materials on the CCNA Security, CCNP Security, and CCIE Security exams, this guide also includes end-of-chapter quizzes to help candidates prepare. · Understand the operational architecture of the Cisco Firepower NGFW, NGIPS, and AMP technologies · Deploy FTD on ASA platform and Firepower appliance running FXOS · Configure and troubleshoot Firepower Management Center (FMC) · Plan and deploy FMC and FTD on VMware virtual appliance · Design and implement the Firepower management network on FMC and FTD · Understand and apply Firepower licenses, and register FTD with FMC · Deploy FTD in Routed, Transparent, Inline, Inline Tap, and Passive Modes · Manage traffic flow with detect-only, block, trust, and bypass operations · Implement rate limiting and analyze quality of service (QoS) · Blacklist suspicious IP addresses via Security Intelligence · Block DNS queries to the malicious domains · Filter URLs based on category, risk, and reputation · Discover a network and implement application visibility and control (AVC) · Control file transfers and block malicious files using advanced malware protection (AMP) · Halt cyber attacks using Snort-based intrusion rule · Masquerade an internal host's original IP address using Network Address Translation (NAT) · Capture traffic and obtain troubleshooting files for advanced analysis · Use command-line tools to identify status, trace packet flows, analyze logs, and debug messages

The Global Innovation Index 2020 provides detailed metrics about the innovation performance of 131 countries and economies around the world. Its 80 indicators explore a broad vision of innovation, including political environment, education, infrastructure and business sophistication. The 2020 edition sheds light on the state of innovation financing by investigating the evolution of financing mechanisms for entrepreneurs and other innovators, and by pointing to progress and remaining challenges – including in the context of the economic slowdown induced by the coronavirus disease (COVID-19) crisis.

From Pulitzer Prize finalist Annie Jacobsen, the untold USA Today bestselling story of the CIA's secret paramilitary units. Surprise . . . your target. Kill . . . your enemy. Vanish . . . without a trace. When diplomacy fails, and war is unwise, the president calls on the CIA's Special Activities Division, a highly-classified branch of the CIA and the most effective, black operations force in the world. Originally known as the president's guerrilla warfare corps, SAD conducts risky and ruthless operations that have evolved over time to defend America from its enemies. Almost every American president since World War II has asked the CIA to conduct sabotage, subversion and, yes, assassination. With unprecedented access to forty-two men and women who proudly and secretly worked on CIA covert operations from the dawn of the Cold War to the present day, along with declassified documents and deep historical research, Pulitzer Prize finalist Annie Jacobsen unveils -- like never before -- a complex world of individuals working in treacherous environments populated with killers, connivers, and saboteurs. Despite Hollywood notions of off-book operations and external secret hires, covert action is actually one piece in a colossal foreign policy machine. Written with the pacing of a thriller, Surprise, Kill, Vanish brings to vivid life the sheer pandemonium and chaos, as well as the unforgettable human will to survive and the intellectual challenge of not giving up hope that define paramilitary and intelligence work. Jacobsen's exclusive interviews -- with members of the CIA's Senior Intelligence Service (equivalent to the Pentagon's generals), its counterterrorism chiefs, targeting officers, and Special Activities Division's Ground Branch operators who conduct today's close-quarters killing operations around the world -- reveal, for the first time, the enormity of this shocking, controversial, and morally complex terrain. Is the CIA's paramilitary army America's weaponized strength, or a liability to its principled standing in the world? Every operation reported in this book, however unsettling, is legal.

