Byod Mobile Security Crowd Research Partners Pdf

Eventually, you will utterly discover a other experience and completion by spending more cash. nevertheless when? accomplish you put up with that you require to acquire those every needs taking into consideration having significantly cash? Why dont you try to acquire something basic in the beginning? Thats something that will lead you to understand even more re the globe, experience, some places, bearing in mind history, amusement, and a lot more?

It is your completely own epoch to feign reviewing habit. in the course of guides you could enjoy now is **Byod Mobile Security Crowd Research Partners Pdf** below.

Race Against the Machine - Erik Brynjolfsson 2012
Examines how information technologies are affecting jobs, skills, wages, and the economy.
Handbook on Innovations in Learning - Marilyn Murphy 2014
The Handbook on Innovations in Learning, developed by the Center on Innovations in Learning, presents commissioned chapters describing current best practices of instruction before embarking on descriptions of selected innovative practices which promise better methods of engaging and teaching students.
Social Media and Trust - Joanna Paliszkiewicz
Researchers and practitioners alike often overlook the vital relationship between trust and social media. ... Authors Joanna Paliszkiewicz and Alex Koohang charted a course to explore this abyss with a view to answering the question how does trust influence the use of social media. [i]Dr. John P. Girard, Peyton Anderson Endowed Chair in Information Technology, Middle Georgia State University[/i] The authors have done an excellent job in explaining how trust plays a significant role in social media. The book begins with a thorough overview of social media to its applications in learning, business, and an analysis of social media and trust. The second part of the book uses data from four different countries to answer multiple valid and vital research questions dealing with social media and trust, including an instrument that measures trust variables. This book presents some meaningful work on how the integration of social media and trust can best be developed. The authors apply their backgrounds in information technology, knowledge management, trust, and business to generate some provocative and instructive guidance to the readers on how to best leverage knowledge internally and externally to meet the organizational strategic goals. [i]Dr. Jay Liebowitz, Distinguished Chair of Applied Business and Finance, Harrisburg University of Science and Technology
CISO COMPASS - Todd Fitzgerald 2018-11-21
Todd Fitzgerald, co-author of the ground-breaking (ISC)2 CISO Leadership: Essential Principles for Success, Information Security Governance Simplified: From the Boardroom to the Keyboard, co-author for the E-C Council CISO Body of Knowledge, and contributor to many others including Official (ISC)2 Guide to the CISSP CBK, COBIT 5 for Information Security, and ISACA CSX Cybersecurity Fundamental Certification, is back with this new book incorporating practical experience in leading, building, and sustaining an information

security/cybersecurity program. CISO COMPASS includes personal, pragmatic perspectives and lessons learned of over 75 award-winning CISOs, security leaders, professional association leaders, and cybersecurity standard setters who have fought the tough battle. Todd has also, for the first time, adapted the McKinsey 7S framework (strategy, structure, systems, shared values, staff, skills and style) for organizational effectiveness to the practice of leading cybersecurity to structure the content to ensure comprehensive coverage by the CISO and security leaders to key issues impacting the delivery of the cybersecurity strategy and demonstrate to the Board of Directors due diligence. The insights will assist the security leader to create programs appreciated and supported by the organization, capable of industry/ peer award-winning recognition, enhance cybersecurity maturity, gain confidence by senior management, and avoid pitfalls. The book is a comprehensive, soup-to-nuts book enabling security leaders to effectively protect information assets and build award-winning programs by covering topics such as developing cybersecurity strategy, emerging trends and technologies, cybersecurity organization structure and reporting models, leveraging current incidents, security control frameworks, risk management, laws and regulations, data protection and privacy, meaningful policies and procedures, multi-generational workforce team dynamics, soft skills, and communicating with the Board of Directors and executive management. The book is valuable to current and future security leaders as a valuable resource and an integral part of any college program for information/ cybersecurity.

Registries for Evaluating Patient Outcomes - Agency for Healthcare Research and Quality/AHRQ 2014-04-01

This User's Guide is intended to support the design, implementation, analysis, interpretation, and quality evaluation of registries created to increase understanding of patient outcomes. For the purposes of this guide, a patient registry is an organized system that uses observational study methods to collect uniform data (clinical and other) to evaluate specified outcomes for a population defined by a particular disease, condition, or exposure, and that serves one or more predetermined scientific, clinical, or policy purposes. A registry database is a file (or files) derived from the registry. Although registries can serve many purposes, this guide focuses on registries created for one or more of the following purposes: to describe the natural history of disease, to determine clinical effectiveness or cost-effectiveness of health care products and services, to measure or monitor safety and harm, and/or to measure quality of care. Registries are classified according to how their populations are defined. For example, product registries include patients who have been exposed to biopharmaceutical products or medical devices. Health services registries consist of patients who have had a common procedure, clinical encounter, or hospitalization. Disease or condition registries are defined by patients having the same diagnosis, such as cystic fibrosis or heart failure. The User's Guide was created by researchers affiliated with AHRQ's Effective Health Care Program, particularly those who participated in AHRQ's DEcIDE (Developing Evidence to Inform Decisions About Effectiveness) program. Chapters were subject to multiple internal and external independent reviews.

