Read Book Gartner S Magic Quadrant For Endpoint Protection Platforms

As recognized, adventure as competently as experience approximately lesson, amusement, as skillfully as arrangement can be gotten by just checking out a ebook **Gartner S Magic Quadrant For Endpoint Protection Platforms** afterward it is not directly done, you could assume even more roughly this life, concerning the world.

We give you this proper as skillfully as easy showing off to acquire those all. We have the funds for Gartner S Magic Quadrant For Endpoint Protection Platforms and numerous books collections from fictions to scientific research in any way. in the midst of them is this Gartner S Magic Quadrant For Endpoint Protection Platforms that can be your partner.

KEY=MAGIC - WIGGINS DOMINIK

Building an Effective Security Program for Distributed Energy Resources and Systems

John Wiley & Sons Building an Effective Security Program for Distributed Energy Resources and Systems Build a critical and effective security program for DERs Building an Effective Security Program for Distributed Energy Resources and Systems requires a unified approach to establishing a critical security program for DER systems and Smart Grid applications. The methodology provided integrates systems security engineering principles, techniques, standards, and best practices. This publication introduces engineers on the design, implementation, and maintenance of a security program for distributed energy resources (DERs), smart grid, and industrial control systems. It provides security professionals with understanding the specific requirements of industrial control systems and real-time constrained applications for power systems. This book: Describes the cybersecurity needs for DERs and power grid as critical infrastructure Introduces the information security principles to assess and manage the security and privacy risks of the emerging Smart Grid technologies Outlines the functions of the security program as well as the scope and differences between traditional IT system security requirements and those required for industrial control systems such as SCADA systems Offers a full array of resources— cybersecurity concepts, frameworks, and emerging trends Security Professionals and Engineers can use Building an Effective Security Program for Distributed Energy Resources and Systems as a reliable resource that is dedicated to the essential topic of security for distributed energy resources and power grids. They will find standards, guidelines, and recommendations from standards organizations, such as ISO, IEC, NIST, IEEE, ENISA, ISA, ISACA, and ISF, conveniently included for reference within chapters.

The Nano Age of Digital Immunity Infrastructure Fundamentals and Applications

The Intelligent Cyber Shield for Smart Cities

CRC Press Present anti-virus technologies do not have the symmetrical weaponry to defeat massive DDoS attacks on smart cities. Smart cities require a new set of holistic and AI-centric cognitive technology, such as autonomic components that replicate the human immune system, and a smart grid that connects all IoT devices. The book introduces Digital Immunity and covers the human immune system, massive distributed attacks (DDoS) and the future generations cyber attacks, the anatomy and critical success factors of smart city, Digital Immunity and the role of the Smart Grid, how Digital Immunity defends the smart city and annihilates massive malware, and Digital Immunity to combat global cyber terrorism.

Scaling Your Startup

Mastering the Four Stages from Idea to $10 Billion

Apress Know how your company can accelerate growth by not only tapping into new growth vectors, but also by adapting its organization, culture, and processes. To oversee growth from an idea to a company with billions in revenue, CEOs must reinvent many aspects of their company in anticipation of it reaching ever-higher revenues. Author Peter Cohan takes you through the four stages of scaling: winning the first customers, building a scalable business model, sprinting to liquidity, and running the marathon. What You'll LearnDiscover how founders keep their CEO positions by managing the organizational change needed to reach the next stage of scalingRead case studies that illustrate how CEOs craft growth strategies, raise capital, create culture, build their organizations, set goals, and manage processes to achieve themDiscover principles of successful scaling through comparisons of successful and less successful companies Use the Scaling Quotient to assess your startup's readiness to growFollow a road map for turning your idea into a company that can change the world Who This Book Is For Entrepreneurs, aspiring CEOs, capital providers, and all other key stakeholders

Secure Knowledge Management In The Artificial Intelligence Era

9th International Conference, SKM 2021, San Antonio, TX, USA, October 8–9, 2021, Proceedings

Springer Nature This book constitutes the refereed proceedings of the 9th International Conference On Secure Knowledge Management In Artificial Intelligence Era, SKM 2021, held in San Antonio, TX, USA, in 2021. Due to the COVID-19 pandemic the conference was held online. The 11 papers presented were carefully reviewed and selected from 30 submissions. They were organized according to the following topical sections: intrusion and malware detection; secure knowledge management; deep learning for security; web and social network.