The digital transformation is in full swing and fundamentally changes how we live, work, and communicate with each other. From retail to finance, many industries see an inflow of new technologies, disruption through innovative platform business models, and employees struggling to cope with the significant shifts occurring. This Fourth Industrial Revolution is predicted to also transform Logistics and Supply Chain Management, with delivery systems becoming automated, smart networks created everywhere, and data being collected and analyzed universally. The Digital Transformation of Logistics: Demystifying Impacts of the Fourth Industrial Revolution provides a holistic overview of this vital subject clouded by buzz, hype, and misinformation. The book is divided into three themed-sections: Technologies such as self-driving cars or virtual reality are not only electrifying science fiction lovers anymore, but are also increasingly presented as cure-all remedies to supply chain challenges. In The Digital Transformation of Logistics: Demystifying Impacts of the Fourth Industrial Revolution, the authors peel back the layers of excitement that have grown around new technologies such as the Internet of Things (IoT), 3D printing, Robotic Process Automation (RPA), Blockchain or Cloud computing, and show use cases that give a glimpse about the fascinating future we can expect. Platforms that allow businesses to centrally acquire and manage their logistics services disrupt an industry that has been relationship-based for centuries. The authors discuss smart contracts, which are one of the most exciting applications of Blockchain, Software as a Service (SaaS) offerings for freight procurement, where numerous data sources can be integrated and decision-making processes automated, and marine terminal operating systems as an integral node for shipments. In The Digital Transformation of Logistics: Demystifying Impacts of the Fourth Industrial Revolution, insights are shared into the cold chain industry where companies respond to increasing quality demands, and how European governments are innovatively responding to challenges of cross-border eCommerce. People are a vital element of the digital transformation and must be on board to drive change. The Digital Transformation of Logistics: Demystifying Impacts of the Fourth Industrial Revolution explains how executives can create sustainable impact and how competencies can be managed in the digital age - especially for sales executives who require urgent upskilling to remain relevant. Best practices are shared for organizational culture change, drawing on studies among senior leaders from the US, Singapore, Thailand, and Australia, and for managing strategic alliances with logistics service providers to offset risks and create cross-functional, cross-company transparency. The Digital Transformation of Logistics: Demystifying Impacts of the Fourth Industrial Revolution provides realistic insights, a ready-to-use knowledge base, and a working vocabulary about current activities and emerging trends of the Logistics industry. Intended readers are supply chain professionals working for manufacturing, trading, and freight forwarding companies as well as students and all interested parties.

Who Will Finance Innovation?

Applied Security Visualization

Sudoku Stories

Sonata Form

We Have Never Been Modern

Jurassic Park

Trust and Privacy in Digital Business

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.

Penetration testers simulate cyber attacks to find security weaknesses in networks, operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. In Penetration Testing, security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pentester needs. Using a virtual machine–based lab that includes Kali Linux and vulnerable operating systems, you'll run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you'll experience the key stages of an actual assessment—including information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more. Learn how to: –Crack passwords and wireless network keys with brute-forcing and wordlists –Test web applications for vulnerabilities –Use the Metasploit Framework to launch exploits and write your own Metasploit modules –Automate social-engineering attacks –Bypass antivirus software –Turn access to one machine into total control of the enterprise in the post exploitation phase You'll even explore writing your own exploits. Then it's on to mobile hacking—Weidman's particular area of research—with her tool, the Smartphone Pentest Framework. With its collection of hands-on lessons that cover key tools and strategies, Penetration Testing is the introduction that every aspiring hacker needs.

Discover high-value Azure security insights, tips, and operational optimizations This book presents comprehensive Azure Security Center techniques for safeguarding cloud and hybrid environments. Leading Microsoft security and cloud experts Yuri Diogenes and Dr. Thomas Shinder show how to apply Azure Security Center's full spectrum of features and capabilities to address protection, detection, and response in key operational scenarios. You'll learn how to secure any Azure workload, and optimize virtually all facets of modern security, from policies and identity to incident response and risk management. Whatever your role in Azure security, you'll learn how to save hours, days, or even weeks by solving problems in most efficient, reliable ways possible. Two of Microsoft's leading cloud security experts show how to: • Assess the impact of cloud and hybrid environments on security, compliance, operations, data protection, and risk management • Master a new security paradigm for a world without traditional perimeters • Gain visibility and control to secure compute, network, storage, and application workloads • Incorporate Azure Security Center into your security operations center • Integrate Azure Security Center with Azure AD Identity Protection Center and third-party solutions • Adapt Azure Security Center's built-in policies and definitions for your organization • Perform security assessments and implement Azure Security Center recommendations • Use incident response features to detect, investigate, and address threats • Create high-fidelity fusion alerts to focus attention on your most urgent security issues • Implement application whitelisting and just-in-time VM access • Monitor user behavior and access, and investigate compromised or misused credentials • Customize and perform operating system security baseline assessments • Leverage integrated threat intelligence to identify known bad actors

The approach used on a given spend item should largely depend on the balance between supply power and demand power. That is the logic behind the bestselling Purchasing Chessboard®, used by hundreds of corporations worldwide to reduce costs and increase value with suppliers. The 64 squares in the Purchasing Chessboard provide a rich reservoir of methods that can be applied either individually or combined. And because many of these methods are not customarily used by procurement, the Purchasing Chessboard is also the perfect tool for helping buyers to think and act outside the box and find new solutions. A well-proven concept that works across all industries and all categories in any given situation, it is little wonder that business leaders and procurement professionals alike are excited by, and enjoy strategizing around, the Purchasing Chessboard. This second edition of The Purchasing Chessboard addresses the new realities of a highly volatile economic environment and describes the many—sometimes surprising—ways in which the Purchasing Chessboard is being used in today's business world. Yet despite all of the great achievements of procurement executives and their teams, they do not always receive the recognition they deserve. In response, the authors have developed and outlined within the book an unequivocal approach to measure procurement's impact on a company's performance—Return on Supply Management Assets (ROSMA®).