Management Information Systems - Kenneth C. Laudon 2004

Management Information Systems provides comprehensive and integrative coverage of essential new technologies, information system applications, and their impact on business models and managerial decision-making in an exciting and interactive manner. The twelfth edition focuses on the major changes that have been made in information technology over the past two years, and includes new opening, closing, and Interactive Session cases.

Information Technology for Management - Efraim Turban 2013-01-14

This text is an unbound, binder-ready edition. Information Technology for Management by Turban, Volonino Over the years, this leading IT textbook had distinguished itself with an emphasis on illustrating the use of cutting edge business technologies for achieving managerial goals and objectives. The 9th ed continues this tradition with coverage of emerging trends in Mobile Computing and Commerce, IT virtualization, Social Media, Cloud Computing and the Management and Analysis of Big Data along with advances in more established areas of Information Technology. The book prepares students for professional careers in a rapidly changing and competitive environment by demonstrating the connection between IT concepts and practice more clearly than any other textbook on the market today. Each chapter contains numerous case studies and real world examples illustrating how businesses increase productivity, improve efficiency, enhance communication and collaboration, and gain competitive advantages through the use of Information Technologies.

Transforming Education - Unesco 2011

Surviving the Rise of Cybercrime - Craig McDonald 2016-12-23

This guide aims to provide a non-technical insight into cybersecurity for time-poor executives who arenew to the threats emerging in this space.In less than 60 minutes, readers will gain an understanding of cybersecurityand what it means for their organizations, tohighlight some real-world examples, and tomake them familiar with some industry jargonand terminology.

Tribe of Hackers Red Team - Marcus J. Carey 2019-08-13

Want Red Team offensive advice from the biggest cybersecurity names in the industry? Join our tribe. The Tribe of Hackers team is back with a new guide packed with insights from dozens of the world's leading Red Team security specialists. With their deep knowledge of system vulnerabilities and innovative solutions for correcting security flaws, Red Team hackers are in high demand. Tribe of Hackers Red Team: Tribal Knowledge from the Best in Offensive Cybersecurity takes the valuable lessons and popular interview format from the original Tribe of Hackers and dives deeper into the world of Red Team security with expert perspectives on issues like penetration testing and ethical hacking. This unique guide includes inspiring interviews from influential security specialists, including David Kennedy, Rob Fuller, Jayson E. Street, and Georgia Weidman, who share their real-world learnings on everything from Red Team tools and tactics to careers and communication, presentation strategies, legal concerns, and more Learn what it takes to secure a Red Team job and to stand out from other candidates Discover how to hone your hacking skills while staying on the right side of the law Get tips for collaborating on documentation and reporting Explore ways to garner support from leadership on your security proposals Identify the most important control to prevent compromising your network Uncover the latest tools for Red Team offensive security Whether you're new to Red Team security, an experienced practitioner, or ready to lead your own team, Tribe of Hackers Red Team has the real-world advice and practical guidance you need to advance your information security career and ready yourself for the Red Team offensive.

Epic Failures in Devsecops - Aubrey Stearn 2018-11-06

We learn more from failures than we do from successes. When something goes as expected, we use that process as a mental template for future projects. Success actually stunts the learning process because we think we have established a successful pattern, even after just one instance of success. It is a flawed confirmation that

