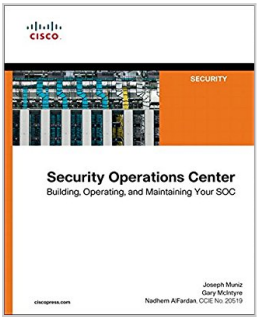

Security Operations Center: Building, Operating, and Maintaining your SOC

By Joseph Muniz, Gary McIntyre, Nadhem AlFardan

Security Operations Center: Building, Operating, and Maintaining your SOC By Joseph Muniz, Gary McIntyre, Nadhem AlFardan

Security Operations Center
Building, Operating, and Maintaining Your SOC

The complete, practical guide to planning, building, and operating an effective Security Operations Center (SOC)

Security Operations Center is the complete guide to building, operating, and managing Security Operations Centers in any environment. Drawing on experience with hundreds of customers ranging from Fortune 500 enterprises to large military organizations, three leading experts thoroughly review each SOC model, including virtual SOCs. You'll learn how to select the right strategic option for your organization, and then plan and execute the strategy you've chosen.

Security Operations Center walks you through every phase required to establish and run an effective SOC, including all significant people, process, and technology capabilities. The authors assess SOC technologies, strategy, infrastructure, governance, planning, implementation, and more. They take a holistic approach considering various commercial and open-source tools found in modern SOCs.

This best-practice guide is written for anybody interested in learning how to develop, manage, or improve a SOC. A background in network security, management, and operations will be helpful but is not required. It is also an indispensable resource for anyone preparing for the Cisco SCYBER exam.

· Review high-level issues, such as vulnerability and risk management, threat intelligence, digital investigation, and data collection/analysis
· Understand the technical components of a modern SOC
· Assess the current state of your SOC and identify areas of improvement
· Plan SOC strategy, mission, functions, and services
· Design and build out SOC infrastructure, from facilities and networks to

systems, storage, and physical security

- Collect and successfully analyze security data
- Establish an effective vulnerability management practice
- Organize incident response teams and measure their performance
- Define an optimal governance and staffing model
- Develop a practical SOC handbook that people can actually use
- Prepare SOC to go live, with comprehensive transition plans
- React quickly and collaboratively to security incidents
- Implement best practice security operations, including continuous enhancement and improvement

Security Operations Center: Building, Operating, and Maintaining your SOC

By Joseph Muniz, Gary McIntyre, Nadhem AlFardan

Security Operations Center: Building, Operating, and Maintaining your SOC By Joseph Muniz, Gary McIntyre, Nadhem AlFardan

Security Operations Center
Building, Operating, and Maintaining Your SOC

The complete, practical guide to planning, building, and operating an effective Security Operations Center (SOC)

Security Operations Center is the complete guide to building, operating, and managing Security Operations Centers in any environment. Drawing on experience with hundreds of customers ranging from Fortune 500 enterprises to large military organizations, three leading experts thoroughly review each SOC model, including virtual SOCs. You'll learn how to select the right strategic option for your organization, and then plan and execute the strategy you've chosen.

Security Operations Center walks you through every phase required to establish and run an effective SOC, including all significant people, process, and technology capabilities. The authors assess SOC technologies, strategy, infrastructure, governance, planning, implementation, and more. They take a holistic approach considering various commercial and open-source tools found in modern SOCs.

This best-practice guide is written for anybody interested in learning how to develop, manage, or improve a SOC. A background in network security, management, and operations will be helpful but is not required. It is also an indispensable resource for anyone preparing for the Cisco SCYBER exam.

· Review high-level issues, such as vulnerability and risk management, threat intelligence, digital investigation, and data collection/analysis
· Understand the technical components of a modern SOC
· Assess the current state of your SOC and identify areas of improvement
· Plan SOC strategy, mission, functions, and services
· Design and build out SOC infrastructure, from facilities and networks to systems, storage, and physical security
· Collect and successfully analyze security data
· Establish an effective vulnerability management practice
· Organize incident response teams and measure their performance
· Define an optimal governance and staffing model
· Develop a practical SOC handbook that people can actually use
· Prepare SOC to go live, with comprehensive transition plans
· React quickly and collaboratively to security incidents
· Implement best practice security operations, including continuous enhancement and improvement

Security Operations Center: Building, Operating, and Maintaining your SOC By Joseph Muniz, Gary McIntyre, Nadhem AlFardan Bibliography

- Sales Rank: #368610 in Books
- Brand: imusti
- Published on: 2015-11-08
- Original language: English
- Number of items: 1
- Dimensions: 8.90" h x 1.10" w x 7.30" l, 1.64 pounds
- Binding: Paperback
- 448 pages

Editorial Review

About the Author

Joseph Muniz is a consultant at Cisco Systems and security researcher. Joseph started his career in software development and later managed networks as a contracted technical resource. Joseph moved into consulting and found a passion for security while meeting with a variety of customers. He has been involved with the design and implementation of multiple projects, ranging from Fortune 500 corporations to large federal networks. Joseph is the author of and contributor to several books and is a speaker for popular security conferences. Check out his blog, http://www.thesecurityblogger.com, which showcases the latest security events, research, and technologies.