CSO

The business to business trade publication for information and physical Security professionals.

Start-Up Secure

Baking Cybersecurity into Your Company from Founding to Exit

John Wiley & Sons Add cybersecurity to your value proposition and protect your company from cyberattacks Cybersecurity is now a requirement for every company in the world regardless of size or industry. Start-Up Secure: Baking Cybersecurity into Your Company from Founding to Exit covers everything a founder, entrepreneur and venture capitalist should know when building a secure company in today’s world. It takes you step-by-step through the cybersecurity moves you need to make at every stage, from landing your first round of funding through to a successful exit. The book describes how to include security and privacy from the start and build a cyber resilient company. You'll learn the basic cybersecurity concepts every founder needs to know, and you'll see how baking in security drives the value proposition for your startup’s target market. This book will also show you how to scale

cybersecurity within your organization, even if you aren't an expert! Cybersecurity as a whole can be overwhelming for startup founders. Start-Up Secure breaks down the essentials so you can determine what is right for your start-up and your customers. You'll learn techniques, tools, and strategies that will ensure data security for yourself, your customers, your funders, and your employees. Pick and choose the suggestions that make the most sense for your situation—based on the solid information in this book. Get primed on the basic cybersecurity concepts every founder needs to know Learn how to use cybersecurity know-how to add to your value proposition Ensure that your company stays secure through all its phases, and scale cybersecurity wisely as your business grows Make a clean and successful exit with the peace of mind that comes with knowing your company's data is fully secure Start-Up Secure is the go-to source on cybersecurity for start-up entrepreneurs, leaders, and individual contributors who need to select the right frameworks and standards at every phase of the entrepreneurial journey.

Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM

IGI Global With the continued progression of technologies such as mobile computing and the internet of things (IoT), cybersecurity has swiftly risen to a prominent field of global interest. This has led to cyberattacks and cybercrime becoming much more sophisticated to a point where cybersecurity can no longer be the exclusive responsibility of an organization's information technology (IT) unit. Cyber warfare is becoming a national issue and causing various governments to reevaluate the current defense strategies they have in place. Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM provides emerging research exploring the practical aspects of reassessing current cybersecurity measures within organizations and international governments and improving upon them using audit and awareness training models, specifically the Cybersecurity Audit Model (CSAM) and the Cybersecurity Awareness Training Model (CATRAM). The book presents multi-case studies on the development and validation of these models and frameworks and analyzes their implementation and ability to sustain and audit national cybersecurity strategies. Featuring coverage on a broad range of topics such as forensic analysis, digital evidence, and incident management, this book is ideally designed for researchers, developers, policymakers, government officials, strategists, security professionals, educators, security analysts, auditors, and students seeking current research on developing training models within cybersecurity management and awareness.

CSO

The business to business trade publication for information and physical Security professionals.

Hidden Champions in CEE and Turkey

Carving Out a Global Niche

Springer Science & Business Media This book presents hidden champions in Central and Eastern Europe (CEE) and Turkey that have been studied as a joint project between CEEMAN and IEDC-Bled School of Management, Slovenia. This is an outcome of extensive research undertaken by over 30 researchers and covers 15 countries from Russia to Albania; covering many contexts, political systems, cultures and infrastructures. The reader is provided with a detailed introduction to the concept of hidden champions and describes the cases studied in this project. This book is an invaluable resource providing a culmination of interdisciplinary, cross-study chapters ranging from leadership to performance drivers; from organization to culture and governance; from innovativeness to sustainability and further to the financial aspects of hidden champions business models. These meta level chapters are followed by 15 country-specific chapters which provide an overview of each country's history, economic indicators and vignettes of the cases involved in this study.

