Gartner Magic Quadrant Application Security Testing

Proceedings of International Conference on Smart Computing and Cyber Security
A Cross-Industry View
Network Security
Digital Business
Application Level Security Management
Practical Cloud Security
ECCWS2016-Proceedings fo the 15th European Conference on Cyber Warfare and Security "
Cloud Computing Basics
How to Monetize, Manage, and Measure Information as an Asset for Competitive Advantage
Advanced Solutions in Diagnostics and Fault Tolerant Control
Security and Privacy in Communication Networks
Computer Security Handbook, Set
Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM
Cutting-Edge Guidance from the World's Leading Experts
13th International Joint Conference, ICETE 2016, Lisbon, Portugal, July 26-28, 2016, Revised Selected Papers
UTM Security with Fortinet
An IT Service Management Approach
How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security
Strategic Foresight, Security Challenges and Innovation (SMARTCYBER 2020)
First International Conference, TrustBus 2004, Zaragoza, Spain, August 30-September 1, 2004, Proceedings
How to Not Screw Up Your Organization's Security
Mastering FortiOS
Trends in Software Testing
Applications and Techniques in Information Security
Cases and Tools
Machine Learning Techniques and Analytics for Cloud Security

Overview of patent out-licencing opportunities
Mobile Platform Security
Research Directions in Data and Applications Security
Infonomics
A Guide to Using Best Practices and Standards
AI in Healthcare
6th International Conference, ATIS 2015, Beijing, China, November 4-6, 2015, Proceedings
Digital Economics
Research Anthology on Business Aspects of Cybersecurity
Intelligent Security Systems
Computer Security in the 21st Century
E-Business and Telecommunications
Trust and Privacy in Digital Business

Gartner Magic Quadrant Application Security Testing

ERIN SINGH

Proceedings of International Conference on Smart Computing and Cyber Security
CRC Press
Across industries, firms vary broadly on how they operate with respect to their Research & Development (R&D) activities. This volume presents a holistic approach to evaluating the critical elements of R&D management, including planning, organization, portfolio management, project management, and knowledge transfer—by assessing R&D management from different sectors. Featuring empirical research and in-depth case studies from industries as diverse as medical imaging, electric vehicles, and cyber security, the authors identify common features of successful R&D management, despite fundamental differences, such as company size, number of employees, industry sector, and the R&D budget. In particular, they consider the implications for decision making with respect to resource allocation and investments, such as site selection, purchasing, and cross-departmental communication.

A Cross-Industry View John Wiley & Sons
Most organizations have been caught off-guard with the proliferation of smart devices. The IT organization was comfortable supporting the Blackberry due to its ease of implementation and maintenance. But the use of Android and iOS smart devices have created a maintenance nightmare not only for the IT organization but for the IT auditors as well. This book will serve as a guide to IT and Audit professionals on how to manage, secure and audit smart device. It provides

guidance on the handling of corporate devices and the Bring Your Own Devices (BYOD) smart devices.

Network Security Pearson Education

This book constitutes the refereed proceedings of the International Conference on Applications and Techniques in Information Security, ATIS 2015, held in Beijing, China, in November 2015. The 25 revised full papers and 10 short papers presented were carefully reviewed and selected from 103 submissions. The papers are organized in topical sections on invited speeches; cryptograph; evaluation, standards and protocols; trust computing and privacy protection; cloud security and applications; tools and methodologies; system design and implementations.

Digital Business River Publishers

Recently, mobile security has garnered considerable interest in both the research community and industry due to the popularity of smartphones. The current smartphone platforms are open systems that allow application development, also for malicious parties. To protect the mobile device, its user, and other mobile ecosystem stakeholders such as network operators, application execution is controlled by a platform security architecture. This book explores how such mobile platform security architectures work. We present a generic model for mobile platform security architectures: the model illustrates commonly used security mechanisms and techniques in mobile devices and allows a systematic comparison of different platforms. We analyze several mobile platforms using the model. In addition, this book explains hardware-security mechanisms typically present in a mobile device. We also discuss enterprise security extensions for mobile platforms and survey recent research in the area of mobile platform security. The objective of this book is to provide a comprehensive overview of the current status of mobile platform security for students, researchers, and practitioners. Table of Contents: Preface / Introduction / Platform Security Model / Mobile Platforms / Platform Comparison / Mobile Hardware Security / Enterprise Security Extensions / Platform Security Research / Conclusions / Bibliography / Authors' Biographies

