Introduction

Security Event Management (SEM) systems, Security Information Management (SIM) systems, and Security Threat Mitigation (STM) systems are all solutions with a primary goal of making it easier to determine when bad things are happening on your network. Ideally, the tools we use to correlate events between various network and security devices or software will detect malicious behavior before damage is done, rather than letting us know when we've already been compromised.

This book is intended to describe how a third-generation tool, the Cisco Security Monitoring, Analysis, and Response System (CS-MARS), performs as an STM solution.

Goals and Methods

The goal of this book is to provide the information you need to successfully use the CS-MARS appliances in a real network, on a day-to-day basis. No SIM or STM solution, out of the box, is a perfect fit for every network. As you read through the chapters, we hope you find tidbits that help you make the most of your investment. We also hope you learn enough to avoid some of the common mistakes and misconfigurations.

CS-MARS is a powerful tool that can dramatically increase your knowledge of activity, whether malicious or not, on your network. There are many case studies and other examples throughout the book that show you how this STM functions in a real-world network. Hopefully, some of these examples will bear a resemblance to your own network.

By the time your finish this book, you should have a good understanding of the overall operations and maintenance tasks involved with a CS-MARS deployment. Some of the things you will learn include:

- How to properly design and size a CS-MARS deployment
- Protection of the information contained with CS-MARS
- Incident investigation techniques
- Customization features to allow support of applications and devices that aren't natively supported
- Creation of custom reports and queries

This Book's Audience

The primary audience for this book comprises information security analysts, security officers, and anyone who is tasked with monitoring or maintaining devices and software, such as:

- Firewalls
- Intrusion prevention systems (IPS) or intrusion detection systems (IDS)
- Antivirus systems
- Host intrusion protection systems
- Virtual Private Network (VPN) devices

- Authentication systems
- Web servers
- Vulnerability assessment systems

This book assumes that you have a basic understanding of networking technologies and security technologies. It also assumes that you are able to perform basic CS-MARS installation tasks and have a basic proficiency with Linux or other UNIX operating systems.

How This Book Is Organized

This book is organized into three parts, each with a number of chapters. Part I introduces CS-MARS and Security Threat Mitigation systems. It describes features and strategies for using CS-MARS as your STM solution. In addition, Part I covers regulatory issues and discusses design and sizing scenarios. Part II focuses on day-to-day operations and forensics. Part III discusses more advanced topics, such as integration with other management solutions or technologies, as well as customization features. The appendixes provide a sample script for parsing MARS data from a third-party application, in addition to useful links and a command reference.

The chapters in this book cover the following topics:

- Part I: Introduction to CS-MARS and Security Threat Mitigation

  Chapter 1: Introducing CS-MARS—This chapter discusses differences between different log aggregation and correlation systems. It also covers an introduction to the various MARS components, the user interface, and the types of devices that typically log to MARS.

  Chapter 2: **Regulatory Challenges in Depth**—This chapter examines many of the regulatory and industry requirements businesses face today, and how MARS assists in meeting these requirements.

  Chapter 3: CS-MARS Deployment Scenarios—This chapter examines the various ways local controllers, standalone controllers, and global controllers can be deployed to best meet your needs. Additionally, it covers techniques for properly sizing your deployment.

- Part II: CS-MARS Operations and Forensics

  Chapter 4: Securing CS-MARS—This chapter focuses on why you need to secure CS-MARS and other security management or monitoring products, and how to protect MARS from attack.

  Chapter 5: Rules, Reports, and Queries—This chapter covers how to understand and use the reporting and query interfaces.

  Chapter 6: Incident Investigation and Forensics—This chapter focuses on what to do when CS-MARS detects an attack.

  Chapter 7: **Archiving and Disaster Recovery**—This chapter focuses on data retention, archiving, and recovering from a disaster.

- Part III: CS-MARS Advanced Topics

  Chapter 8: Integration with Cisco Security Manager—Cisco Security Manager is a management product for Cisco security products. This chapter demonstrates integration between the two products and describes how to use the strengths of each.

  Chapter 9: **Troubleshooting CS-MARS**—This chapter discusses what to do when things don't work like they should. What do you do before calling TAC?

  Chapter 10: **Network Admission Control**—This chapter discusses the Cisco Network Admission Control set of products that allow or deny network access based on a host's capability to meet a certain posture level, and describes how NAC integrates into CS-MARS.

  Chapter 11: **CS-MARS Custom Parser**—This chapter dives into configuring CS-MARS to use security logs from officially unsupported devices and software.

  Chapter 12: **Global Controller Operations**—This chapter focuses on what is involved in using a global controller to manage and monitor a group of MARS local controllers.

- Part IV: Appendixes

  Appendix A: Querying the Archive—This appendix discusses how the MARS archiving feature allows integration with command-line and other applications, to provide a lightweight query capability. A sample Python script is provided.

  Appendix B: CS-MARS Command Reference—This appendix provides a reference to the various commands available from the MARS command-line interface.

  Appendix C: Useful Websites—This appendix provides a list of websites the authors have found useful in working with CS-MARS.