Open Research Problems in Network Security

IFIP WG 11.4 International Workshop, iNetSec 2010, Sofia, Bulgaria, March 5-6, 2010, Revised Selected Papers

Springer This book constitutes the refereed post-conference proceedings of the IFIP WG 11.4 International Workshop, iNetSec 2010, held in Sofia, Bulgaria, in March 2010. The 14 revised full papers presented together with an invited talk were carefully reviewed and selected during two rounds of refereeing. The papers are organized in topical sections on scheduling, adversaries, protecting resources, secure processes, and security for clouds.

The Challenge of BRIC Multinationals

Emerald Group Publishing This PIBR volume examines a number of idiosyncratic elements in the internationalization strategies of BRIC MNEs and, in particular, in their relationship with home country policies.

Russian Cyber Operations

Coding the Boundaries of Conflict

Georgetown University Press Russia has deployed cyber operations while maintaining a veneer of deniability and avoiding direct acts of war. In Russian Cyber Operations, Scott Jasper dives into the legal and technical maneuvers of Russian cyber strategies, proposing nations develop solutions for resilience to withstand attacks.

CSO

The business to business trade publication for information and physical Security professionals.

Modern Cybersecurity Strategies for Enterprises

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

(English Edition)

BPB Publications 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

Predictive Analytics in Human Resource Management

A Hands-on Approach

Taylor & Francis This volume is a step-by-step guide to implementing predictive data analytics in human resource management (HRM). It demonstrates how to apply and predict various HR outcomes which have an organisational impact, to aid in strategising and better decision-making. The book: Presents key concepts and expands on the need and role of HR analytics in business management. Utilises popular analytical tools like artificial neural networks (ANNs) and K-nearest neighbour (KNN) to provide practical demonstrations through R scripts for predicting turnover and applicant screening. Discusses real-world corporate examples and employee data collected first-hand by the authors. Includes individual chapter exercises and case studies for students and teachers. Comprehensive and accessible, this guide will be useful for students, teachers, and researchers of data analytics, Big Data, human resource management, statistics, and economics. It will also be of interest to readers interested in learning more about statistics or programming.

CSO

The business to business trade publication for information and physical Security professionals.

Integrating a Usable Security Protocol into User Authentication Services Design Process

CRC Press There is an intrinsic conflict between creating secure systems and usable systems. But usability and security can be made synergistic by providing requirements and design tools with specific usable security principles earlier in the requirements and design phase. In certain situations, it is possible to increase usability and security by revisiting design decisions made in the past; in others, to align security and usability by changing the regulatory environment in which the computers operate. This book addresses creation of a usable security protocol for user authentication as a natural outcome of the requirements and design phase of the authentication method development life cycle.

Security and Privacy in Communication Networks

17th EAI International Conference, SecureComm 2021, Virtual Event, September 6–9, 2021, Proceedings, Part I

Springer Nature This two-volume set LNICST 398 and 399 constitutes the post-conference proceedings of the 17th International Conference on Security and Privacy in Communication Networks, SecureComm 2021, held in September 2021. Due to COVID-19 pandemic the conference was held virtually. The 56 full papers were carefully reviewed and selected from 143 submissions. The papers focus on the latest scientific research results in security and privacy in wired, mobile, hybrid and ad hoc networks, in IoT technologies, in cyber-physical systems, in next-generation communication systems in web and systems security and in pervasive and ubiquitous computing.

The Economist

Computer Security Handbook, Set

John Wiley & Sons Computer security touches every part of our daily lives from our computers and connected devices to the wireless signals around us. Breaches have real and immediate financial, privacy, and safety consequences. This handbook has compiled advice from top professionals working in the real world about how to minimize the possibility of computer security breaches in your systems. Written for professionals and college students, it provides comprehensive best guidance about how to minimize hacking, fraud, human error, the effects of natural disasters, and more. This essential and highly-regarded reference maintains timeless lessons and is fully revised and updated with current information on security issues for social networks, cloud computing, virtualization, and more.

