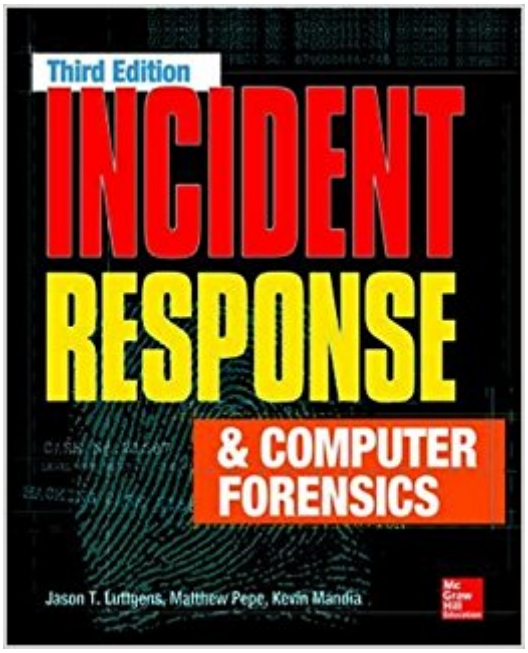
Incident Response & Computer Forensics, Third Edition (Networking & Comm - OMG)



Synopsis

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

Book Information

Series: Networking & Comm - OMG
Paperback: 624 pages
Publisher: McGraw-Hill Education; 3 edition (August 4, 2014)
Language: English
ISBN-10: 0071798684
ISBN-13: 978-0071798686
Product Dimensions: 7.8 x 1.2 x 9.3 inches
Shipping Weight: 2.3 pounds (View shipping rates and policies)
Average Customer Review: 4.4 out of 5 stars 22 customer reviews
Best Sellers Rank: #51,018 in Books (See Top 100 in Books) #31 inÂ Books > Computers & Technology > Security & Encryption > Privacy & Online Safety #32 inÂ Books > Computers & Technology > Networking & Cloud Computing > Networks, Protocols & APIs > Networks #60 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security

Customer Reviews

Jason T. Luttgens is a former technical director of the security consulting firm Mandiant where he led dozens of global investigations involving industrial espionage, cardholder data theft, and other crimes. A veteran of NASA and the U.S. Air Force, he served in the Office of Special Investigations and at the Department of Defense's Computer Forensics Laboratory. Matthew Pepe is a senior technical director and co-founder of Mandiant where he has led numerous investigations, serves as

a subject matter expert, and developed the forensic capabilities that are in use today. A veteran of the U.S. Air Force, he served in the Office of Special Investigations' Computer Forensics Laboratory. Kevin Mandia is senior vice president and chief operating officer of FireEye. He founded Mandiant in 2004 and served as the chief executive officer. While in the U.S. Air Force, Kevin served as a computer security officer at the Pentagon and as a special agent in the Air Force Office of Special Investigations.

I would like to add the following comments - I personally know two of the authors and the technical editor for over 15 years. I have edition one and two and recently purchased edition three.I not only recommend the read for security professionals - I recommend the read for CXOs of companies and senior management in the Federal, State, Local governments - and of course the Military.Their Real-World Incidents are exceptional - the Live Data Collection section (I would rate at 10 Star) -Spend sometime reading and understanding the Foreword section - written by Jamie, another expert in the area. He sets the tone for a valuable education trip.There are many lessons learned and good advice given. They also answered the "So What?" question throughout the book.Lastly in Chapter 18 they "set the Strategic Direction" - They list 10 recommendations - Follow them if you want to keep your system as safe as possible with today's technology.Kudos go to the authors and the people who supported them throughout their professional careers.

Bought for an IR class. Great read considering I'm supposed to be learning... :)

I love this book. It is probably the easiest to understand forensics book.

A "must-have" for the Information Security Engineer!

This book takes you through setup, organization, structure, where and how, case studies, plus provides rationale on why! Thumbs up!

The first 6 chapters are a bit repetitive, but after that's been seared into your memory it becomes a great guid. When you've finished it's nice to keep around for referencing.

Very well written and organized book. I throughly enjoyed reading this book (half way through)

This is an excellent book for all classes of incident responders. The concepts are easy to follow and it provides references to the appropriate tools for the job.

Incident Response & Computer Forensics, Third Edition (Networking & Comm - OMG) Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation (Networking & Comm - OMG) Beyond Initial Response--2Nd Edition: Using The National Incident Management System Incident Command System COMM (with COMM Online, 1 term (6 months) Printed Access Card) (New, Engaging Titles from 4LTR Press) Incident Log: Large Notebook Template For Businesses (Accident & Incident Record Log Book) The Far Time Incident (The Incident Series Book 1) Computer Forensics: Investigating File and Operating Systems, Wireless Networks, and Storage (CHFI), 2nd Edition (Computer Hacking Forensic Investigator) IT Auditing Using Controls to Protect Information Assets, 2nd Edition (Networking & Communication - OMG) The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics The Practice of Network Security Monitoring: Understanding Incident Detection and Response Principles of Incident Response and Disaster Recovery Cisco CCNA Networking For Beginners : The Ultimate Guide To Become A Cisco Certified Network Associate! - Learn Cisco CCNA Networking In Now Time! Data Communications and Networking (McGraw-Hill Forouzan Networking) Third Eye: Third Eye Activation Mastery, Easy And Simple Guide To Activating Your Third Eye Within 24 Hours (Third Eye Awakening, Pineal Gland Activation, Opening the Third Eye) Computer Forensics: Investigating Network Intrusions and Cybercrime (CHFI), 2nd Edition 1st Grade Computer Basics : The Computer and Its Parts: Computers for Kids First Grade (Children's Computer Hardware Books) CISA Certified Information Systems Auditor All-in-One Exam Guide, Third Edition (Certification & Career - OMG) A Practical Guide to SysML, Third Edition: The Systems Modeling Language (The MK/OMG Press) Host Response to Biomaterials: The Impact of Host Response on Biomaterial Selection Computer Forensics