The Practice of Network Security Monitoring: Understanding Incident Detection and Response

Richard Bejtlich

The Practice of Network Security Monitoring: Understanding Incident Detection and Response

Richard Bejtlich

The Practice of Network Security Monitoring: Understanding Incident Detection and Response
Richard Bejtlich

Network security is not simply about building impenetrable walls — determined attackers *will* eventually overcome traditional defenses. The most effective computer security strategies integrate network security monitoring (NSM): the collection and analysis of data to help you detect and respond to intrusions.

In *The Practice of Network Security Monitoring*, Mandiant CSO Richard Bejtlich shows you how to use NSM to add a robust layer of protection around your networks — no prior experience required. To help you avoid costly and inflexible solutions, he teaches you how to deploy, build, and run an NSM operation using open source software and vendor-neutral tools.

You'll learn how to:

- Determine where to deploy NSM platforms, and size them for the monitored networks
- Deploy stand-alone or distributed NSM installations
- Use command line and graphical packet analysis tools, and NSM consoles
- Interpret network evidence from server-side and client-side intrusions
- Integrate threat intelligence into NSM software to identify sophisticated adversaries

There's no foolproof way to keep attackers out of your network. But when they get in, you'll be prepared. *The Practice of Network Security Monitoring* will show you how to build a security net to detect, contain, and control them. Attacks are inevitable, but losing sensitive data shouldn't be.

Download and Read Free Online The Practice of Network Security Monitoring: Understanding Incident Detection and Response Richard Bejtlich

---

From reader reviews:

John McDole:

The particular book The Practice of Network Security Monitoring: Understanding Incident Detection and Response will bring you to the new experience of reading some sort of book. The author style to elucidate the idea is very unique. If you try to find new book to read, this book very ideal to you. The book The Practice of Network Security Monitoring: Understanding Incident Detection and Response is much recommended to you to see. You can also get the e-book from your official web site, so you can more easily to read the book.

Raymond Hollander:

In this period globalization it is important to someone to get information. The information will make you to definitely understand the condition of the world. The healthiness of the world makes the information much easier to share. You can find a lot of personal references to get information example: internet, classifieds, book, and soon. You will see that now, a lot of publisher that print many kinds of book. The particular book that recommended to you is The Practice of Network Security Monitoring: Understanding Incident Detection and Response this publication consist a lot of the information from the condition of this world now. This particular book was represented how can the world has grown up. The words styles that writer value to explain it is easy to understand. The particular writer made some analysis when he makes this book. Honestly, that is why this book suited all of you.

Harry Thomas:

Is it an individual who having spare time and then spend it whole day simply by watching television programs or just resting on the bed? Do you need something new? This The Practice of Network Security Monitoring: Understanding Incident Detection and Response can be the response, oh how comes? A fresh book you know. You are therefore out of date, spending your free time by reading in this brand-new era is common not a geek activity. So what these textbooks have than the others?

Carl Vang:

Don't be worry for anyone who is afraid that this book may filled the space in your house, you will get it in e-book technique, more simple and reachable. This kind of The Practice of Network Security Monitoring: Understanding Incident Detection and Response can give you a lot of pals because by you taking a look at this one book you have thing that they don't and make anyone more like an interesting person. This kind of book can be one of a step for you to get success. This reserve offer you information that might be your friend doesn't recognize, by knowing more than other make you to be great people. So , why hesitate? Let's have The Practice of Network Security Monitoring: Understanding Incident Detection and Response.

Read The Practice of Network Security Monitoring: Understanding Incident Detection and Response by Richard Bejtlich for online ebook

The Practice of Network Security Monitoring: Understanding Incident Detection and Response by Richard Bejtlich Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read The Practice of Network Security Monitoring: Understanding Incident Detection and Response by Richard Bejtlich books to read online.

Online The Practice of Network Security Monitoring: Understanding Incident Detection and Response by Richard Bejtlich ebook PDF download

The Practice of Network Security Monitoring: Understanding Incident Detection and Response by Richard Bejtlich Doc

The Practice of Network Security Monitoring: Understanding Incident Detection and Response by Richard Bejtlich Mobipocket

The Practice of Network Security Monitoring: Understanding Incident Detection and Response by Richard Bejtlich EPub