Principles and Applications of Business Intelligence Research

IGI Global "This book provides the latest ideas and research on advancing the understanding and implementation of business intelligence within organizations"--Provided by publisher.

Evidence-Based Cybersecurity

Foundations, Research, and Practice

CRC Press The prevalence of cyber-dependent crimes and illegal activities that can only be performed using a computer, computer networks, or other forms of information communication technology has significantly increased during the last two decades in the USA and worldwide. As a result, cybersecurity scholars and practitioners have developed various tools and policies to reduce individuals' and organizations' risk of experiencing cyber-dependent crimes. However, although cybersecurity research and tools production efforts have increased substantially, very little attention has been devoted to identifying potential comprehensive interventions that consider both human and technical aspects of the local ecology within which these crimes emerge and persist. Moreover, it appears that rigorous scientific assessments of these technologies and policies "in the wild" have been dismissed in the process of encouraging innovation and marketing. Consequently, governmental organizations, public, and private companies allocate a considerable portion of their operations budgets to protecting their computer and internet infrastructures without understanding the effectiveness of various tools and policies in reducing the myriad of risks they face. Unfortunately, this practice may complicate organizational workflows and increase costs for government entities, businesses, and consumers. The success of the evidence-based approach in improving performance in a wide range of professions (for example, medicine, policing, and education) leads us to believe that an evidence-based cybersecurity approach is critical for improving cybersecurity efforts. This book seeks to explain the foundation of the evidence-based cybersecurity approach, review its relevance in the context of existing security tools and policies, and provide concrete examples of how adopting this approach could improve cybersecurity operations and guide policymakers' decision-making process. The evidence-based cybersecurity approach explained aims to support security professionals', policymakers', and individual computer users' decision-making regarding the deployment of security policies and tools by calling for rigorous scientific investigations of the effectiveness of these policies and mechanisms in achieving their goals to protect critical assets. This book illustrates how this approach provides an ideal framework for conceptualizing an interdisciplinary problem like cybersecurity because it stresses moving beyond decision-makers' political, financial, social, and personal experience backgrounds when adopting cybersecurity tools and policies. This approach is also a model in which policy decisions are made based on scientific research findings.

Official (ISC)2 Guide to the ISSAP CBK

CRC Press Candidates for the CISSP-ISSAP professional certification need to not only demonstrate a thorough understanding of the six domains of the ISSAP CBK, but also need to have the ability to apply this in-depth knowledge to develop a detailed security architecture. Supplying an authoritative review of the key concepts and requirements of the ISSAP CBK, the Official (ISC)2® Guide to the ISSAP® CBK®, Second Edition provides the practical understanding required to implement the latest security protocols to improve productivity, profitability, security, and efficiency. Encompassing all of the knowledge elements needed to create secure architectures, the text covers the six domains: Access Control Systems and Methodology, Communications and Network Security, Cryptology, Security Architecture Analysis, BCP/DRP, and Physical Security Considerations. Newly Enhanced Design – This Guide Has It All! Only guide endorsed by (ISC)2 Most up-to-date CISSP-ISSAP CBK Evolving terminology and changing requirements for security professionals Practical examples that illustrate how to apply concepts in real-life situations Chapter outlines and objectives Review questions and answers References to free study resources Read It. Study It. Refer to It Often. Build your knowledge and improve your chance of achieving certification the first time around. Endorsed by (ISC)2 and compiled and reviewed by CISSP-ISSAPs and (ISC)2 members, this book provides unrivaled preparation for the certification exam and is a reference that will serve you well into your career. Earning your ISSAP is a deserving achievement that gives you a competitive advantage and makes you a member of an elite network of professionals worldwide.