Application Level Security Management Springer

As industries are rapidly being digitalized and information is being more heavily stored and transmitted online, the security of information has become a top priority in securing the use of online networks as a safe and effective platform. With the vast and diverse potential of artificial intelligence (AI) applications, it has become easier than ever to identify cyber vulnerabilities, potential threats, and the identification of solutions to these unique problems. The latest tools and technologies for AI applications have untapped potential that conventional systems and human security systems cannot meet, leading AI to be a frontrunner in the fight against malware, cyber-attacks, and various security issues. However, even with the tremendous progress AI has made within the sphere of security, it’s important to understand the impacts, implications, and critical issues and challenges of AI applications along with the many benefits and emerging trends in this essential field of security-based research. Research Anthology on Artificial Intelligence Applications in Security seeks to address the fundamental

advancements and technologies being used in AI applications for the security of digital data and information. The included chapters cover a wide range of topics related to AI in security stemming from the development and design of these applications, the latest tools and technologies, as well as the utilization of AI and what challenges and impacts have been discovered along the way. This resource work is a critical exploration of the latest research on security and an overview of how AI has impacted the field and will continue to advance as an essential tool for security, safety, and privacy online. This book is ideally intended for cyber security analysts, computer engineers, IT specialists, practitioners, stakeholders, researchers, academicians, and students interested in AI applications in the realm of security research.

Practical Cloud Security Springer Nature

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.

ECCWS2016-Proceedings fo the 15th European Conference on Cyber Warfare and Security " John Wiley & Sons

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

Cloud Computing Basics "O'Reilly Media, Inc."

This book highlights the latest achievements concerning the theory, methods and practice of fault diagnostics, fault tolerant systems and cyber safety. When considering the diagnostics of industrial processes and systems, increasingly important safety issues cannot be ignored. In this context, diagnostics plays a crucial role as a primary measure of the improvement of the overall system safety integrity level. Obtaining the desired diagnostic coverage or providing an appropriate level of inviolability of the integrity of a system is now practically inconceivable without the use of fault detection and isolation methods. Given the breadth and depth of its coverage, the book will be of interest to researchers faced with the challenge of designing technical and medical diagnosis systems, as well as junior researchers and students in the fields of automatic control, robotics, computer science and artificial intelligence.

How to Monetize, Manage, and Measure Information as an Asset for Competitive Advantage Springer

Your guide to planning and executing a complete mobile web strategy Revisit your approach to the mobile web—and deliver effective solutions that reach customers and clients on a variety of mobile devices. In this practical guide, web development luminary Dino Esposito shows you how to develop a solid mobile strategy for the enterprise, starting with an effective mobile website. You'll receive essential architectural and implementation guidance, as well as mobile-specific design patterns for building cross-platform and native applications. Discover how to: Architect a website accessible from many different mobile devices Implement design patterns specific to mobile app development Examine tools that enable you to write one codebase for many platforms Use technologies for building Windows Phone, iPhone, and Android apps Develop cross-platform app features, such as localization and offline behavior

Advanced Solutions in Diagnostics and Fault Tolerant Control IGI Global

Cybersecurity is vital for all businesses, regardless of sector. With constant threats and potential online dangers, businesses must remain aware of the current research and information available to them in order to protect themselves and their employees. Maintaining tight cybersecurity can be difficult for businesses as there are so many moving parts to contend with, but remaining vigilant and having protective measures and training in place is essential for a successful company. The Research Anthology on Business Aspects of Cybersecurity considers all emerging aspects of cybersecurity in the business sector including frameworks, models, best practices, and emerging areas of interest. This comprehensive reference source is split into three sections with the first discussing audits and risk assessments that businesses can conduct to ensure the security of their systems. The second section covers training and awareness initiatives for staff that promotes a

security culture. The final section discusses software and systems that can be used to secure and manage cybersecurity threats. Covering topics such as audit models, security behavior, and insider threats, it is ideal for businesses, business professionals, managers, security analysts, IT specialists, executives, academicians, researchers, computer engineers, graduate students, and practitioners.

Security and Privacy in Communication Networks Larstan Publishing Inc.

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

Computer Security Handbook, Set diplom.de

Inhaltsangabe:Abstract: Today, more and more enterprises are developing business applications for Internet usage, which results in the exposure of their sensitive data not only to customers, and business partners but also to hackers. Because web applications provide the interface between users sitting somewhere within the World Wide Web and enterprises backend-resources, hackers can execute sophisticated attacks that are almost untraceable, aiming to steal, modify or delete enterprises vital data, even when it is protected by passwords or encryption. As recent viruses and worms such as Nimda, CodeRed or MSBlast have shown, modern attacks are occurring at the application itself, since this is where high-value information is most vulnerable. Such attack scenarios a becoming very problematic nowadays, since traditional network security products such as firewalls or network intrusion detection systems are completely blind to those malicious activities and therefore can not offer any protection at all. Modern protection mechanisms require more sophisticated detection capabilities in order to protect enterprises assets from such attacks now and in the future. Additionally web application security currently is a highly dynamic and also very emerging field within enterprises IT security activities. Therefore this diploma thesis aims to provide a strong focussed picture on the current state of web application security and its different possibilities to raise the overall security level of already implemented web applications and also of future web applications. Acting as a basis for further analysis, the currently most common web application vulnerabilities are described to get an overview of what a web application has to be protected of and where the root problems of these weaknesses are lying. Although these generic categories may not be applicable to every actually implemented web application, they may be used as baseline for future web applications. Armed with the background of the current vulnerabilities and their related root causes, a detailed analysis of currently available countermeasures will provide

recommendations that may be taken at each of the certain stages of a web application s lifecycle. Since all further decisions generally should be based upon risk evaluations of specifically considered systems, a possible risk management assessment methodology is provided within the thesis. Controls and countermeasures are provided from an […]

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

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

Cutting-Edge Guidance from the World's Leading Experts CRC Press

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

13th International Joint Conference, ICETE 2016, Lisbon, Portugal, July 26-28, 2016, Revised Selected Papers Newnes

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.

