
Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches

Getting the books Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches now is not type of inspiring means. You could not and no-one else going gone books gathering or library or borrowing from your contacts to entrance them. This is an very easy means to specifically acquire guide by on-line. This online message Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches can be one of the options to accompany you following having further time.

It will not waste your time. take on me, the e-book will unquestionably song you new matter to read. Just invest tiny times to retrieve this on-line publication Oracle Incident Response And Forensics Preparing For And Responding To Data Breaches as well as review them wherever you are now.



Organizational Auditing and Assurance in the Digital Age Apress
The definitive guide to incident response--updated for the first time in a decade! Thoroughly revised to cover the latest and most effective tools and techniques, Incident Response & Computer Forensics, Third Edition arms you with the information you need to get your organization out of trouble when data breaches occur. This practical resource covers the entire lifecycle of incident response, including preparation, data collection, data analysis, and remediation. Real-world case studies reveal the methods behind--and remediation

strategies for--today's most insidious attacks. Architect an infrastructure that allows for methodical investigation and remediation Develop leads, identify indicators of compromise, and determine incident scope Collect and preserve live data Perform forensic duplication Analyze data from networks, enterprise services, and applications Investigate Windows and Mac OS X systems Perform malware triage Write detailed incident response reports Create and implement comprehensive remediation plans
Data Breach Preparation and Response Elsevier

Data Breach Preparation and Response: Breaches are Certain, Impact is Not is the first book to provide 360 degree visibility and guidance on how to proactively prepare for and manage a data breach and limit impact. Data breaches are inevitable incidents that can disrupt business operations and carry severe reputational and financial impact, making them one of the largest risks facing organizations today. The effects of a breach can be felt across multiple departments within an organization, who will each play a role in effectively managing the breach. Kevvie Fowler has assembled a team of leading forensics, security, privacy, legal, public relations and cyber insurance experts to create the definitive breach management reference for the whole organization. Discusses the cyber criminals behind data breaches and the underground dark web forums they use to trade and sell stolen data Features never-before published techniques to qualify and discount a suspected breach or to verify and precisely scope a confirmed breach Helps identify your sensitive data, and the commonly overlooked data sets that, if stolen, can result in a

material breach Defines breach response plan requirements and describes how to develop a plan tailored for effectiveness within your organization Explains strategies for proactively self-detecting a breach and simplifying a response Covers critical first-responder steps and breach management practices, including containing a breach and getting the scope right, the first time Shows how to leverage threat intelligence to improve breach response and management effectiveness Offers guidance on how to manage internal and external breach communications,

restore trust, and resume business operations after a breach, including the critical steps after the breach to reduce breach-related litigation and regulatory fines Illustrates how to define your cyber-defensible position to improve data protection and demonstrate proper due diligence practices

Monitoring Internal Control Systems and IT CRC Press

Oracle Endeca Information Discovery Best Practices Maximize the powerful capabilities of this self-service enterprise data discovery platform. Master Competitive Analytics with Oracle Endeca Information Discovery reveals how to unlock insights from any type of data,

regardless of structure. The first part of the book is a complete technical guide to the product's architecture, components, and implementation. The second part presents a comprehensive collection of business analytics use cases in various industries, including financial services, healthcare, research, manufacturing, retail, consumer packaged goods, and public sector. Step-by-step instructions on implementing some of these use cases are included in this Oracle Press book. Install and manage Oracle Endeca Server Design Oracle Endeca Information Discovery Studio visualizations to facilitate user-driven data exploration and discovery Enable enterprise-driven data exploration with Oracle Endeca Information Discovery Integrator Develop and

implement a fraud detection and analysis application Build a healthcare correlation application that integrates claims, patient, and operations analysis; partners; clinical research; and remote monitoring Use an enterprise architecture approach to incrementally establish big data and analytical capabilities

Incident Response Cengage Learning
Cyberforensics is a fairly new word in the technology our industry, but one that nevertheless has immediately recognizable meaning. Although the word forensics may have its origins in formal debates using evidence, it is now most closely associated with investigation into evidence of crime. As the word cyber has become synonymous with the use of electronic technology, the word cyberforensics bears no mystery. It immediately conveys a serious and concentrated endeavor to identify the evidence of crimes or other attacks committed in cyberspace.

