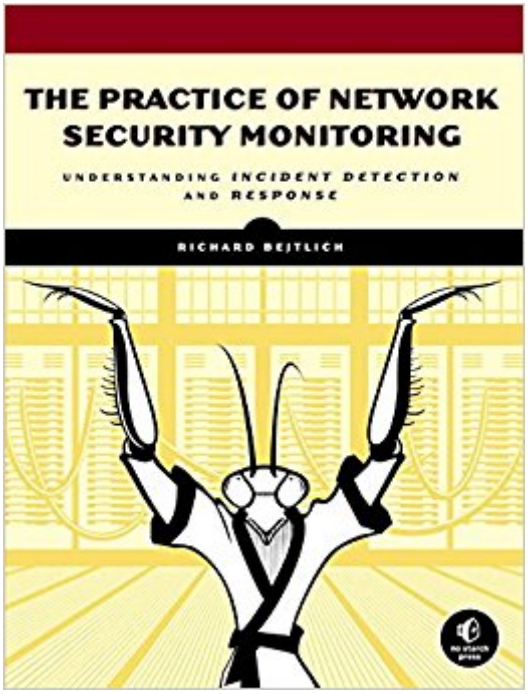
# The Practice Of Network Security Monitoring: Understanding Incident Detection And Response



## Synopsis

Network security is not simply about building impenetrable wallsâ ”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 networksâ ”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:â “Determine where to deploy NSM platforms, and size them for the monitored networksâ “Deploy stand-alone or distributed NSM installationsâ “Use command line and graphical packet analysis tools, and NSM consolesâ “Interpret network evidence from server-side and client-side intrusionsâ “Integrate threat intelligence into NSM software to identify sophisticated adversariesThereâ ™s no foolproof way to keep attackers out of your network. But when they get in, youâ ™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.

## Book Information

Paperback: 376 pages
Publisher: No Starch Press; 1 edition (July 15, 2013)
Language: English
ISBN-10: 1593275099
ISBN-13: 978-1593275099
Product Dimensions: 7 x 1 x 9.2 inches
Shipping Weight: 1.8 pounds (View shipping rates and policies)
Average Customer Review: 4.7 out of 5 stars 43 customer reviews
Best Sellers Rank: #79,899 in Books (See Top 100 in Books) #7 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Administration > Disaster & Recovery #52 inÂ Books > Computers & Technology > Networking & Cloud Computing > Networks, Protocols & APIs > Networks #92 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security

## Customer Reviews

Richard Bejtlich is Chief Security Strategist at FireEye, and was formerly Chief Security Officer at

Mandiant. He also served as Director of Incident Response for General Electric, where he built and led the 40-member GE Computer Incident Response Team (GE-CIRT). He is a graduate of Harvard University and the United States Air Force Academy. His previous works include The Tao of Network Security Monitoring, Extrusion Detection, and Real Digital Forensics (all from Addison-Wesley). He blogs (http://taosecurity.blogspot.com/) and writes on Twitter as @taosecurity.

Actually I've read it from a pirated-PDF but the book was so well and couldn't resist to buy it originally and put it into my book shelf. Thanks Richard (and of course Doug)Best technical book I've ever read.

Well written and a great guide to assist you in security focused architecture design and implementation. It's an inspiring feeling to read books from this author and realize your infrastructure was influenced so much by the same person.

I'm new to network security monitoring, and this is an excellent guide. I love that they share an open source option, with just about a step by step guide to implement, after a decent breakdown of the process and technology of packets.

Great books, must read for people who work with NSMs.

An excellent book full of tools and suggestions on best practices for NSM, a must have.

Book in perfect condition, of course it was the contents that I got it for and that is excellent. Overall very pleased with the book and contents if I may be redundundant.

I thought the Practice of Network Security Monitoring was a great book. I see companies spend millions of dollars on their NSM solution all while there is an open source solution. Spend some money on hardware and network taps and your ready to go! I really like how Bejtlich went into sensor placement and NAT issues. There is nothing worse then doing investigations with with multiple layers or NAT. I would have like to seen a little bit more on how to handle event load that a IDS will produce in a network and maybe some best practices on what signatures to enable.I really enjoyed chapter 12 extending SO, being able to track Binaries and do MD5's and compare them against tools like virus total and other external tools helps stay ahead of the bad guys. It would have

been also neat to show how to extract URLs out of SMTP emails and run them against third party analysis. I believe email attachments are not as easy as getting a user to click on URL. I also would of liked to see a little bit more advanced solution that automatically queries virus total via API then the results are sent back into the monitoring solution via syslog, so the analyst never has to leave the console.Overall a great book!

I found this book very interesting, which is really something for an infosec book. I like the fact the book provides both the high level overview of hows and why, along with the detailed step by step implementation.