UTM Security with Fortinet EGBG Services LLC

This book is the culmination of literally more than thirty thousand hands on practical hours of log review, log assessment, enterprise-level packet capture forensics, live dynamic malware analysis, behavior malware root-cause triage analysis, use-case data analysis, and more, which have led to the remediation of nation state systemic malware infection droppers, command-and-control-compromised computers, exfiltration from targeted attackers and insider attacks, and more. This book will get you and your security operation center teams started in the correct direction instead of sitting around, pretending to do security, and not get fired by your bosses when they find out. This book will save your career and show you where your security manager or security peer lied to you about technology that they never understood. All this and more is at your fingertips. You can reinvigorate your career with security results that have been proven by my hands. Everyone in security operation center life is struggling to get into a role that is promising, and they are struggling to find a way up. Information Security is an expertise-driven field. This book and the others that will follow such as Consequence, Lies, Misconceptions, and Pains of Incompetent Security and Splunk Data Analysis Handbook and Cookbook for Everyone will invigorate your career and make you the envy of your peers. This may include your management, so be careful. Managers are scared of expertise. You will be in the driver's seat of data analysis, but first, you must walk through untying and unbinding all the broken premises and broken ideas that you have learned and relearned from year to year. You must unsubscribe to the bad notions that you take as commonplace watercooler talk. You need to do this now with this book. I will walk you through, step-by-step, to understand what is real security and what is fake security. This is where the rubber meets the road in breaking you free from the shackles of a silo-mentality or a silo-position. Too often crummy managers will leave you to rot in a security operations center with no growth and no hope to get out. This book is what you need to get your promotion somewhere else. Be the leader that you want to be. Be the discussion changer and not just the guy that nods and can never disagree or offer something fulfilling to a team. All the ideas contained in this book and the others come from results-proven security. This is not theory. This is technical, strategy guidance that is born from detecting the things that have put companies on the news, which have been hacked from exfiltration, insider attacks, nation-state botnet malware, ghost malware, network-level postcompromise, and so on. I have found them all using no alerts and no threat intelligence ever. This is the protection that you want.

An IT Service Management Approach EGBG Services LLC

This document brings together a set of latest data points and publicly available information relevant for Platforms & Applications Industry. We are very excited

to share this content and believe that readers will benefit from this periodic publication immensely.

How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security Springer

The statistics are staggering: security losses in the billions, unauthorized computer usage in 50 percent of businesses, $2 million spent per company on a single virus attack. The Black Book on Corporate Security offers a wide range of solutions to these challenging problems. Written by the brightest minds in the field, each of the essays in this book takes on a different aspect of corporate security. Individual chapters cover such topics as maintaining data safety, fighting online identity theft, managing and protecting intellectual property in a shared information environment, securing content, and much more. Written in clear, intelligible language, the book is designed around a “spy” motif that presents advanced information in a simple, entertaining format. Each spread features an “Insider Notes” sidebar, while the research conducted specifically for the book is displayed in easy-to-read charts accompanied by author analysis. Case studies, a glossary, and a resource index multiply the book’s utility.

Strategic Foresight, Security Challenges and Innovation (SMARTCYBER 2020) Springer

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.

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

This edited volume covers essential and recent development in the engineering and management of data centers. Data centers are complex systems requiring ongoing support, and their high value for keeping business continuity operations is crucial. The book presents core topics on the planning, design, implementation, operation and control, and sustainability of a data center from a didactical and practitioner viewpoint. Chapters include: · Foundations of data centers: Key Concepts and Taxonomies · ITSDM: A Methodology for IT Services Design · Managing Risks on Data Centers through Dashboards · Risk Analysis in Data Center Disaster Recovery Plans · Best practices in Data Center Management Case: KIO Networks · QoS in NaaS (Network as a Service) using Software Defined Networking · Optimization of Data Center Fault-Tolerance Design · Energetic Data Centre Design Considering Energy Efficiency Improvements During Operation · Demand-side Flexibility and Supply-side Management: The Use Case of Data Centers and Energy Utilities · DevOps: Foundations and its Utilization in Data Centers · Sustainable and Resilient Network Infrastructure Design for Cloud Data Centres · Application Software in

Cloud-Ready Data Centers This book bridges the gap between academia and the industry, offering essential reading for practitioners in data centers, researchers in the area, and faculty teaching related courses on data centers. The book can be used as a complementary text for traditional courses on Computer Networks, as well as innovative courses on IT Architecture, IT Service Management, IT Operations, and Data Centers.