Gary McIntyre is a seasoned information security professional focusing on the development and operation of large-scale information security programs. As an architect, manager, and consultant, he has worked with a wide range of public and private sector organizations around the world to design, build, and maintain small to large security operations teams. He currently holds a Masters degree from the University of Toronto and has also been a long-time $(ISC)^2$ instructor.

Dr. Nadhem AlFardan has more than 15 years of experience in the area of information security and holds a Ph.D. in Information Security from Royal Holloway, University of London. Nadhem is a senior security solution architect working for Cisco Systems. Before joining Cisco, he worked for Schlumbeger and HSBC. Nadhem is CISSP certified and is an ISO 27001 lead auditor. He is also CCIE Security certified. In his Ph.D. research, Nadhem published a number of papers in prestige conferences, such as IEEE S&P and USENIX Security, mainly around cryptoanalysis topics. His work involved him working with organizations such as Google, Microsoft, Cisco, Mozilla, OpenSSL, and many others, mainly to help them assess and fix major findings in the Transport Layer Security/Secure Sockets Layer (TLS/SSL) protocol. His work is referenced in a number of IETF standards.

Users Review

From reader reviews:

Steven Zakrzewski:

Hey guys, do you desires to finds a new book to see? May be the book with the name Security Operations Center: Building, Operating, and Maintaining your SOC suitable to you? The actual book was written by famous writer in this era. The book untitled Security Operations Center: Building, Operating, and Maintaining your SOCis one of several books which everyone read now. This specific book was inspired many people in the world. When you read this book you will enter the new shape that you ever know ahead of. The author explained their plan in the simple way, consequently all of people can easily to understand the core of this book. This book will give you a lot of information about this world now. So that you can see the represented of the world on this book.

Colleen Thompson:

Exactly why? Because this Security Operations Center: Building, Operating, and Maintaining your SOC is an unordinary book that the inside of the reserve waiting for you to snap that but latter it will jolt you with the secret the idea inside. Reading this book adjacent to it was fantastic author who else write the book in such wonderful way makes the content on the inside easier to understand, entertaining way but still convey the meaning completely. So , it is good for you because of not hesitating having this any more or you going to regret it. This unique book will give you a lot of advantages than the other book have got such as help improving your ability and your critical thinking method. So , still want to hold up having that book? If I ended up you I will go to the e-book store hurriedly.

Rodney Sierra:

This Security Operations Center: Building, Operating, and Maintaining your SOC is great book for you because the content which can be full of information for you who have always deal with world and have to make decision every minute. This particular book reveal it info accurately using great organize word or we can point out no rambling sentences inside. So if you are read this hurriedly you can have whole information in it. Doesn't mean it only will give you straight forward sentences but tricky core information with wonderful delivering sentences. Having Security Operations Center: Building, Operating, and Maintaining your SOC in your hand like getting the world in your arm, data in it is not ridiculous a single. We can say that no e-book that offer you world in ten or fifteen small right but this reserve already do that. So , this can be good reading book. Hi Mr. and Mrs. hectic do you still doubt in which?

Jill Vaughn:

Is it an individual who having spare time in that case spend it whole day simply by watching television programs or just resting on the bed? Do you need something new? This Security Operations Center: Building, Operating, and Maintaining your SOC can be the respond to, oh how comes? The new book you know. You are and so out of date, spending your spare time by reading in this new era is common not a nerd activity. So what these publications have than the others?

Read Security Operations Center: Building, Operating, and Maintaining your SOC By Joseph Muniz, Gary McIntyre, Nadhem AlFardan for online ebook

Security Operations Center: Building, Operating, and Maintaining your SOC By Joseph Muniz, Gary McIntyre, Nadhem AlFardan 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: Building, Operating, and Maintaining your SOC By Joseph Muniz, Gary McIntyre, Nadhem AlFardan books to read online.

Online Security Operations Center: Building, Operating, and Maintaining your SOC By Joseph Muniz, Gary McIntyre, Nadhem AlFardan ebook PDF download

Security Operations Center: Building, Operating, and Maintaining your SOC By Joseph Muniz, Gary McIntyre, Nadhem AlFardan Doc

Security Operations Center: Building, Operating, and Maintaining your SOC By Joseph Muniz, Gary McIntyre, Nadhem AlFardan Mobipocket

Security Operations Center: Building, Operating, and Maintaining your SOC By Joseph Muniz, Gary McIntyre, Nadhem AlFardan EPub