Nevertheless, the full implications of the word are less well understood. Cyberforensic activities remain a mystery to most people, even those fully immersed in the design and operation of cyber technology. This book sheds light on those activities in a way that is comprehensible not only to technology professionals but also to the technology hobbyist and those simply curious about the field. When I started contributing to the field of cybersecurity, it was an obscure field, rarely mentioned in the mainstream media. According to the FBI, by 2009 organized crime syndicates were making more money via cybercrime than in drug trafficking. In spite of the rise in cybercrime and the advance of sophisticated threat actors online, the cyber security profession continues to lag behind in its ability to investigate cybercrime and understand the root causes of cyber attacks. In the late 1990s I worked to respond to sophisticated attacks as part of the U. S.

Cybersecurity and Privacy in Cyber Physical Systems Oreilly & Associates Incorporated

Dissecting the dark side of the Internet with its infectious worms, botnets, rootkits, and Trojan horse programs (known as malware) is a treacherous condition for any forensic investigator or analyst. Written by information security experts with real-world investigative experience, *Malware Forensics Field Guide for Windows Systems* is a "tool" with checklists for specific tasks, case studies of difficult situations, and expert analyst tips. *A condensed hand-held guide complete with on-the-job tasks and checklists *Specific for Windows-based systems, the largest running OS in the world *Authors are world-renowned leaders in investigating and analyzing malicious code
Mastering Mobile Forensics Springer Nature
This timely text/reference presents a detailed

introduction to the essential aspects of computer network forensics. The book considers not only how to uncover information hidden in email messages, web pages and web servers, but also what this reveals about the functioning of the Internet and its core protocols. This, in turn, enables the identification of shortcomings and highlights where improvements can be made for a more secure network. Topics and features: provides learning objectives in every chapter, and review questions throughout the book to test understanding; introduces the basic concepts of network process models, network forensics frameworks and network forensics tools; discusses various techniques for the acquisition of packets in a network forensics system, network forensics analysis, and attribution in network forensics; examines a range of advanced topics, including botnet, smartphone, and cloud forensics; reviews a

number of freely available tools for performing forensic activities.

Hack Proofing Your E-commerce Web Site Apress

The field of digital forensics is rapidly evolving and continues to gain significance in both the law enforcement and the scientific community. Being intrinsically interdisciplinary, it draws upon a wide range of subject areas such as information & communication technologies, law, social sciences and business administration. With this in mind, the workshop on Digital Forensics and Incident Analysis (WDFIA) specifically addresses this multi-faceted aspect, with papers invited from the full spectrum of issues relating to digital forensics and incident analysis. This book represents the proceedings from the 2012 event, which was held in Crete, Greece. A total of 13 papers are included, spanning a range of topics including systems and network

investigation, services and applications and supporting the forensic process. All of the papers were subject to double-blind peer review, with each being reviewed by at least two members of the international programme committee.

The CISM Prep Guide Academic Conferences and publishing limited

From the authors of the bestselling Hack Proofing Your Network! Yahoo!, E-Bay, Amazon. Three of the most popular, well-established, and lavishly funded Web sites in existence, yet hackers managed to penetrate their security systems and cripple these and many other Web giants for almost 24 hours. E-Commerce giants, previously thought to be impenetrable are now being exposed as incredibly vulnerable. This book will give e-commerce architects and engineers insight into the tools and techniques used by hackers to compromise their sites. The security of e-

commerce sites is even more imperative than non-commerce sites, because the site has the added responsibility of maintaining the security of their customer's personal and financial information. Hack Proofing Your E-Commerce Site will provide computer architects and engineers all of the information they need to design and implement security measures. * Heightened media awareness of malicious attacks against "secure" sites guarantees a wide audience * Uses forensics-based analysis to give the reader insight to the mind of a hacker. This understanding is crucial for security professionals to defend against attacks

Network Security Assessment John Wiley & Sons

"Incident Response is a complete guide for organizations of all sizes and types who are addressing their computer security issues."--Jacket.