"This is the correct way to do it," which has a tendency to morph into "This is the only way to do it."Real learning comes through crisis.If something goes wrong, horribly wrong, we have to scramble, experiment, hack, scream and taze our way through the process. Our minds flail for new ideas, are more willing to experiment, are more open to external input when we're in crisis mode.The Genesis of an IdeaThat's where the idea for this book came from. When I was in Singapore for DevSecOps Days 2018. Edwin Kwan, Stefan Streichsbier and DJ Schleen were swapping war stories over a couple of beers.The conclusion of their evening of telling tales was the desire to find a way to get those stories out to the community. They spoke with me about putting together a team of authors who would tell their own stories in the hope of helping the DevSecOps Community understand that failure is an option.Yes. You read that right. Failure is an option.Failure is part of the process of making the cultural and technological transformation that needs to happen in order to keep innovating. It is part of the journey to DevSecOps. The stories presented here aren't a roadmap. What they do is acknowledge failure as a part of the knowledge base of the DevSecOps Community.The days of stand-alone security teams isolated from the real process of development are coming to an end. Paraphrasing Caroline Wong, "Security needs to be invited to the party, not perceived as a goon standing at the front door denying admission." With DevSecOps, security is now part of the team.After reading these stories, we hope you will realize you are not alone in your journey. Not only are you not alone, there are early adopters who have gone before you, not exactly "hacking a trail through the swamp,"but at least marking the booby traps, putting flags next to the quick-sandpits and holding up a 'Dragons be here' sign at perilous cave openings

IoT Security Issues - Alasdair Gilchrist 2017

IoT Security Issues looks at the burgeoning growth of devices of all kinds controlled over the Internet of all varieties, where product comes first and security second. In this case, security trails badly. This book examines the issues surrounding these problems, vulnerabilities, what can be done to solve the problem, investigating the stack for the roots of the problems and how programming and attention to good security practice can combat the problems today that are a result of lax security processes on the Internet of Things. This book is for people interested in understanding the vulnerabilities on the Internet of Things, such as programmers who have not yet been focusing on the IoT, security professionals and a wide array of interested hackers and makers. This book assumes little experience or knowledge of the Internet of Things. To fully appreciate the book, limited programming background would be helpful for some of the chapters later in the book, though the basic content is explained. The author, Alasdair Gilchrist, has spent 25 years as a company director in the fields of IT, Data Communications, Mobile Telecoms and latterly Cloud/SDN/NFV technologies, as a professional technician, support manager, network and security architect. He has project-managed both agile SDLC software development as well as technical network architecture design. He has experience in the deployment and integration of systems in enterprise, cloud, fixed/mobile telecoms, and service provider networks. He is therefore knowledgeable in a wide range of technologies and has written a number of books in related fields.

CEH V10 - Ip Specialist 2018-09-24

CEH v10 covers new modules for the security of IoT devices, vulnerability analysis, focus on emerging attack vectors on the cloud, artificial intelligence, and machine learning including a complete malware analysis process. Added 150+ Exam Practice Questions to help you in the exam & Free Resources

Handbook of Research on Machine and Deep Learning Applications for Cyber Security - Ganapathi, Padmavathi 2019-07-26

As the advancement of technology continues, cyber security continues to play a significant role in today s world. With society becoming more dependent on the internet, new opportunities for virtual attacks can lead to the exposure of critical information. Machine and deep learning techniques to prevent this exposure of information are being applied to address mounting concerns in computer security. The Handbook of Research on Machine and Deep Learning Applications for Cyber Security is a pivotal reference source that provides vital research on the application of machine learning techniques for network security research. While highlighting topics such as web security, malware detection, and secure information sharing, this publication explores recent research findings in the area of electronic security as well as challenges and countermeasures in cyber security research. It is ideally designed for software engineers, IT specialists, cybersecurity analysts, industrial experts, academicians, researchers, and post-graduate students.

Trends and Challenges in Digital Business Innovation - Vincenzo Morabito 2014-02-04

This book describes the trends in digital innovation that are of most importance for businesses and explores the key challenges. The book is in three parts, the first of which focuses on developments in digital systems. Here, the ever-growing relevance of big data, cloud computing, and mobile services for business is discussed, and detailed consideration is given to the importance of social listening for understanding user behavior and needs and the implications of IT consumerization. In the second part, trends in digital management are examined, with chapters devoted to work practice, digital business identity as well as branding and governance. The final part of the book presents and reviews case studies of digital innovation at the global level that provide a benchmark of best practices, with inclusion of instructive fact sheets. While the book offers academic coverage of the digital transformation of business organizations and the associated challenges, it also describes concrete, real-world issues in clear, easy-to-understand language and will serve as a toolbox for managers that can be readily consulted. The text is supported by informative illustrations and tables, and practitioners will also benefit from the reported case studies and highlighted insights and recommendations.