Studies in Sociology, Organizations and Strategy at the Crossroads

Enterprise Cybersecurity

UTM Security with Fortinet

Enduring Questions in a Time of Rising Powers, Rogue Regimes, and Terrorism

Shaping the Future of Your Enterprise

Concepts, Principles, and Practices

Technology Strategy

Know how to mitigate and handle ransomware attacks via the essential cybersecurity training in this book so you can stop attacks before they happen. Learn the types of ransomware, distribution methods, internal structure, families (variants), defense strategies, recovery methods, and legal issues related to reporting ransomware incidents to authorities and other affected parties. This book also teaches you how to develop a ransomware incident response plan to minimize ransomware damage and recover normal operations quickly. Ransomware is a category of malware that can encrypt your computer and mobile device files until you pay a ransom to unlock them. Ransomware attacks are considered the most prevalent cybersecurity threats today—the number of new ransomware variants has grown 30-fold since 2015 and they currently account for roughly 40% of all spam messages. Attacks have increased in occurrence from one every 40 seconds to one every 14 seconds. Government and private corporations are targets. Despite the security controls set by organizations to protect their digital assets, ransomware is still dominating the world of security and will continue to do so in the future. Ransomware Revealed discusses the steps to follow if a ransomware infection occurs, such as how to pay the ransom through anonymous payment methods, perform a backup and restore your affected files, and search online to find a decryption tool to unlock (decrypt) your files for free. Mitigation steps are discussed in depth for both endpoint devices and network systems. What You Will Learn Be aware of how ransomware infects your system Comprehend ransomware components in simple terms Recognize the different types of ransomware familiesIdentify the attack vectors employed by ransomware to infect computer systemsKnow how to prevent ransomware attacks from successfully comprising your system and network (i.e., mitigation strategies) Know what to do if a successful ransomware infection takes place Understand how to pay the ransom as well as the pros and cons of paying Set up a ransomware response plan to recover from such attacks Who This Book Is For Those who do not specialize in the cybersecurity field (but have adequate IT skills) and want to fully understand the anatomy of ransomware threats. Although most of the book's content will be understood by ordinary computer users, it will also prove useful for experienced IT users aiming to understand the ins and outs of ransomware threats without diving deep into the technical jargon of the internal structure of ransomware.

An American bioengineering research firm erects a theme park on a Caribbean island, complete with living dinosaurs, and invites a group of scientists to be its first terrified guests.

With the rise of science, we moderns believe, the world changed irrevocably, separating us forever from our primitive, premodern ancestors. But if we were to let go of this fond conviction, Bruno Latour asks, what would the world look like? His book, an anthropology of science, shows us how much of modernity is actually a matter of faith. What does it mean to be modern? What difference does the scientific method make? The difference, Latour explains, is in our careful distinctions between nature and society, between human and thing, distinctions that our benighted ancestors, in their world of alchemy, astrology, and phrenology, never made. But alongside this purifying practice that defines modernity, there exists another seemingly contrary one: the construction of systems that mix politics, science, technology, and nature. The ozone debate is such a hybrid, in Latour ' s analysis, as are global warming, deforestation, even the idea of black holes. As these hybrids proliferate, the prospect of keeping nature and culture in their separate mental chambers becomes overwhelming—and rather than try, Latour suggests, we should rethink our distinctions, rethink the definition and constitution of modernity itself. His book offers a new explanation of science that finally recognizes the connections between nature and culture—and so, between our culture and others, past and present. Nothing short of a reworking of our mental landscape. We Have Never Been Modern blurs the boundaries among science, the humanities, and the social sciences to enhance understanding on all sides. A summation of the work of one of the most influential and provocative interpreters of science, it aims at saving what is good and valuable in modernity and replacing the rest with a broader, fairer, and finer sense of possibility.

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

Managerial Perspectives on Intelligent Big Data Analytics

Network Security

Defending Against Digital Extortion

A Strategic Guide to the Network Economy