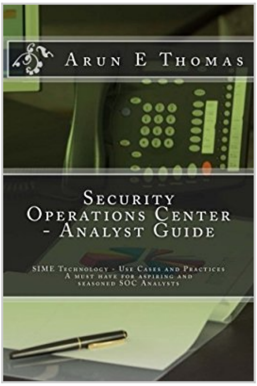

Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices

By Arun E Thomas

Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices By Arun E Thomas

Security analytics can be defined as the process of continuously monitoring and analyzing all the activities in your enterprise network to ensure the minimal number of occurrences of security breaches. Security Analyst is the individual that is qualified to perform the functions necessary to accomplish the security monitoring goals of the organization. This book is intended to improve the ability of a security analyst to perform their day to day work functions in a more professional manner. Deeper knowledge of tools, processes and technology is needed for this. A firm understanding of all the domains of this book is going to be vital in achieving the desired skill set to become a professional security analyst. The attempt of this book is to address the problems associated with the content development (use cases and correlation rules) of SIEM deployments.

Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices

By Arun E Thomas

Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices By Arun E Thomas

Security analytics can be defined as the process of continuously monitoring and analyzing all the activities in your enterprise network to ensure the minimal number of occurrences of security breaches. Security Analyst is the individual that is qualified to perform the functions necessary to accomplish the security monitoring goals of the organization. This book is intended to improve the ability of a security analyst to perform their day to day work functions in a more professional manner. Deeper knowledge of tools, processes and technology is needed for this. A firm understanding of all the domains of this book is going to be vital in achieving the desired skill set to become a professional security analyst. The attempt of this book is to address the problems associated with the content development (use cases and correlation rules) of SIEM deployments.

Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices By Arun E Thomas Bibliography

- Rank: #1094411 in Books
- Published on: 2016-05-22
- Original language: English
- Dimensions: 9.00" h x .57" w x 6.00" l, .99 pounds
- Binding: Paperback
- 224 pages

Download and Read Free Online Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices By Arun E Thomas

Editorial Review

About the Author
With over 15 years of experience as Information Security Professional, Arun holds Multiple Information Security patents and 28+ Professional IT certifications including CISSP concentrations, SSCP, CASP, ECSA/LPT and CCSE . He is the author of several books and is the Chief Security Architect & CTO of NetSentries Technologies (UAE and India). Arun holds his dual Engineering Degree from Institution of Engineers (India) and has held a number of positions during his professional career including Chief Security Architect, CTO, SOC SME, Security Analyst, Consultant and Security Practice Lead.

Users Review

From reader reviews:

Esta Banks:

Have you spare time for any day? What do you do when you have a lot more or little spare time? Sure, you can choose the suitable activity intended for spend your time. Any person spent their spare time to take a go walking, shopping, or went to the Mall. How about open or perhaps read a book called Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices? Maybe it is to become best activity for you. You understand beside you can spend your time with the favorite's book, you can more intelligent than before. Do you agree with it has the opinion or you have different opinion?

Edgar Foley:

A lot of people always spent their free time to vacation or go to the outside with them loved ones or their friend. Do you realize? Many a lot of people spent that they free time just watching TV, or even playing video games all day long. If you need to try to find a new activity that is look different you can read any book. It is really fun for yourself. If you enjoy the book which you read you can spent the whole day to reading a reserve. The book Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices it is extremely good to read. There are a lot of people that recommended this book. These folks were enjoying reading this book. In the event you did not have enough space to develop this book you can buy typically the e-book. You can m0ore effortlessly to read this book out of your smart phone. The price is not too costly but this book offers high quality.

Dave Arreola:

This Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices is great e-book for you because the content and that is full of information for you who also always deal with world and possess to make decision every minute. This book reveal it facts accurately using great manage word or we can state no rambling sentences inside it. So if you are read the item hurriedly you can have whole info in it. Doesn't mean it only provides you with straight forward sentences but hard core information with wonderful delivering sentences. Having Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and

Practices in your hand like finding the world in your arm, information in it is not ridiculous just one. We can say that no e-book that offer you world in ten or fifteen tiny right but this guide already do that. So , it is good reading book. Heya Mr. and Mrs. active do you still doubt that will?

Jesus Rhode:

What is your hobby? Have you heard that will question when you got scholars? We believe that that problem was given by teacher with their students. Many kinds of hobby, All people has different hobby. And also you know that little person similar to reading or as studying become their hobby. You must know that reading is very important and book as to be the thing. Book is important thing to provide you knowledge, except your teacher or lecturer. You find good news or update concerning something by book. A substantial number of sorts of books that can you take to be your object. One of them is this Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices.

Download and Read Online Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices By Arun E Thomas #RPXV36UC9YK

Read Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices By Arun E Thomas for online ebook

Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices By Arun E Thomas 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 Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices By Arun E Thomas books to read online.

Online Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices By Arun E Thomas ebook PDF download

Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices By Arun E Thomas Doc

Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices By Arun E Thomas Mobipocket

Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices By Arun E Thomas EPub