Foreword

Today's biggest challenge in computer security is dealing with the huge amounts of data that pour in from disparate and distributed sources. Gigabytes of firewall logs, intrusion detection system logs, and user activity logs are more than any human can expect to cope with or analyze; we need software layers to help sort through the mass of data and turn it into useful, actionable information. The notion of "actionable" information, in this context, is especially important. It's no longer enough to inform a security administrator, "Something suspicious happened on this host at 11:54 p.m." The threats are too complex and fast-moving for a human to be effective inside the response cycle. We need software that wraps the data analysis with a knowledge base of what are reasonable reactions to take to certain classes of events, so that an administrator is presented not merely with a problem diagnosis but also a resolution recommendation. That's what Cisco's MARS is all about—turning data into actionable information and recommendations.

Typically a technical book's foreword is a chance for someone who has read the book to ramble for a couple pages about some high-level topic, then end with a ringing exhortation to "buy and read this book!" For most of us, that adds nothing (except for two or three pages you can flip past), so I thought I'd approach this foreword a bit differently. To me, one of the things lacking in most technical books is a feeling for the authors themselves. Who are these guys? What motivated them to write this book? Besides, you probably didn't pick up this book because you wanted to read *my* pontifications—you wanted to see what Dale and Greg have to say!

Instead of my opinions, I thought I'd use this space to interview the authors about some of the things you *won't* find elsewhere in the book. Dear reader, let me introduce Dale Tesch, Jr, and Greg Abelar:

Marcus: *So CS-MARS is obviously a system in which you have a lot of time and energy invested. How did you first get involved with it, and what got you excited about it?*

Dale: I was first introduced to MARS while I was a security engineer for Cisco working with Channel Partners. I had a partner approach me looking for a solution that could help them deploy a security managed service to their customers. They had customers with all kinds of products and looked to Cisco to help them find a solution. Cisco did not have a product that could help them, so I started looking outside the Cisco product set. I turned to my fellow engineers in Cisco and discovered one of them left Cisco to start up Protego Networks. They had a product that may do what my Cisco Partners needed. I contacted him and fell in love with the product. As a security engineer I was very passionate about security technology that promised what it delivered, and MARS delivered what I needed and more. It filled a gap in the security market that no company was fulfilling. I knew it was going to take off! Protego MARS was so simple to operate yet very strong in SIM and behavioral analysis. It was making me so successful with our key security partners that I decided to leave Cisco and join Protego.

Greg: I first experienced CS-MARS when it was still part of a company called Protego. I was deeply involved in network intrusion prevention systems (IPS) at the time. IPSs have their strengths, but their value is diminished by the huge volume of noise and false positive alerts they generate. A friend of mine called me asking about a company called Protego that had a device that could supposedly reduce false positive alerts. Intrigued, I set out to find out a little bit about this technology. As luck would have it, the next day I saw some engineers testing a Protego box in the lab, so I hung out to see what the big deal was. Big deal, indeed. I saw a demo where they ran an attack that triggered a group of IPS alerts, but CS-MARS consolidated those alerts to a single event and also recommended a command to mitigate the attack. It did multidevice event consolidation and event correlation. It was easy to use and also made and deployed mitigation recommendations. The rest is history. I was hooked. Cisco acquired Protego, and the daily nightmare that security responders faced dealing with several thousand alerts was significantly reduced. They suddenly had a tool that improved their efficiency to a level that was staggering.

Marcus: *You're talking about a technology that sits right in the middle of the entire computer/network security problem—it's a lot to get a handle on! How did you figure out where to start?*

Greg: On the surface CS-MARS appears to be a tame animal. You launch the GUI, configure it, then off you go, right? Well, right but also wrong. Your question indicates there is much more to it than that, and you are correct. You can configure CS-MARS with a basic configuration and get some valuable data that will help you respond to threats. But to get the most out of your CS-MARS appliance, you need to have a good understanding of your network topology, your security devices, and how attacks work. Then you need to understand the capabilities of the CS-MARS product.

This book answers exactly this question. It not only addresses how to start working with CS-MARS, but it also addresses where you go after you have started. Looking at the book from a high level, we take the reader from the basics of security reporting and mitigation, explain any new terminology and technology used by CS-MARS, explain basic configurations, and then explain how to interpret incidents as they are reported. To simplify the learning experience for the reader, the book includes plenty of step-by-step guidelines as well as clearly explained technical tidbits to give you an excellent jumpstart into this technology.

Dale: Good old trial and error worked for me! You can take all kinds of advice, training courses, or pointers from the pro's, but until you get your feet wet in real operational networks with the technology, you can never get the insight and experience on how to solve business problems with it.