The Flipped Classroom - Carl Reidsema 2017-02-27

Teaching and learning within higher education continues to evolve with innovative and new practices such as flipped teaching. This book contributes to the literature by developing a much deeper understanding of the complex phenomenon of flipped classroom approaches within higher education. It also serves as a practical guide to implementing flipped classroom teaching in academic practice across different higher educational institutions and disciplines. Part 1 of this book (Practice) describes the considerations involved in flipped classroom teaching, including the challenges faced in transforming teaching and learning within higher education. Further, it reviews the educational concepts on which the flipped classroom is based, including a selected history of similar innovations in the past. The final sections of Part 1 explore the tools needed for flipping, the design steps, assessment methods and the role of reflective practice within flipped teaching environments. “p>Part 2 of the book (Practices) provides a range of case studies from higher educational institutions in different countries and disciplines to demonstrate the many shapes and sizes of flipped classrooms. Many of the challenges, such as engaging students in their own learning and shifting them from spectators in the learning process to active participants, prove to be universal.

It's Complicated - Danah Boyd 2014-02-25

Surveys the online social habits of American teens and analyzes the role technology and social media plays in their lives, examining common misconceptions about such topics as identity, privacy, danger, and bullying.

IBM MobileFirst Strategy Software Approach - Tony Duong 2014-05-08

IBM® MobileFirst enables an enterprise to support a mobile strategy. With this end-to-end solution, IBM makes it possible for an enterprise to benefit from mobile interactions with customers, with business partners, and in organizations. There are products available from the IBM MobileFirst solution to support management, security, analytics, and development of the application and data platforms in a mobile environment. This IBM Redbooks® publication explores four areas crucial to developing a mobile strategy: Application development Mobile quality management Mobile device management Mobile analytics Each area is addressed in two parts. The first part contains information about the architectural considerations of each technology, and the second part provides prescriptive guidance. This IBM Redbooks publication provides an in-depth look at IBM Worklight®, IBM Rational® Test Workbench, IBM Endpoint Manager for Mobile Devices, and IBM Tealeaf® CX Mobile. This book is of interest to architects looking to design mobile enterprise solutions, and to practitioners looking to build these solutions. Related blog post 5 Things To Know About IBM MobileFirst

Information Security Governance - S.H. Solms 2008-12-16

IT Security governance is becoming an increasingly important issue for all levels of a company. IT systems are continuously exposed to a wide range of threats, which can result in huge risks that threaten to compromise the confidentiality, integrity, and availability of information. This book will be of use to those studying information security, as well as those in industry.

ICT Policy, Research, and Innovation - Svetlana Klessova 2020-12-10

A comprehensive discussion of the findings of the PICASSO initiative on ICT policy ICT Policy, Research, and Innovation: Perspectives and Prospects for EU-US Collaboration provides a clearly readable overview of selected information and communication technology (ICT) and policy topics. Rather than deluge the reader with technical details, the distinguished authors provide just enough technical background to make sense of the underlying policy discussions. The book covers policy, research, and innovation topics on technologies as wide-ranging as: Internet of Things Cyber physical systems 5G Big data ICT Policy, Research, and Innovation compares and contrasts the policy approaches taken by the EU and the US in a variety of areas. The potential for future cooperation is outlined as well. Later chapters provide policy perspectives about some major issues affecting EU/US development cooperation, while the book closes with a discussion of how the development of these new technologies is changing our conceptions of fundamental aspects of society.

Challenges in Cybersecurity and Privacy - Jorge Bernal Bernabe 2019

This book introduces several cybersecurity and privacy research challenges and how they are being addressed in the scope of 15 European research projects.Each chapter is dedicated to a different funded European Research project, which aims to cope with digital security and privacy aspects, risks, threats and cybersecurity issues.

Security+ Guide to Network Security Fundamentals - Mark Ciampa 2012-07-27

Reflecting the latest trends and developments from the information security field, best-selling Security+ Guide to Network Security Fundamentals, Fourth Edition, provides a complete introduction to practical network and computer security and maps to the CompTIA Security+ SY0-301 Certification Exam. The text covers the fundamentals of network security, including compliance and operational security; threats and vulnerabilities;

application, data, and host security; access control and identity management; and cryptography. The updated edition includes new topics, such as psychological approaches to social engineering attacks, Web application attacks, penetration testing, data loss prevention, cloud computing security, and application programming development security. The new edition features activities that link to the Information Security Community Site, which offers video lectures, podcats, discussion boards, additional hands-on activities and more to provide a wealth of resources and up-to-the minute information. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Hacking Exposed Mobile - Neil Bergman 2013-08-05

