Security Monitoring with Cisco Security MARS

Gary Halleen, Greg Kellogg

Security Monitoring with Cisco Security MARS

Gary Halleen, Greg Kellogg

Security Monitoring with Cisco Security MARS Gary Halleen, Greg Kellogg
Security Monitoring with Cisco Security MARS

Threat mitigation system deployment

Gary Halleen
Greg Kellogg

Networks and hosts are probed hundreds or thousands of times a day in an attempt to discover vulnerabilities. An even greater number of automated attacks from worms and viruses stress the same devices. The sheer volume of log messages or events generated by these attacks and probes, combined with the complexity of an analyst needing to use multiple monitoring tools, often makes it impossible to adequately investigate what is happening.

Cisco® Security Monitoring, Analysis, and Response System (MARS) is a next-generation Security Threat Mitigation system (STM). Cisco Security MARS receives raw network and security data and performs correlation and investigation of host and network information to provide you with actionable intelligence. This easy-to-use family of threat mitigation appliances enables you to centralize, detect, mitigate, and report on priority threats by leveraging the network and security devices already deployed in a network, even if the devices are from multiple vendors.

Security Monitoring with Cisco Security MARS helps you plan a MARS deployment and learn the installation and administration tasks you can expect to face. Additionally, this book teaches you how to use the advanced features of the product, such as the custom parser, Network Admission Control (NAC), and global controller operations. Through the use of real-world deployment examples, this book leads you through all the steps necessary for proper design and sizing, installation and troubleshooting, forensic analysis of security events, report creation and archiving, and integration of the appliance with Cisco and third-party vulnerability assessment tools.

“In many modern enterprise networks, Security Information Management tools are crucial in helping to manage, analyze, and correlate a mountain of event data. Greg Kellogg and Gary Halleen have distilled an immense amount of extremely valuable knowledge in these pages. By relying on the wisdom of Kellogg and Halleen embedded in this book, you will vastly improve your MARS deployment.”
—Ed Skoudis, Vice President of Security Strategy, Predictive Systems

Gary Halleen is a security consulting systems engineer with Cisco. He has in-depth knowledge of security systems as well as remote-access and routing/switching technology. Gary is a CISSP and ISSAP. His diligence was responsible for the first successful computer crimes conviction in the state of Oregon. Gary is a regular speaker at security events and presents at Cisco Networkers conferences.

Greg Kellogg is the vice president of security solutions for Calence, LLC. He is responsible for managing the company’s overall security strategy. Greg has more than 15 years of networking industry experience, including serving as a senior security business consultant for the Cisco Enterprise Channel organization. Additionally, Greg worked for Protego Networks, Inc. (where MARS was originally developed). There he was responsible for developing channel partner programs and helped solution providers increase their security revenue.

Learn the differences between various log aggregation and correlation systems

- Examine regulatory and industry requirements
- Evaluate various deployment scenarios
- Properly size your deployment
- Protect the Cisco Security MARS appliance from attack
- Generate reports, archive data, and implement disaster recovery plans
- Investigate incidents when Cisco Security MARS detects an attack
- Troubleshoot Cisco Security MARS operation
- Integrate Cisco Security MARS with Cisco Security Manager, NAC, and third-party devices
- Manage groups of MARS controllers with global controller operations

This security book is part of the Cisco Press® Networking Technology Series. Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end self-defending networks.

Category: Cisco Press—Security
Covers: Security Threat Mitigation

Download and Read Free Online Security Monitoring with Cisco Security MARS Gary Halleen, Greg Kellogg

From reader reviews:

Alvin Shaw:

The book Security Monitoring with Cisco Security MARS can give more knowledge and information about everything you want. So why must we leave the good thing like a book Security Monitoring with Cisco Security MARS? Several of you have a different opinion about guide. But one aim that book can give many facts for us. It is absolutely proper. Right now, try to closer along with your book. Knowledge or details that you take for that, you may give for each other; you may share all of these. Book Security Monitoring with Cisco Security MARS has simple shape however you know: it has great and massive function for you. You can appear the enormous world by start and read a publication. So it is very wonderful.

Robert Arnett:

Can you one of the book lovers? If so, do you ever feeling doubt while you are in the book store? Attempt to pick one book that you never know the inside because don't ascertain book by its cover may doesn't work is difficult job because you are frightened that the inside maybe not seeing that fantastic as in the outside appearance likes. Maybe you answer may be Security Monitoring with Cisco Security MARS why because the fantastic cover that make you consider in regards to the content will not disappoint an individual. The inside or content is definitely fantastic as the outside or even cover. Your reading 6th sense will directly assist you to pick up this book.

Aurelio Ashley:

Reading a book being new life style in this 12 months; every people loves to read a book. When you read a book you can get a large amount of benefit. When you read publications, you can improve your knowledge, since book has a lot of information in it. The information that you will get depend on what kinds of book that you have read. If you want to get information about your research, you can read education books, but if you want to entertain yourself read a fiction books, this sort of us novel, comics, along with soon. The Security Monitoring with Cisco Security MARS provide you with a new experience in looking at a book.

Patricia McGuire:

You can spend your free time you just read this book this book. This Security Monitoring with Cisco Security MARS is simple to create you can read it in the area, in the beach, train and soon. If you did not have much space to bring the actual printed book, you can buy the actual e-book. It is make you easier to read it. You can save typically the book in your smart phone. And so there are a lot of benefits that you will get when one buys this book.

Download and Read Online Security Monitoring with Cisco Security MARS Gary Halleen, Greg Kellogg #ZMH51RNWSK8

Read Security Monitoring with Cisco Security MARS by Gary Halleen, Greg Kellogg for online ebook

Security Monitoring with Cisco Security MARS by Gary Halleen, Greg Kellogg 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 Security Monitoring with Cisco Security MARS by Gary Halleen, Greg Kellogg books to read online.

Online Security Monitoring with Cisco Security MARS by Gary Halleen, Greg Kellogg ebook PDF download

Security Monitoring with Cisco Security MARS by Gary Halleen, Greg Kellogg Doc

Security Monitoring with Cisco Security MARS by Gary Halleen, Greg Kellogg Mobipocket

Security Monitoring with Cisco Security MARS by Gary Halleen, Greg Kellogg EPub