Biologically Inspired Cognitive Architectures (BICA) for Young Scientists

Proceedings of the First International Early Research Career Enhancement School on BICA and Cybersecurity (FIERCES 2017)

Springer This book includes papers from the second year of the prestigious First International Early Research Career Enhancement School (FIERCES) series: a successful, new format that puts a school in direct connection with a conference and a social program, all dedicated to young scientists. Reflecting the friendly, social atmosphere of excitement and opportunity, the papers represent a good mixture of cutting-edge research focused on advances towards the most inspiring challenges of our time and first ambitious attempts at major challenges by as yet unknown, talented young scientists. In this second year of FIERCES, the BICA Challenge (to replicate all the essential aspects of the human mind in the digital environment) meets the Cybersecurity Challenge (to protect all the essential assets of the human mind in the digital environment), which is equally important in our age. As a result, the book fosters lively discussions on today’s hot topics in science and technology, and stimulates the emergence of new cross-disciplinary, cross-generation and cross-cultural collaboration. FIERCES 2017, or the First International Early Research Career Enhancement School on Biologically Inspired Cognitive Architectures and Cybersecurity, was held on August 1–5 at the Baltschug Kempinski in Moscow, Russia.

System Center 2012 Service Manager Unleashed

Sams Publishing This comprehensive resource will help you automate and optimize all facets of service management with System Center 2012 Service Manager. Expert consultants offer deep “in the trenches” insights for improving problem resolution, change control, release management, asset lifecycle management, chargeback, and more. You’ll learn how to implement high-value best practices from ITIL and the Microsoft Operations Framework. The authors begin with an expert overview of Service Manager, its evolution, and its new capabilities. Next, they walk through overall planning, design, implementation, and upgrades. Then, to help you focus your efforts, they present stepwise coverage of all topics in each feature area, linking technical information about Service Manager with essential knowledge about the technologies it depends on. Whatever your role in deploying or running Service Manager, this guide will help you deliver more responsive support at lower cost and drive more value from all your IT investments. • Leverage MOF and ITIL processes built into System Center 2012 Service Manager • Plan and design your Service Manager deployment • Install Service Manager or upgrade from earlier versions • Efficiently administer work and configuration items • Use connectors to integrate with Active Directory, Exchange, and System Center components • Create service maps • Enable end user access through Service Manager’s self-service portal • Implement incident, problem, change, and release management • Utilize workflows to automate key support processes • Create service level agreements with calendars, metrics, and objectives • Provide quick access to a standardized catalog of services • Use notification to ensure that Service Manager items are promptly addressed • Secure Service Manager and its data warehouse/reporting platform • Perform maintenance, backup, and recovery • Manage Service Manager performance • Customize Service Manager

The New Normal in IT

How the Global Pandemic Changed Information Technology Forever

John Wiley & Sons Learn how IT leaders are adapting to the new reality of life during and after COVID-19 COVID-19 has caused fundamental shifts in attitudes around remote and office work. And in The New Normal in IT: How the Global Pandemic Changed Information Technology Forever, internationally renowned IT executive Gregory S. Smith explains how and why companies today are shedding corporate office locations and reducing office footprints. You'll learn about how companies realized the value of information technology and a distributed workforce and what that means for IT professionals going forward. The book offers insightful lessons regarding: How to best take advantage of remote collaboration and hybrid remote/office workforces How to implement updated risk mitigation strategies and disaster recovery planning and testing to shield your organization from worst case scenarios How today's CIOs and CTOs adapt their IT governance frameworks to meet new challenges, including cybersecurity risks The New Normal in IT is an indispensable resource for IT professionals, executives, graduate technology management students, and managers in any industry. It's also a must-read for anyone interested in the impact that COVID-19 had, and continues to have, on the information technology industry.