Proven security tactics for today's mobile apps, devices, and networks "A great overview of the new threats created by mobile devices. ...The authors have heaps of experience in the topics and bring that to every chapter." -- Slashdot Hacking Exposed Mobile continues in the great tradition of the Hacking Exposed series, arming business leaders and technology practitioners with an in-depth understanding of the latest attacks and countermeasures--so they can leverage the power of mobile platforms while ensuring that security risks are contained." -- Jamil Farshchi, Senior Business Leader of Strategic Planning and Initiatives, VISA Identify and evade key threats across the expanding mobile risk landscape. Hacking Exposed Mobile: Security Secrets & Solutions covers the wide range of attacks to your mobile deployment alongside ready-to-use countermeasures. Find out how attackers compromise networks and devices, attack mobile services, and subvert mobile apps. Learn how to encrypt mobile data, fortify mobile platforms, and eradicate malware. This cutting-edge guide reveals secure mobile development guidelines, how to leverage mobile OS features and MDM to isolate apps and data, and the techniques the pros use to secure mobile payment systems. Tour the mobile risk ecosystem with expert guides to both attack and defense Learn how cellular network attacks compromise devices over-the-air See the latest Android and iOS attacks in action, and learn how to stop them Delve into mobile malware at the code level to understand how to write resilient apps Defend against server-side mobile attacks, including SQL and XML injection Discover mobile web attacks, including abuse of custom URI schemes and JavaScript bridges Develop stronger mobile authentication routines using OAuth and SAML Get comprehensive mobile app development security guidance covering everything from threat modeling to iOS- and Android-specific tips Get started quickly using our mobile pen testing and consumer security checklists

Growth Poles of the Global Economy: Emergence, Changes and Future Perspectives - Elena G. Popkova 2019-08-03

The book presents the best contributions from the international scientific conference “Growth Poles of the Global Economy: Emergence, Changes and Future,” which was organized by the Institute of Scientific Communications (Volgograd, Russia) together with the universities of Kyrgyzstan and various other cities in Russia. The 143 papers selected, focus on spatial and sectorial structures of the modern global economy according to the theory of growth poles. It is intended for representatives of the academic community: university and college staff developing study guides on socio-humanitarian disciplines in connection with the theory of growth poles, researchers, and undergraduates, masters, and postgraduates who are interested in the recent inventions and developments in the field. It is also a valuable resource for expert practitioners managing entrepreneurial structures in the existing and prospective growth poles of the global economy as well as those at international institutes that regulate growth poles. The first part of the book investigates the factors and conditions affecting the emergence of the growth poles of the modern global economy. The second part then

discusses transformation processes in the traditional growth poles of the global economy under the influence of the technological progress. The third part examines how social factors affect the formation of new growth poles of the modern global economy. Lastly, the fourth part offers perspectives on the future growth of the global economy on the basis of the digital economy and Industry 4.0.

The Oxford Handbook of Mobile Communication and Society - Rich Ling 2020-04-22

Mobile communication has dramatically changed over the past decade with the diffusion of smartphones. Unlike the basic 2G mobile phones, which "merely" facilitated communication between individuals on the move, smartphones allow individuals to communicate, to entertain and inform themselves, to transact, to navigate, to take photos, and countless other things. Mobile communication has thus transformed society by allowing new forms of coordination, communication, consumption, social interaction, and access to news/entertainment. All of this is regardless of the space in which users are immersed. Set in the context of the developed and the developing world, The Oxford Handbook of Mobile Communication and Society updates current scholarship surrounding mobile media and communication. The 43 chapters in this handbook examine mobile communication and its evolving impact on individuals, institutions, groups, societies, and businesses. Contributors examine the communal benefits, social consequences, theoretical perspectives, organizational potential, and future consequences of mobile communication. Topics covered include, among many other things, trends in the Global South, location-based services, and the "appification" of mobile communication and society.

MSSP Playbook - Charles Henson 2020-04-03

Charles Henson, managing partner of Nashville Computer, the premiere cyber security and IT service firm in Music City, offers advice in this book on how MSPs can protect their clients from ransom ware, data theft, and other malicious acts by hackers.The unfortunate truth is some MSPs' credentials and backend access are available today for sale on the dark web. Small business owners can't afford systems to protect themselves and their clients that cost hundreds of thousands of dollars. That's why MSSP Playbook is vital. It will walk you through what Charles' company has done, as well as how he's worked with other MSPs in building out a security stack. You'll learn how to vet those essential security vendors, what dangers to look out for, and how to eliminate the need to hire a six-figure security engineer and instead find a strategic partner who has already hired, trained and staffed the Security Operations Center (SOC).