The CIO's Guide to Oracle Products and Solutions Athul Jayaram

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

Principles of Incident Response and Disaster Recovery ISACA

This book written by Cybersecurity expert Athul Jayaram shows you how to protect and secure your business from various kinds of attacks that you are

vulnerable to. It also highlight how important cybersecurity is to your business and case study of various attacks that have happened recently.

Protecting Oracle Database 12c Elsevier

This book covers a variety of topics that span from industry to academics: hybrid AI model for IDS in IoT, intelligent authentication framework for IoMT mobile devices for extracting bioelectrical signals, security audit in terms of vulnerability analysis to protect the electronic medical records in healthcare system using AI, classification using CNN a multi-face recognition attendance system with anti-spoofing capability, challenges in face morphing attack detection, a dimensionality reduction and feature-level fusion technique for morphing attack detection

(MAD) systems, findings and discussion on AI-assisted forensics, challenges and open issues in the application of AI in forensics, a terrorist computational model that uses Baum-Welch optimization to improve the intelligence and predictive accuracy of the activities of criminal elements, a novel method for detecting security violations in IDSs, graphical-based city block distance algorithm method for E-payment systems, image encryption, and AI methods in ransomware mitigation and detection. It assists the reader in exploring new research areas, wherein AI can be applied to offer solutions through the contribution from researchers and academia.

Migrating to the Cloud McGraw Hill
Professional
Migrating to the Cloud: Oracle

Client/Server Modernization is a reference guide for migrating client/server applications to the Oracle cloud. Organized into 14 chapters, the book offers tips on planning, determining effort and budget, designing the Oracle cloud infrastructure, implementing the migration, and moving the Oracle cloud environment into production. Aside from Oracle application and database cloud offerings, the book looks at various tools and technologies that can facilitate migration to the cloud. It includes useful code snippets and step-by-step instructions in database migration, along with four case studies that highlight service enablement of DOS-based applications, Sybase to Oracle, PowerBuilder to APEX, and Forms to Java EE. Finally, it considers current challenges and future trends in cloud computing and

client/server migration. This book will be useful to IT professionals, such as developers, architects, database administrators, IT project managers, and executives, in developing migration strategies and best practices, as well as finding appropriate solutions. Focuses on Oracle architecture, Middleware and COTS business applications Explains the tools and technologies necessary for your legacy migration Gives useful information about various strategies, migration methodologies and efficient plans for executing migration projects

Computerworld John Wiley & Sons
Take the right steps when a breach of your Oracle Database environment becomes known or suspected. You will learn techniques for discerning how an

attacker got in, what data they saw, and what else they might have done. This book helps you understand forensics in relation to Oracle Database, and the tools and techniques that should be used to investigate a database breach. You will learn the measures to put in place now to make it harder for an attack to be successful, and to aid in the detection and investigation of future attacks. You will know how to bring together tools and methods to create a holistic approach and investigation when an event occurs, helping you to be confident of your ability to react correctly and responsibly to threats against your organization's data. What You'll Learn
Detect when breaches have or may

have occurred React with confidence using an organized plan Determine whether a suspected breach is real Determine the scope of data that has been compromised Preserve evidence for possible criminal prosecutions Put in place measures to aid future investigations Who This Book is For Database administrators, system administrators, and other technology professionals who may be called upon to investigate breaches of security involving Oracle Database **OS X Incident Response** ISACA Auditing is constantly and quickly changing due to the continuous evolution of information and communication technologies. As the

auditing process is forced to adapt to these changes, issues have arisen that lead to a decrease in the auditing effectiveness and efficiency, leading to a greater dissatisfaction among users. More research is needed to provide effective management and mitigation of the risk associated to organizational transactions and to assign a more reliable and accurate character to the execution of business transactions and processes. Organizational Auditing and Assurance in the Digital Age is an essential reference source that discusses challenges, identifies opportunities, and presents solutions in relation to issues in auditing, information systems auditing, and assurance

services and provides best practices for ensuring accountability, accuracy, and transparency. Featuring research on topics such as forensic auditing, financial services, and corporate governance, this book is ideally designed for internal and external auditors, assurance providers, managers, risk managers, academicians, professionals, and students.