Computerworld

Learning Microsoft Endpoint Manager

Scott Duffey The first-ever book on Microsoft Endpoint Manager (MEM), written by Microsoft Program Manager Scott Duffey! Did you just land an IT job only to learn your new employer is using Microsoft Endpoint Manager (MEM) for device management? Perhaps you stretched the truth on your resume and suggested you knew it already? Maybe you are an old-hat, know-your-stuff device management pro for another MDM or PC management product but your company is now migrating? Whatever the case, this book will be your zero-to-hero ramp-up guide. Microsoft Endpoint Manager has rapidly become the tool of choice for IT professionals around the world for managing corporate and personal devices but the learning curve can be steep. This book can be used to fast-track your understanding of MEM by laying out the concepts, including examples and tips for the real world, along with guided lab exercises. Topics include: • Microsoft Endpoint Manager – What it is and how to use it • How to set up a MEM learning environment • Mobile Device Management (MDM) for iOS, macOS, Android, and Windows 10 devices with Microsoft Intune • Device enrollment concepts for Personal and Corporate devices including Windows Autopilot, Apple Automated Device Enrollment (ADE), and Google ZeroTouch • Endpoint Security configuration in MEM including device Compliance and Azure AD Conditional Access across Microsoft Intune, Configuration Manager, Azure AD, Microsoft Defender for Endpoint, and Office 365. • Deploying, protecting, and configuring mobile and desktop applications with Microsoft Intune.

Enterprise Cybersecurity

How to Build a Successful Cyberdefense Program Against Advanced Threats

Apress 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.

Microsoft Azure Security Center

Microsoft Press 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

Ransomware

Defending Against Digital Extortion

"O'Reilly Media, Inc." 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

The CISO's Next Frontier

AI, Post-Quantum Cryptography and Advanced Security Paradigms

Springer Nature This book provides an advanced understanding of cyber threats as well as the risks companies are facing. It includes a detailed analysis of many technologies and approaches important to decreasing, mitigating or remediating those threats and risks. Cyber security technologies discussed in this book are futuristic and current. Advanced security topics such as secure remote work, data security, network security, application and device security, cloud security, and cyber risk and privacy are presented in this book. At the end of every chapter, an evaluation of the topic from a CISO's perspective is provided. This book also addresses quantum computing, artificial intelligence and machine learning for cyber security The opening chapters describe the power and danger of quantum computing, proposing two solutions for protection from probable quantum computer attacks: the tactical enhancement of existing algorithms to make them quantum-resistant, and the strategic implementation of quantum-safe algorithms and cryptosystems. The following chapters make the case for using supervised and unsupervised AI/ML to develop predictive, prescriptive, cognitive and auto-reactive threat detection, mitigation, and remediation capabilities against advanced attacks perpetrated by sophisticated threat actors, APT and polymorphic/metamorphic malware. CISOs must be concerned about current on-going sophisticated cyber-attacks, and can address them with advanced security measures. The latter half of this book discusses some current sophisticated cyber-attacks and available protective measures enabled by the advancement of cybersecurity capabilities in various IT domains. Chapters 6-10 discuss secure remote work; chapters 11-17, advanced data security paradigms; chapters 18-28, Network Security; chapters 29-35, application and device security; chapters 36-39, Cloud security; and chapters 40-46 organizational cyber risk measurement and event probability. Security and IT engineers, administrators and developers, CIOs, CTOs, CISOs, and CFOs will want to purchase this book. Risk personnel, CROs, IT and Security Auditors as well as security researchers and journalists will also find this useful.