Formulating Research Methods for Information Systems - Chris Sauer 2014-01-14

This edited two-volume collection presents the most interesting and compelling articles pertaining to the formulation of research methods used to study information systems from the 30-year publication history of the Journal of Information Technology .

The Cyber Risk Handbook - Domenic Antonucci 2017-05-01

Actionable guidance and expert perspective for real-world cybersecurity The Cyber Risk Handbook is the practitioner's guide to implementing, measuring and improving the counter-cyber capabilities of the modern enterprise. The first resource of its kind, this book provides authoritative guidance for real-world situations, and cross-functional solutions for enterprise-wide improvement. Beginning with an overview of counter-cyber evolution, the discussion quickly turns practical with design and implementation guidance for the range of capabilities expected of a robust cyber risk management system that is integrated with the enterprise risk management (ERM) system. Expert contributors from around the globe weigh in on specialized topics with

tools and techniques to help any type or size of organization create a robust system tailored to its needs. Chapter summaries of required capabilities are aggregated to provide a new cyber risk maturity model used to benchmark capabilities and to road-map gap-improvement. Cyber risk is a fast-growing enterprise risk, not just an IT risk. Yet seldom is guidance provided as to what this means. This book is the first to tackle in detail those enterprise-wide capabilities expected by Board, CEO and Internal Audit, of the diverse executive management functions that need to team up with the Information Security function in order to provide integrated solutions. Learn how cyber risk management can be integrated to better protect your enterprise Design and benchmark new and improved practical counter-cyber capabilities Examine planning and implementation approaches, models, methods, and more Adopt a new cyber risk maturity model tailored to your enterprise needs The need to manage cyber risk across the enterprise—inclusive of the IT operations—is a growing concern as massive data breaches make the news on an alarmingly frequent basis. With a cyber risk management system now a business-necessary requirement, practitioners need to assess the effectiveness of their current system, and measure its gap-improvement over time in response to a dynamic and fast-moving threat landscape. The Cyber Risk Handbook brings the world's best thinking to bear on aligning that system to the enterprise and vice-a-versa. Every functional head of any organization must have a copy at-hand to understand their role in achieving that alignment.

Computer Security Handbook - Seymour Bosworth 2014-03-31

Information and Technology Literacy: Concepts, Methodologies, Tools, and Applications - Management Association, Information Resources 2017-08-30

People currently live in a digital age in which technology is now a ubiquitous part of society. It has become imperative to develop and maintain a comprehensive understanding of emerging innovations and technologies. Information and Technology Literacy: Concepts, Methodologies, Tools, and Applications is an authoritative reference source for the latest scholarly research on techniques, trends, and opportunities within the areas of digital literacy. Highlighting a wide range of topics and concepts such as social media, professional development, and educational applications, this multi-volume book is ideally designed for academics, technology developers, researchers, students, practitioners, and professionals interested in the importance of understanding technological innovations.

Securing DevOps - Julien Vehent 2018-08-20

Summary Securing DevOps explores how the techniques of DevOps and security should be applied together to make cloud services safer. This introductory book reviews the latest practices used in securing web applications and their infrastructure and teaches you techniques to integrate security directly into your product. You'll also learn the core concepts of DevOps, such as continuous integration, continuous delivery, and infrastructure as a service. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology An application running in the cloud can benefit from incredible efficiencies, but they come with unique security threats too. A DevOps team's highest priority is understanding those risks and hardening the system against them. About the Book Securing DevOps teaches you the essential techniques to secure your cloud services. Using compelling case studies, it shows you how to build security into automated testing, continuous delivery, and other core DevOps processes. This experience-rich book is filled with mission-critical strategies to protect web applications against attacks, deter fraud

attempts, and make your services safer when operating at scale. You'll also learn to identify, assess, and secure the unique vulnerabilities posed by cloud deployments and automation tools commonly used in modern infrastructures. What's inside An approach to continuous security Implementing test-driven security in DevOps Security techniques for cloud services Watching for fraud and responding to incidents Security testing and risk assessment About the Reader Readers should be comfortable with Linux and standard DevOps practices like CI, CD, and unit testing. About the Author Julien Vehent is a security architect and DevOps advocate. He leads the Firefox Operations Security team at Mozilla, and is responsible for the security of Firefox's high-traffic cloud services and public websites. Table of Contents Securing DevOps PART 1 - Case study: applying layers of security to a simple DevOps pipeline Building a barebones DevOps pipeline Security layer 1: protecting web applications Security layer 2: protecting cloud infrastructures Security layer 3: securing communications Security layer 4: securing the delivery pipeline PART 2 - Watching for anomalies and protecting services against attacks Collecting and storing logs Analyzing logs for fraud and attacks Detecting intrusions The Caribbean breach: a case study in incident response PART 3 - Maturing DevOps security Assessing risks Testing security Continuous security

