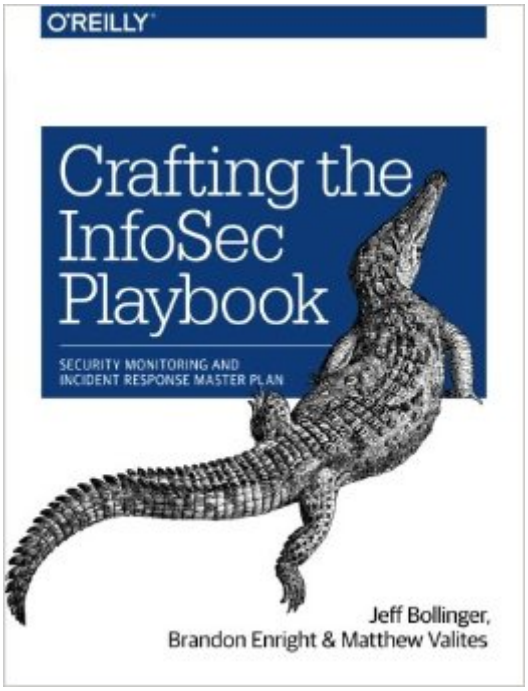
Crafting The InfoSec Playbook: Security Monitoring And Incident Response Master Plan



Synopsis

Any good attacker will tell you that expensive security monitoring and prevention tools arenâ ™t enough to keep you secure. This practical book demonstrates a data-centric approach to distilling complex security monitoring, incident response, and threat analysis ideas into their most basic elements. Youâ ™ll learn how to develop your own threat intelligence and incident detection strategy, rather than depend on security tools alone.Written by members of Ciscoâ ™s Computer Security Incident Response Team, this book shows IT and information security professionals how to create an InfoSec playbook by developing strategy, technique, and architecture.Learn incident response fundamentalsâ ”and the importance of getting back to basicsUnderstand threats you face and what you should be protectingCollect, mine, organize, and analyze as many relevant data sources as possibleBuild your own playbook of repeatable methods for security monitoring and responseLearn how to put your plan into action and keep it running smoothlySelect the right monitoring and detection tools for your environmentDevelop queries to help you sort through data and create valuable reportsKnow what actions to take during the incident response phase

Book Information

Paperback: 276 pages

Publisher: O'Reilly Media; 1 edition (May 24, 2015)

Language: English

ISBN-10: 1491949406

ISBN-13: 978-1491949405

Product Dimensions: 7 x 0.6 x 9.2 inches

Shipping Weight: 1.1 pounds (View shipping rates and policies)

Average Customer Review: 4.4 out of 5 starsÂ Â See all reviewsÂ (8 customer reviews)

Best Sellers Rank: #405,926 in Books (See Top 100 in Books) #88 inÂ Books > Computers & Technology > Security & Encryption > Viruses #353 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security #413 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Administration

Customer Reviews

An extremely important piece of advice in Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan is on page 85, where authors Jeff Bollinger, Brandon Enright and Matthew Valites write that you will need at least one dedicated and full-time person to analyze your security event data.When creating programs for information security monitoring and its

corresponding incident response plans, far too many firms focus solely on the software, hardware and appliances; not realizing it takes people to make it work. The book shows how to take the potential of them devices, and put them into actuality. The book notes that itâ ™s not a trivial matter, but itâ ™s not rocket science, and it can be done.The premise of the book is that only when you know and can describe exactly what you are trying to protect; can you develop an information security playbook and incident response program. The book then goes into detail just how to do that.The book is an extremely valuable reference for anyone who wants to build out a security monitoring and incident program. The authors take a very hands-on approach on how to develop a strategy to ensure that the process is done effectively, rather than by simply installing a few appliances and hoping for the best.While the authors are all part of the Cisco Computer Security Incident Response Team, the book takes a vendor agnostic approach to the topic.Security monitoring and incident response are two critical component of a larger information security program. For those that are serious about building that out, Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan is a great resource to start with.

Very good guide on InfoSec program policy development. I think this should be mandatory for anyone moving 'up the chain' in security. In my role as a consultant, I find that there are smart people doing good things...in silos. This guide is a good foundation for building a program that ties disparate efforts together as a cohesive and effective infosec program. This book continues to be a good reference.I think the book could have been improved with more pictures of alligators and other dangerous reptilian creatures.

Phenomenal book, chock full of great ideas about how to build and operationalize your SOC. Includes high level concepts as well as detailed technical ideas. Highly recommended for anyone building or improving a security program.

Down to earth with tips you can take straight to the InfoSec bank.

Friendship, and Purpose in Your Marriage Beautiful Data: A History of Vision and Reason since 1945 (Experimental Futures) Garden City: Work, Rest, and the Art of Being Human. Fear and Faith: Finding the Peace Your Heart Craves To Heaven and Back: The Journey of a Roman Catholic Priest A Doctor's Tools (Community Helpers and Their Tools) Why Suffering?: Finding Meaning and Comfort When Life Doesn't Make Sense Rainbow Warriors and the Golden Bow: Yoga Adventure for Children (Rainbow Warriors Yoga Series) Touching Heaven: A Cardiologist's Encounters with Death and Living Proof of an Afterlife Machines of Loving Grace: The Quest for Common Ground Between Humans and Robots Husband After God: Drawing Closer To God And Your Wife Sex is a Funny Word: A Book about Bodies, Feelings, and YOU Learn Command Line and Batch Script Fast, Vol II: A course from the basics of Windows to the edge of networking How to Start a Business Analyst Career: The handbook to apply business analysis techniques, select requirements training, and explore job roles ... career (Business Analyst Career Guide)