Microsoft System Center Endpoint Protection Cookbook

Packt Publishing Ltd Over 31 simple yet incredibly effective recipes for installing and managing System Center 2016 Endpoint Protection About This Book This is the most practical and up-to-date book covering important new features of System Center 2016 Endpoint protection Gain confidence in managing IT and protecting your server against malware and other threats Configure and automate reporting features and also prepare yourself for a simple and pain-free migration process Who This Book Is For If you are a System Administrator or Engineer using System Center 2016 Endpoint Protection, then this book is for you. You should have a good background with Microsoft products in general, although no knowledge of Endpoint Protection is required. What You Will Learn Explore the best practices for Endpoint Protection in System Center Configuration Manager Provision the Endpoint Protection Client in a Disk Image in Configuration Manager Get to know more about the Security Center Configure definition and engine client updates to be optimum for your bandwidth Make your application or server work with Endpoint Protection enabled Find out how to deal with typical issues that may occur with Endpoint Protection Know how to respond to infections that often occur In Detail System Center Configuration Manager is now used by over 70% of all the business in the world today and many have taken advantage engaging the System Center Endpoint Protection within that great product. Through this book, you will gain knowledge about System Center Endpoint Protection, and see how to work with it from System Center Configuration Manager from an objective perspective. We'll show you several tips, tricks, and recipes to not only help you understand and resolve your daily challenges, but hopefully enhance the security level of your business. Different scenarios will be covered, such as planning and setting up Endpoint Protection, daily operations and maintenance tips, configuring Endpoint Protection for different servers and applications, as well as workstation computers. You'll also see how to deal with malware and infected systems that are discovered. You'll find out how perform OS deployment, Bitlocker, and Applocker, and discover what to do if there is an attack or outbreak. You'll find out how to ensure good control and reporting, and great defense against threats and malware software. You'll see the huge benefits when dealing with application deployments, and get to grips with OS deployments, software updates, and disk encryption such as Bitlocker. By the end, you will be fully aware of the benefits of the System Center 2016 Endpoint Protection anti-malware product, ready to ensure your business is watertight against any threat you could face. Style and approach Build robust SCEP and AV policies and discover the new potential of exciting new features of SCEP 2016.

Ransomware Revealed

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

Apress 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.

Penetration Testing

A Hands-On Introduction to Hacking

No Starch Press 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.

The Practice of Network Security Monitoring

Understanding Incident Detection and Response

No Starch Press 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.

Digital Economics

The Digital Transformation of Global Business

BoD – Books on Demand In the 2010s, new technological and business trends threaten, or promise, to disrupt multiple industries to such a degree that we might be moving into a new and fourth industrial revolution. The background and content of these new developments are laid out in the book from a holistic perspective. Based on an outline of the nature and developments of the market economy, business, global business industries and IT, the new technological and business trends are thoroughly dealt with, including issues such as internet, mobile, cloud, big data, internet of things, 3D-printing, the sharing economy, social media, gamification, and the way they transform industries and businesses

No Safe Harbor

The Inside Truth About Cybercrime—and How To Protect Your Business

Page Two "Stories of massive data breaches litter the 24-hour newsday headlines. Hackers and cybercrime syndicates are hitting a who's who of banks, retailers, law firms, and healthcare organizations: companies with sophisticated security systems designed to stop crime before it starts. They're also hitting companies that thought they were too small to matter. So how do cybercriminals continue to breach the defenses of the big companies--and why do they go after the small ones? And, most importantly, how can companies of all sizes protect themselves? Cybersecurity expert Mark Sangster deftly weaves together real-life cases in a thrilling narrative that illustrates the human complexities behind the scenes that can lead to companies throwing their digital front doors open to criminals. Within a security context, deep social engineering is the newest and biggest means of breaching our systems. Sangster shows readers that cybersecurity is not an IT problem to solve--it is a business risk to manage. Organizations need to shift the security discussion away from technology gates alone toward a focus on leadership, team behaviors, and mutual support. Sangster punctuates his eye-opening narratives with sets of questions businesspeople at all levels need to ask themselves, facts they need to know, and principles they need to follow to keep their companies secure."--

Applied Cyber Security and the Smart Grid

Implementing Security Controls into the Modern Power Infrastructure

Newnes Many people think of the Smart Grid as a power distribution group built on advanced smart metering—but that’s just one aspect of a much larger and more complex system. The "Smart Grid" requires new technologies throughout energy generation, transmission and distribution, and even the homes and businesses being served by the grid. This also represents new information paths between these new systems and services, all of which represents risk, requiring a more thorough approach to where and how cyber security controls are implemented. This insight provides a detailed architecture of the entire Smart Grid, with recommended cyber security measures for everything from the supply chain to the consumer. Discover the potential of the Smart Grid Learn in depth about its systems See its vulnerabilities and how best to protect it

BMC Control-M 7

A Journey from Traditional Batch Scheduling to Workload Automation

Packt Publishing Ltd Master one of the world?s most powerful enterprise workload automation tools? BMC Control-M 7 - using this book and eBook.