Enterprise Class Mobile Application Development - Leigh Williamson 2015-11-19

Build and Deploy Mobile Business Apps That Smoothly Integrate with Enterprise IT For today’s enterprises, mobile apps can have a truly transformational impact. However, to maximize their value, you can’t build them in isolation. Your new mobile apps must reflect the revolutionary mobile paradigm and delight today’s mobile users--but they must also integrate smoothly with existing systems and leverage previous generations of IT investment. In this guide, a team of IBM’s leading experts show how to meet all these goals. Drawing on extensive experience with pioneering enterprise clients, they cover every facet of planning, building, integrating, and deploying mobile apps in large-scale production environments. You’ll find proven advice and best practices for architecture, cloud integration, security, user experience, coding, testing, and much more. Each chapter can stand alone to help you solve specific real-world problems. Together, they help you establish a flow of DevOps activities and lifecycle processes fully optimized for enterprise mobility.

Privileged Attack Vectors - Morey J. Haber 2020-06-13

See how privileges, insecure passwords, administrative rights, and remote access can be combined as an attack vector to breach any organization. Cyber attacks continue to increase in volume and sophistication. It is not a matter of if, but when, your organization will be breached. Threat actors target the path of least resistance: users and their privileges. In decades past, an entire enterprise might be sufficiently managed through just a handful of credentials. Today’s environmental complexity has seen an explosion of privileged credentials for many different account types such as domain and local administrators, operating systems (Windows, Unix, Linux, macOS, etc.), directory services, databases, applications, cloud instances, networking hardware, Internet of Things (IoT), social media, and so many more. When unmanaged, these privileged credentials pose a significant threat from external hackers and insider threats. We are experiencing an expanding universe of privileged accounts almost everywhere. There is no one solution or strategy to provide the protection you need against all vectors and stages of an attack. And while some new and innovative products will help protect against or detect against a privilege attack, they are not guaranteed to stop 100% of malicious activity. The volume and frequency of privilege-based attacks continues to increase and test the limits of existing security controls and solution implementations. Privileged Attack Vectors details the risks associated with poor

privilege management, the techniques that threat actors leverage, and the defensive measures that organizations should adopt to protect against an incident, protect against lateral movement, and improve the ability to detect malicious activity due to the inappropriate usage of privileged credentials. This revised and expanded second edition covers new attack vectors, has updated definitions for privileged access management (PAM), new strategies for defense, tested empirical steps for a successful implementation, and includes new disciplines for least privilege endpoint management and privileged remote access. What You Will Learn Know how identities, accounts, credentials, passwords, and exploits can be leveraged to escalate privileges during an attack Implement defensive and monitoring strategies to mitigate privilege threats and risk Understand a 10-step universal privilege management implementation plan to guide you through a successful privilege access management journeyDevelop a comprehensive model for documenting risk, compliance, and reporting based on privilege session activity Who This Book Is For Security management professionals, new security professionals, and auditors looking to understand and solve privilege access management problems

Negotiating Control - Keri K. Stephens 2018-07-23

The fast-food worker finds refuge in a bathroom stall to respond to her boyfriend's fifth message in an hour. The human resources manager sees a colleague sending a stream of text messages during a meeting and quickly grabs her mobile to make sure she's also multitasking. These scenarios are common, but unique to the 21st century. Until the early 2000s, workplaces provided most of the computers and portable devices that employees used to perform their jobs and communicate with others. Today, people bring their own mobile devices to work and create new norms for how communication occurs in the workplace. Managers and organizations respond by setting and enforcing new policies that are intended to help them navigate the ever-changing mobile-communication environment. In Negotiating Control: Organizations and Mobile Communication, Keri K. Stephens responds to the struggles of employees, organizations, and even friends and family, as they try to understand new norms for connectedness in the workplace. Drawing on over two decades of her own research and fieldwork, , representing people in over 35 different types of jobs, Stephens claims that though people assume mobile communication is a uniform practice, there are underlying -- and often hidden -- issues of control and power at play, which shape how people are permitted and expected to use mobiles to communicate while working. The accounts Stephens offers reveal the many ways that these portable tools are actually used across work environments today, integrating information, communication, and data, and connecting people in expected and often conflicting ways.