The Risk IT Framework IGI Global

How secure is your network? The best way to find out is to attack it, using the same tactics attackers employ to identify and exploit weaknesses. With the third edition of this practical book, you'll learn how to perform network-based penetration testing in a structured manner. Security expert Chris

McNab demonstrates common vulnerabilities, and the steps you can take to identify them in your environment. System complexity and attack surfaces continue to grow. This book provides a process to help you mitigate risks posed to your network. Each chapter includes a checklist summarizing attacker techniques, along with effective countermeasures you can use immediately. Learn how to effectively test system components, including: Common services such as SSH, FTP, Kerberos, SNMP, and LDAP Microsoft services, including NetBIOS, SMB, RPC, and RDP SMTP, POP3, and IMAP email services IPsec and PPTP services that provide secure network access TLS protocols and features providing transport security Web server software, including Microsoft IIS, Apache, and Nginx Frameworks including Rails, Django, Microsoft ASP.NET, and PHP Database servers, storage protocols, and distributed key-value stores

Springer

Oracle Incident Response and
ForensicsApress

Handbook of Information Security, Threats,
Vulnerabilities, Prevention, Detection, and
Management ISACA

* Prepares readers for the Certified Information Security Manager (CISM) exam, ISACA's new certification that launches in June 2003 * CISM is business-oriented and intended for the individual who must manage, design, oversee, and assess an enterprise's information security * Essential reading for those who are cramming for this new test and need an authoritative study guide * Many out-of-work IT professionals are seeking security management certification as a vehicle to re-employment * CD-ROM includes a Boson-powered test engine with all the questions and answers from the book

Illumination of Artificial Intelligence in Cybersecurity and Forensics

Lulu.com

The Handbook of Information Security is a definitive 3-volume handbook that offers coverage of both established and cutting-edge theories and developments on information and computer security.

The text contains 180 articles from over 200 leading experts, providing the benchmark resource for information security, network security, information privacy, and information warfare.

Master Competitive Analytics with
Oracle Endeca Information Discovery

McGraw Hill Professional

Develop the capacity to dig deeper into mobile device data acquisition About

This Book A mastering guide to help you mobile device forensics Acquire in-depth overcome the roadblocks you face when knowledge about smartphone dealing with mobile forensics Excel at acquisition and acquisition methods the art of extracting data, recovering Gain a solid understanding of the deleted data, bypassing screen locks, architecture of operating systems, file and much more Get best practices to formats, and mobile phone internal how to collect and analyze mobile memory Explore the topics of of mobile device data and accurately document security, data leak, and evidence your investigations Who This Book Is recovery Dive into advanced topics such For The book is for mobile forensics as GPS analysis, file carving, professionals who have experience in encryption, encoding, unpacking, and handling forensic tools and methods. decompiling mobile application processes In Detail Mobile forensics This book is designed for skilled digital forensic examiners, mobile forensic presents a real challenge to the forensic investigators, and law enforcement community due to the fast and officers. What You Will Learn unstoppable changes in technology. Understand the mobile forensics This book aims to provide the forensic process model and get guidelines on community an in-depth insight into

mobile forensic techniques when it comes to deal with recent smartphones operating systems Starting with a brief overview of forensic strategies and investigation procedures, you will understand the concepts of file carving, GPS analysis, and string analyzing. You will also see the difference between encryption, encoding, and hashing methods and get to grips with the fundamentals of reverse code engineering. Next, the book will walk you through the iOS, Android and Windows Phone architectures and filesystem, followed by showing you various forensic approaches and data gathering techniques. You will also explore advanced forensic techniques

and find out how to deal with third-applications using case studies. The book will help you master data acquisition on Windows Phone 8. By the end of this book, you will be acquainted with best practices and the different models used in mobile forensics. Style and approach The book is a comprehensive guide that will help the IT forensics community to go more in-depth into the investigation process and mobile devices take-over.