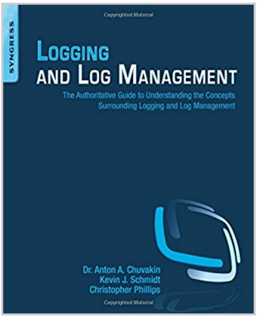

Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management

By Anton A. Chuvakin, Kevin J. Schmidt

Download now

Read Online ➔

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

Download Logging and Log Management: The Authoritative Guid ...pdf

Read Online Logging and Log Management: The Authoritative Gu ...pdf

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

Download Logging and Log Management: The Authoritative Guid ...pdf

Read Online Logging and Log Management: The Authoritative Gu ...pdf

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

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:

George Hinnenkamp:

The book Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management make you feel enjoy for your spare time. You can use to make your capable a lot more increase. Book can being your best friend when you getting tension or having big problem using your subject. If you can make looking at a book Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management to get your habit, you can get more advantages, like add your own personal capable, increase your knowledge about some or all subjects. It is possible to know everything if you like available and read a reserve Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Kinds of book are several. It means that, science reserve or encyclopedia or other folks. So , how do you think about this e-book?

Daniel Rhoads:

Many people spending their time period by playing outside together with friends, fun activity along with family or just watching TV 24 hours a day. You can have new activity to invest your whole day by reading through a book. Ugh, do you consider reading a book will surely hard because you have to bring the book everywhere? It okay you can have the e-book, having everywhere you want in your Mobile phone. Like Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management which is obtaining the e-book version. So , why not try out this book? Let's observe.

India Mead:

This Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management is completely new way for you who has intense curiosity to look for some information mainly because it relief your hunger of information. Getting deeper you into it getting knowledge more you know or perhaps you who still having small amount of digest in reading this Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management can be the light food for yourself because the information inside this book is easy to get through anyone. These books acquire itself in the form and that is reachable by anyone, that's why I mean in the e-book contact form. People who think that in guide form make them feel sleepy even dizzy this e-book is the answer. So there is no in reading a book especially this one. You can find actually looking for. It should be here for you. So , don't miss the idea! Just read this e-book style for your better life and knowledge.

Melvin Dwyer:

Reserve is one of source of know-how. We can add our information from it. Not only for students and also native or citizen have to have book to know the up-date information of year to help year. As we know those textbooks have many advantages. Beside all of us add our knowledge, may also bring us to around the world. With the book Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management we can consider more advantage. Don't you to be creative people? To become creative person must like to read a book. Just choose the best book that suitable with your aim. Don't possibly be doubt to change your life by this book Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. You can more pleasing than now.

Download and Read Online Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management By Anton A. Chuvakin, Kevin J. Schmidt #9TIG2MY3OXK

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

9TIG2MY3OXK: Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management By Anton A. Chuvakin, Kevin J. Schmidt