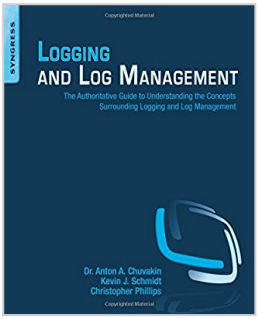

Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management

By Anton A. Chuvakin, Kevin J. Schmidt

Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management By Anton A. Chuvakin, Kevin J. Schmidt

Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management introduces information technology professionals to the basic concepts of logging and log management. It provides tools and techniques to analyze log data and detect malicious activity. The book consists of 22 chapters that cover the basics of log data; log data sources; log storage technologies; a case study on how syslog-ng is deployed in a real environment for log collection; covert logging; planning and preparing for the analysis log data; simple analysis techniques; and tools and techniques for reviewing logs for potential problems. The book also discusses statistical analysis; log data mining; visualizing log data; logging laws and logging mistakes; open source and commercial toolsets for log data collection and analysis; log management procedures; and attacks against logging systems. In addition, the book addresses logging for programmers; logging and compliance with regulations and policies; planning for log analysis system deployment; cloud logging; and the future of log standards, logging, and log analysis.
This book was written for anyone interested in learning more about logging and log management. These include systems administrators, junior security engineers, application developers, and managers.

- Comprehensive coverage of log management including analysis, visualization, reporting and more
- Includes information on different uses for logs -- from system operations to regulatory compliance
- Features case Studies on syslog-ng and actual real-world situations where logs came in handy in incident response
- Provides practical guidance in the areas of report, log analysis system selection, planning a log analysis system and log data normalization and correlation

Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management

By Anton A. Chuvakin, Kevin J. Schmidt

Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management By Anton A. Chuvakin, Kevin J. Schmidt

Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management introduces information technology professionals to the basic concepts of logging and log management. It provides tools and techniques to analyze log data and detect malicious activity.
The book consists of 22 chapters that cover the basics of log data; log data sources; log storage technologies; a case study on how syslog-ng is deployed in a real environment for log collection; covert logging; planning and preparing for the analysis log data; simple analysis techniques; and tools and techniques for reviewing logs for potential problems. The book also discusses statistical analysis; log data mining; visualizing log data; logging laws and logging mistakes; open source and commercial toolsets for log data collection and analysis; log management procedures; and attacks against logging systems. In addition, the book addresses logging for programmers; logging and compliance with regulations and policies; planning for log analysis system deployment; cloud logging; and the future of log standards, logging, and log analysis.
This book was written for anyone interested in learning more about logging and log management. These include systems administrators, junior security engineers, application developers, and managers.

- Comprehensive coverage of log management including analysis, visualization, reporting and more
- Includes information on different uses for logs -- from system operations to regulatory compliance
- Features case Studies on syslog-ng and actual real-world situations where logs came in handy in incident response
- Provides practical guidance in the areas of report, log analysis system selection, planning a log analysis system and log data normalization and correlation

Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management By Anton A. Chuvakin, Kevin J. Schmidt Bibliography

- Sales Rank: #947843 in Books
- Brand: Brand: Syngress
- Published on: 2012-12-13
- Released on: 2012-11-29
- Original language: English
- Number of items: 1
- Dimensions: 9.25" h x 1.05" w x 7.50" l, 1.50 pounds
- Binding: Paperback
- 460 pages

Editorial Review

Review

*"The authors provide a way to simplify the complex process of analyzing large quantities of varied logs. The log management and log analysis approaches they recommend are addressed in detail."--**Reference and Research Book News,* **August 2013** *"…Anton Chuvakin and his co-authors Kevin Schmidt and Christopher Phillips bring significant real-world experience to the reader and an important book on the topic....For those that want to find the gold in their logs…[it] is a great resource that shows how to maximize the gold that often lays hidden in your large stores of log data."--RSA Conference,* December 2012

From the Back Cover

Effectively analyzing large volumes of diverse logs can pose many challenges. *Logging and Log Management* helps to simplify this complex process using practical guidance and real-world examples. Packed with information you need to know for system, network and security logging. Log management and log analysis methods are covered in detail, including approaches to creating useful logs on systems and applications, log searching and log review.

