Google Drive

Security Information and Event Management (SIEM) Implementation (Network Pro Library)

David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask

Security Information and Event Management (SIEM) Implementation (Network Pro Library)

David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask

Security Information and Event Management (SIEM) Implementation (Network Pro Library) David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask

Implement a robust SIEM system

Effectively manage the security information and events produced by your network with help from this authoritative guide. Written by IT security experts, *Security Information and Event Management (SIEM) Implementation* shows you how to deploy SIEM technologies to monitor, identify, document, and respond to security threats and reduce false-positive alerts. The book explains how to implement SIEM products from different vendors, and discusses the strengths, weaknesses, and advanced tuning of these systems. You'll also learn how to use SIEM capabilities for business intelligence. Real-world case studies are included in this comprehensive resource.

- Assess your organization's business models, threat models, and regulatory compliance requirements
- Determine the necessary SIEM components for small- and medium-size businesses
- Understand SIEM anatomy—source device, log collection, parsing/normalization of logs, rule engine, log storage, and event monitoring
- Develop an effective incident response program
- Use the inherent capabilities of your SIEM system for business intelligence
- Develop filters and correlated event rules to reduce false-positive alerts
- Implement AlienVault's Open Source Security Information Management (OSSIM)
- Deploy the Cisco Monitoring Analysis and Response System (MARS)
- Configure and use the Q1 Labs QRadar SIEM system
- Implement ArcSight Enterprise Security Management (ESM) v4.5
- Develop your SIEM security analyst skills

⬇ **Download** Security Information and Event Management (SIEM) I ...pdf

▤ **Read Online** Security Information and Event Management (SIEM) ...pdf

Download and Read Free Online Security Information and Event Management (SIEM) Implementation (Network Pro Library) David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask

---

From reader reviews:

Willie Davis:

Book is usually written, printed, or illustrated for everything. You can learn everything you want by a publication. Book has a different type. To be sure that book is important matter to bring us around the world. Next to that you can your reading skill was fluently. A reserve Security Information and Event Management (SIEM) Implementation (Network Pro Library) will make you to be smarter. You can feel much more confidence if you can know about anything. But some of you think that open or reading some sort of book make you bored. It is not necessarily make you fun. Why they might be thought like that? Have you searching for best book or acceptable book with you?

Martha Furman:

Now a day folks who Living in the era where everything reachable by connect with the internet and the resources inside can be true or not call for people to be aware of each information they get. How many people to be smart in receiving any information nowadays? Of course the reply is reading a book. Reading a book can help folks out of this uncertainty Information particularly this Security Information and Event Management (SIEM) Implementation (Network Pro Library) book since this book offers you rich info and knowledge. Of course the knowledge in this book hundred percent guarantees there is no doubt in it everbody knows.

William Ward:

Spent a free a chance to be fun activity to complete! A lot of people spent their leisure time with their family, or their friends. Usually they undertaking activity like watching television, going to beach, or picnic in the park. They actually doing ditto every week. Do you feel it? Do you need to something different to fill your own personal free time/ holiday? May be reading a book is usually option to fill your no cost time/ holiday. The first thing that you ask may be what kinds of publication that you should read. If you want to test look for book, may be the e-book untitled Security Information and Event Management (SIEM) Implementation (Network Pro Library) can be very good book to read. May be it is usually best activity to you.

Ernest Poole:

As a college student exactly feel bored for you to reading. If their teacher questioned them to go to the library in order to make summary for some reserve, they are complained. Just very little students that has reading's heart and soul or real their leisure activity. They just do what the teacher want, like asked to the library. They go to there but nothing reading significantly. Any students feel that reading is not important, boring in addition to can't see colorful pictures on there. Yeah, it is for being complicated. Book is very important for yourself. As we know that on this age, many ways to get whatever we would like. Likewise word says, many ways to reach Chinese's country. So , this Security Information and Event Management

(SIEM) Implementation (Network Pro Library) can make you feel more interested to read.

Download and Read Online Security Information and Event Management (SIEM) Implementation (Network Pro Library) David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask #HEBTQV6J5C8

Read Security Information and Event Management (SIEM) Implementation (Network Pro Library) by David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask for online ebook

Security Information and Event Management (SIEM) Implementation (Network Pro Library) by David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask 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 Information and Event Management (SIEM) Implementation (Network Pro Library) by David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask books to read online.

Online Security Information and Event Management (SIEM) Implementation (Network Pro Library) by David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask ebook PDF download

Security Information and Event Management (SIEM) Implementation (Network Pro Library) by David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask Doc

Security Information and Event Management (SIEM) Implementation (Network Pro Library) by David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask Mobipocket

Security Information and Event Management (SIEM) Implementation (Network Pro Library) by David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask EPub