Incident Response & Computer Forensics, Third Edition

DOWNLOAD EBOOK
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

Paperback: 624 pages
Publisher: McGraw-Hill Education; 3 edition (August 4, 2014)
Language: English
ISBN-10: 0071798684
Product Dimensions: 7.4 x 1.4 x 9.1 inches
Shipping Weight: 2.3 pounds (View shipping rates and policies)
Average Customer Review: 4.5 out of 5 stars
(See all reviews (17 customer reviews))

Customer Reviews

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.

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

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.

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.

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

Great read on IR topic. Finding lots of valuable content

good book. highly recommend :)

Great read, very informative.

Download to continue reading...


Dmca