Marcus: *Dale, you say it's important to experiment. Do you remember any "AHA!" moments that you've had that really made things click for you? I've found with many of the products I've worked, sometimes you use it in a way that nobody expects, and it works great. It's always fun when you talk to the designers and say, "It's great for doing blah blah blah," and they respond, "Really!!? We never thought of that!"*

Dale: When I first joined Protego and really started working with MARS, I discovered the product was schizophrenic. Meaning, it had many personalities. The appliance was built for security threat detection, analysis, and mitigation, yet it could play many other roles in a network. Shortly before the acquisition by Cisco, I was in a VARS SOC. I was rather impressed by the facility they had and how automated it was. They were bragging about how they could manage it remotely from anywhere via the web. Their HVAC system, physical security system, and lighting systems were all automated and sent log data via SNMP. Just for show and tell and a little experiment, we configured the systems to report to MARS and built rules outlining normal behavior of temperatures, lighting, and physical access control. We began to design rules and alarms to go off when temps went out of range, visitors checked in but not out, and even when certain lights were turned on during odd hours. The VAR then took this to the company that sold them the building systems and they bought one for themselves. They are now positioning it as a monitoring solution for their building automation products. They recently installed one for an airport in Canada with three terminals and use it solely for building monitoring. Rather odd application, but it works great!

Marcus: *The idea of a piece of software recommending how to respond to an attack is interesting! I'm sure we can all imagine ways that could go horribly wrong—or be very comforting. What's your experience with that?*

Greg: This is a very important question that should be asked by every single customer before moving forward on a CS-MARS deployment. Obviously Cisco has a very high confidence that the quality of the decisions made by this software is accurate. The quality assurance cycle to ensure the software operates as advertised is immense. Probably the most comforting part of the way the software makes critical decisions is the fact that it correlates messages from several different security and network sources. The more sources correlated is directly related to more accurate and decisive decisions. True, a customer could find themselves in a position where very little information is being correlated, which could lead CS-MARS software to report false positives. To reduce the impact of this problem, CS-MARS engineers either will not make a mitigation recommendation or elect to only suggest mitigation commands and give the customer the final decision on whether to actually deploy the mitigation command. Regardless of these safeguards, my personal experience has been that the mitigation recommendations even in a minimally configured CS-MARS appliance have been extremely accurate.

Marcus: *One of the things I've heard a lot of authors say is that they learn much more in the process of writing a book than they ever expected. What's the biggest/most important lesson you've come away with from this experience?*

Dale: Marcus, this is so true and I never would have fully realized it unless I experienced it. Since I worked with the product since its infancy, I really thought I knew most of it. Writing this book opened my eyes to how much I didn't know. I have always been comfortable with explaining the technology to people and how they can use it. What I really didn't know is what made this thing really tick (the "secret sauce") and what it took to do it. Additionally, I learned what this could not do and how not to use it.

Greg: This is the second book I've authored. The lesson I learned in the first book held true while writing this book also. As a technical author I need to write about something that I believe in, and something that I feel will bring real value to people who read the book. CS-MARS is such a critical technology and can add so much value to security responders that it was very easy for me to stay motivated and bring this project to closure. I'm not fooling myself into believing that this book will be a best-seller and Dale and I will become famous because of it. However, I do feel confident that whoever reads this book will learn about CS-MARS and will be able to use it and add value to any security deployment.

Marcus: *So what's your favorite part of this book? What did you enjoy writing the most? If you could tell a reader, "Hey, whatever you do, make sure you read the part about XYZ!" what would it be?*

Dale: It would be Chapter 9. I had lots of flexibility on how to write the customer stories and no technical guidelines. So I was a bit more free in my approach to writing this chapter. What was fun was that I personally experienced every single story in this chapter, and they were amazing to experience. I really enjoyed telling about them. The disappointing part is that I had so many "cool" stories to tell about the success of the product but could only pick a few. I had a hard time deciding which ones to use. I would recommend everyone read this chapter, because it gives real-life examples of how this product really worked for all different kinds of customers. Readers can really understand the benefits of this product simply by identifying the stories to their own experiences.

Marcus: *Final word: What's the most important thing in security?*

Dale: Good qualified people with a plan! O.K. that is kind of two things, but they need to be together. No matter how you look at security (either network or physical security), the purposes of both are practically pointless unless you have motivated, well-trained people executing a well-written plan. I have consulted for very large firms who have some very sophisticated network security systems with no written security policy or business continuity plan. They spent millions of dollars on great product and people. They have talented individuals who could do just about anything, but no plan on how to use them or what to do if something goes wrong. I find that a lot of organizations, from governments to commercial business, implement security because they are being told to do so. When an organization is out to satisfy some piece of legislation that is poorly written to begin with, their focus tends to be on not getting in trouble instead of how to continue operations if something does go wrong. Security is hard to justify, and organizations need to look at it like insurance to protect their business instead of an operations expense chewing away at their revenues. Once they adopt this reasoning, they'll understand they need a POLICY to implement the insurance to protect their operations and a PLAN to make a claim on that POLICY for business continuity. Bottom line: no plan, no security.

Marcus: *Gentlemen, thank you! And thank you for taking the time to write this book.*

So there you have it, dear reader. Perhaps this little chat has given you a chance to get to know Dale and Greg a little bit. I've certainly enjoyed meeting them and reading this book, and I hope you will, too.

Marcus J. Ranum

July 26, 2006

Bellwether Farm, Morrisdale PA