Hard Choices - Hillary Rodham Clinton 2014-06-10

Hillary Rodham Clinton’s inside account of the crises, choices, and challenges she faced during her four years as America’s 67th Secretary of State, and how those experiences drive her view of the future. “All of us face hard choices in our lives,” Hillary Rodham Clinton writes at the start of this personal chronicle of years at the center of world events. “Life is about making such choices. Our choices and how we handle them shape the people we become.” In the aftermath of her 2008 presidential run, she expected to return to representing New York in the United States Senate. To her surprise, her former rival for the Democratic Party nomination, newly elected President Barack Obama, asked her to serve in his administration as Secretary of State. This memoir is the story of the four extraordinary and historic years that followed, and the hard choices that she and her colleagues confronted. Secretary Clinton and President Obama had to decide how to repair fractured alliances, wind down two wars, and address a global financial crisis. They faced a rising competitor in China, growing

threats from Iran and North Korea, and revolutions across the Middle East. Along the way, they grappled with some of the toughest dilemmas of US foreign policy, especially the decision to send Americans into harm's way, from Afghanistan to Libya to the hunt for Osama bin Laden. By the end of her tenure, Secretary Clinton had visited 112 countries, traveled nearly one million miles, and gained a truly global perspective on many of the major trends reshaping the landscape of the twenty-first century, from economic inequality to climate change to revolutions in energy, communications, and health. Drawing on conversations with numerous leaders and experts, Secretary Clinton offers her views on what it will take for the United States to compete and thrive in an interdependent world. She makes a passionate case for human rights and the full participation in society of women, youth, and LGBT people. An astute eyewitness to decades of social change, she distinguishes the trendlines from the headlines and describes the progress occurring throughout the world, day after day. Secretary Clinton's descriptions of diplomatic conversations at the highest levels offer readers a master class in international relations, as does her analysis of how we can best use "smart power" to deliver security and prosperity in a rapidly changing world—one in which America remains the indispensable nation.

Zero Trust Networks - Evan Gilman 2017-06-19

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

Corporate Security Management - Marko Cabric 2015-03-30

Corporate Security Management provides practical advice on efficiently and effectively protecting an organization's processes, tangible and intangible assets, and people. The book merges business and security perspectives to help transform this often conflicted relationship into a successful and sustainable partnership. It combines security doctrine, business priorities, and best practices to uniquely answer the Who, What, Where, Why, When and How of corporate security. Corporate Security Management explores the diverse structures of security organizations in different industries. It shows the crucial corporate security competencies needed and demonstrates how they blend with the competencies of the entire organization. This book shows how to identify, understand, evaluate and anticipate the specific risks that threaten enterprises and how to design successful protection strategies against them. It guides readers in developing a systematic approach to assessing, analyzing, planning, quantifying, administrating, and measuring the security function. Addresses the often opposing objectives between the security department and the rest of the business concerning risk, protection, outsourcing, and more Shows security managers how to develop business acumen in a corporate security environment Analyzes the management and communication skills needed for the corporate security manager Focuses on simplicity, logic and creativity instead of security technology Shows the true challenges of

performing security in a profit-oriented environment, suggesting ways to successfully overcome them Illustrates the numerous security approaches and requirements in a wide variety of industries Includes case studies, glossary, chapter objectives, discussion questions and exercises

SQL Injection Attacks and Defense - Justin Clarke 2012-06-18

What is SQL injection? -- Testing for SQL injection -- Reviewing code for SQL injection -- Exploiting SQL injection -- Blind SQL injection exploitation -- Exploiting the operating system -- Advanced topics -- Code-level defenses -- Platform level defenses -- Confirming and recovering from SQL injection attacks -- References.

Computer Security: Principles and Practice - Stallings William 2008-09

Building Products for the Enterprise - Blair Reeves 2018-03-09

If you're new to software product management or just want to learn more about it, there's plenty of advice available—but most of it is geared toward consumer products. Creating high-quality software for the enterprise involves a much different set of challenges. In this practical book, two expert product managers provide straightforward guidance for people looking to join the thriving enterprise market. Authors Blair Reeves and Benjamin Gaines explain critical differences between enterprise and consumer products, and deliver strategies for overcoming challenges when building for the enterprise. You'll learn how to cultivate knowledge of your organization, the products you build, and the industry you serve. Explore why: Identifying customer vs user problems is an enterprise project manager's main challenge Effective collaboration requires in-depth knowledge of the organization Analyzing data is key to understanding why users buy and retain your product Having experience in the industry you're building products for is valuable Product longevity depends on knowing where the industry isheaded