Foreword

If a tree falls in the forest but nobody is around to hear it, does it make a sound? Philosophers and physicists have volleyed that brainteaser for years. But consider it as a metaphor for your computer systems. If an event is logged on your network, but nobody monitors your logs, how can you determine whether an attack occurred? By missing out on the opportunity to catch bad guys early through solid event analysis, you've extended and deepened your exposure to the attacker's foul plot. You'll never know what's going on until the bad guys start making blatant changes on your systems, wreaking all kinds of damage. In many modern enterprise networks, Security Information Management tools, or SIMs for short, are crucial in helping to manage, analyze, and correlate a mountain of event data. Increasingly, SIM solutions act as our eyes and ears to let us know when trees start falling in our networks.

Have you ever seen the television show *24*? If you haven't, the story centers around a high-tech Counter Terrorism Unit (CTU) working exhaustive hours to foil bad guys who try to deal death and destruction to innocent victims. Jack Bauer, played by Kiefer Sutherland, is the world's ultimate good-guy field agent, heading up each action-packed episode. While Jack's skills are important, he relies heavily on the technical wizardry and information analysis abilities of his coworkers back at the office. In almost every nail-biting episode, these data analysts pull the proverbial needle out of the information haystack just in the nick of time to help Jack save civilization. With all the data flowing into CTU, these analysts must rely on the ultimate SIM infrastructure to work their magic.

So what does *24* have to do with this book? Besides the passing resemblance of this book's authors to Jack Bauer, *24* highlights the importance of information management in thwarting bad guys: integrating and correlating data from a myriad of system types. I'm sorry to say that this book won't turn you into Jack Bauer, nor will it let you create a mythical SIM solution that matches the functionality of the all-seeing analysts of the *24* TV show. But if you read this book and live by its principles, you can design and deploy a SIM solution that maximizes your abilities to understand and monitor your systems using the Cisco MARS product.

Unfortunately, many SIM deployments are not well planned and result in either abject failure or an infrastructure that barely scratches the surface of potential MARS functionality. That's why deploying and using MARS without reading this book is like throwing money away. Greg Kellogg and Gary Halleen have distilled an immense amount of extremely valuable knowledge in these pages. By relying on the wisdom of Kellogg and Halleen embedded in this book, you will vastly improve your MARS deployment, helping your own metaphorical field agents detect, dodge, and even stop falling trees.

—Ed Skoudis

December 2006

Vice President of Security Strategy

Predictive Systems