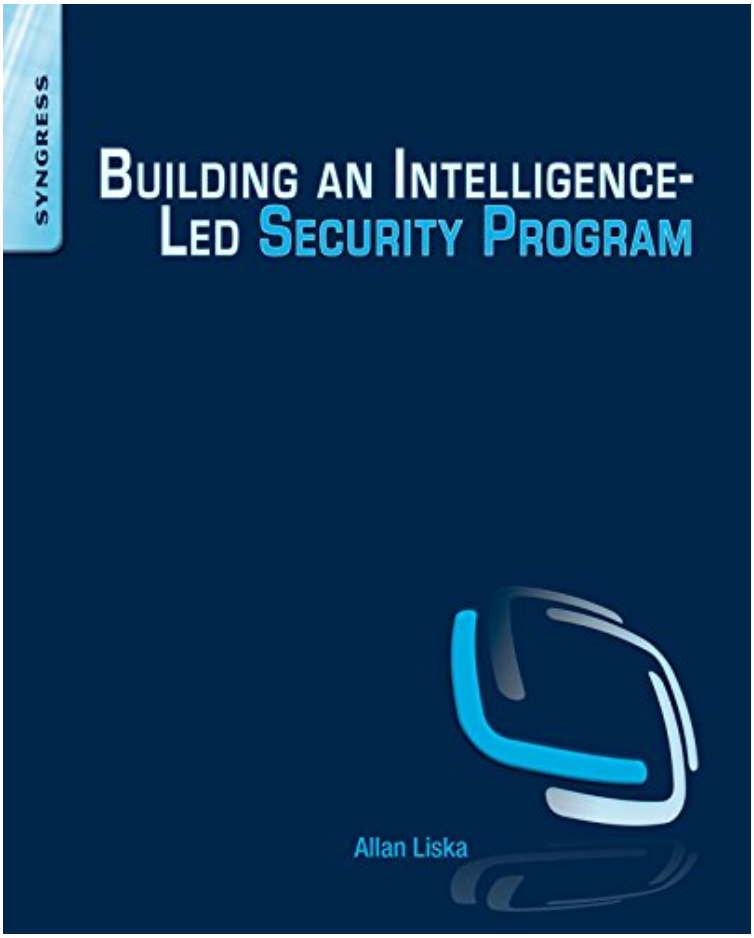
Building an Intelligence-Led Security Program

Allan Liska
*ePub | *DOC | audiobook | ebooks | Download PDF*



#1608382 in eBooks 2014-12-10 2014-12-10File Name: B00R4DX84G | File size: 35.Mb

Allan Liska : Building an Intelligence-Led Security Program before purchasing it in order to gage whether or not it would be worth my time, and all praised Building an Intelligence-Led Security Program:

5 of 5 people found the following review helpful. Valuable ideas that you can leverage for greater security.By B GutzFor myself the one thing more than anything else the author has missed is that the center of network and system security is always what and where is the data, where are the crown jewels? Its not that its not encompassed in the pages but for myself I think this is the one thing in security and in this book and most others that needs to be in plain English so it doesn't get lost. My other little quibble is the book has more material cited than a college text book and even though this is the correct way to do things its a little overwhelming. The last two chapters seem to be more forced on to the book rather than integrated but still worth a look. Still pointing out different resources and what can be gained and how it can be integrated is extremely helpful. Recommended but do have a little patience with the style, the material itself is well worth while!Overall I would certainly buy this book again, and it presents a wide scope of useful information, and the authors overall depth and considerations are solid. This book belongs in the library of anyone concerned with such a subject and network intelligence.1 of 1 people found the following review helpful. Tie your

defense togetherBy Matthew MonteMr. Liska makes the case that the process of security, how you think about and then fashion and execute an effective defense, is more important than the specific technologies deployed. His guiding principle is that the intelligence lifecycle, from data collection through analysis through dissemination, forms the backbone of evaluating and implementing any of a number of individual defensive tools.The book offers a wealth of specific tools and processes, and most importantly, how a business can phase in the implementation. For that reason alone, I would recommend it, as we all know many business approach security at the extremes: either not caring at all or just trying to throw money at the problem.Overall, while I may not necessarily agree with every tactic, this book does a great job of detailing the current state of the art and how those technologies could fit into an overall plan. It is useful to anyone looking to setup a coherent security process.Disclaimer: I am a colleague of Allanrsquo;s though we have never worked for the same company.0 of 1 people found the following review helpful. Not with itBy Anthony SgroiThis book is exactly 32 pages. No, that's not a typo 32 pages. Taking into account the price, this was not worth it. You can find better information on the internet for free.

As recently as five years ago, securing a network meant putting in a firewall, intrusion detection system, and installing antivirus software on the desktop. Unfortunately, attackers have grown more nimble and effective, meaning that traditional security programs are no longer effective. Today's effective cyber security programs take these best practices and overlay them with intelligence. Adding cyber threat intelligence can help security teams uncover events not detected by traditional security platforms and correlate seemingly disparate events across the network. Properly-implemented intelligence also makes the life of the security practitioner easier by helping him more effectively prioritize and respond to security incidents. The problem with current efforts is that many security practitioners don't know how to properly implement an intelligence-led program, or are afraid that it is out of their budget. Building an Intelligence-Led Security Program is the first book to show how to implement an intelligence-led program in your enterprise on any budget. It will show you how to implement a security information a security information and event management system, collect and analyze logs, and how to practice real cyber threat intelligence. You'll learn how to understand your network in-depth so that you can protect it in the best possible way.Provides a roadmap and direction on how to build an intelligence-led information security program to protect your company.Learn how to understand your network through logs and client monitoring, so you can effectively evaluate threat intelligence.Learn how to use popular tools such as BIND, SNORT, squid, STIX, TAXII, CyBox, and splunk to conduct network intelligence.

About the AuthorAllan Liska has more than 15 years of experience in the world of information security. Mr. Liska has worked both as a security practitioner and an ethical hacker, so he is familiar with both sides of the security aisle and, through his work at Symantec and iSIGHT Partners, has helped countless organizations improve their security posture using more effective intelligence. In addition to security experience, Mr. Liska also authored the book The Practice of Network Security and contributed the security-focused chapters to The Apache Administrators Handbook.