About the Author
Dr. Anton Chuvakin is a recognized security expert in the field of log

management and PCI DSS compliance. He is an author of the books "Security Warrior" and "PCI

Compliance" and has contributed to many others, while also publishing dozens of papers on

log management, correlation, data analysis, PCI DSS, and security management. His blog

(http://www.securitywarrior.org) is one of the most popular in the industry.

Additionaly, Anton teaches classes and presents at many security conferences across the world

and he works on emerging security standards and serves on the advisory boards of

several security start-ups. Currently, Anton is developing his security consulting practice,

focusing on logging and PCI DSS compliance for security vendors and Fortune 500 organizations.

Anton earned his Ph.D. from Stony Brook University.

Kevin J. Schmidt is a senior manager at Dell SecureWorks, Inc., an industry leading MSSP, which is part of Dell. He is responsible for the design and development of a major part of the company’s SIEM platform. This includes data acquisition, correlation and analysis of log data.

Prior to SecureWorks, Kevin worked for Reflex Security where he worked on an IPS engine and anti-virus

software. And prior to this he was a lead developer and architect at GuardedNet, Inc.,which built one of the industry’s first SIEM platforms. Kevin is also a commissioned officer in the United States Navy Reserve (USNR).

Kevin has over 19 years of experience in software development and design, 11 of which have been in the network security space. He holds a B.Sc. in computer science.

Christopher Phillips is a manager and senior software developer at Dell SecureWorks, Inc. He is responsible for the design and development of the company's Threat Intelligence service platform. He also has responsibility for a team involved in integrating log and event information from many third party providers for customers to have their information analyzed by the Dell SecureWorks systems and security professionals. Prior to Dell SecureWorks, Christopher has worked for McKesson and Allscripts where he worked with clients on HIPAA compliance and security and integrating healthcare systems. Christopher has over 18 years of experience in software development and design. He holds a Bachelors of Science in Computer Science and an MBA.

Users Review

From reader reviews:

Jeraldine Thurman:

Do you one of the book lovers? If so, do you ever feeling doubt if you are in the book store? Try and pick one book that you find out the inside because don't assess book by its protect may doesn't work this is difficult job because you are frightened that the inside maybe not as fantastic as in the outside seem likes. Maybe you answer might be Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management why because the excellent cover that make you consider concerning the content will not disappoint a person. The inside or content is definitely fantastic as the outside as well as cover. Your reading 6th sense will directly direct you to pick up this book.

Dominic Maddock:

Many people spending their time period by playing outside along with friends, fun activity along with family or just watching TV the whole day. You can have new activity to invest your whole day by reading a book. Ugh, ya think reading a book can definitely hard because you have to bring the book everywhere? It okay you can have the e-book, taking everywhere you want in your Smart phone. Like Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management which is getting the e-book version. So , why not try out this book? Let's observe.

Peter Christensen:

In this era which is the greater particular person or who has ability to do something more are more treasured than other. Do you want to become certainly one of it? It is just simple method to have that. What you should do is just spending your time almost no but quite enough to possess a look at some books. One of several books in the top collection in your reading list is actually Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. This book that is certainly qualified as The Hungry Inclines can get you closer in turning out to be precious person. By

looking up and review this e-book you can get many advantages.

Abigail Shelton:

Many people said that they feel fed up when they reading a guide. They are directly felt that when they get a half areas of the book. You can choose typically the book Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management to make your current reading is interesting. Your skill of reading skill is developing when you similar to reading. Try to choose basic book to make you enjoy to read it and mingle the feeling about book and reading especially. It is to be initial opinion for you to like to open a book and go through it. Beside that the e-book Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management can to be your new friend when you're truly feel alone and confuse in what must you're doing of these time.

Read Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management By Anton A. Chuvakin, Kevin J. Schmidt for online ebook

Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management By Anton A. Chuvakin, Kevin J. Schmidt 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 Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management By Anton A. Chuvakin, Kevin J. Schmidt books to read online.

Online Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management By Anton A. Chuvakin, Kevin J. Schmidt ebook PDF download

Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management By Anton A. Chuvakin, Kevin J. Schmidt Doc

Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management By Anton A. Chuvakin, Kevin J. Schmidt Mobipocket

Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management By Anton A. Chuvakin, Kevin J. Schmidt EPub