



Implementing Cisco Security Monitoring, Analysis, and Response System

Length
4 days

Format
Lecture/lab

Version
3.0

Course Description

The Cisco Security Monitoring, Analysis, and Response System (MARS) is a family of high-performance, scalable appliances for threat management, monitoring, and mitigation, enabling more effective use of network and security devices by combining network intelligence, context correlation, vector analysis, anomaly detection, hotspot identification, and automated mitigation capabilities. This 4-day, lab-intensive course shows you how to use MARS to identify, manage, and eliminate network attacks.

Who Should Attend

This course is designed for network professionals who will be implementing or administering the MARS system.

Recommended Prerequisites

- CCNA certification or equivalent knowledge
- Fundamental knowledge of implementing network security
- CCSP or Security CQS recommended

Related Courses

- Securing Cisco Network Devices (SND)
- Securing Networks with Cisco Routers and Switches (SNRS)

MARS

Learning Objectives

After completing this course, you will be able to:

- Describe a CS-MARS solution and its role in Cisco Threat-Defense System management
- Describe the software components of CS-MARS architectural design
- Configure the network reporting devices to work with the CS-MARS appliance
- Use network reporting and mitigation devices with the CS-MARS appliance
- View the security status of your network
- Configure a rule that detects patterns of network activity and anomalous network behavior
- Generate queries and reports
- Perform incident investigation
- Configure user-defined log parser templates
- Integrate Cisco Security Manager and CS-MARS
- Perform common maintenance and troubleshooting tasks
- Describe the functions of the CS-MARS Global Controller



Learning
Solutions

www.fireflycom.net

(c) 2008 Firefly Communications, LLC. All rights reserved.



Implementing Cisco Security Monitoring, Analysis, and Response System

Lesson 1: Introducing CS-MARS

Effective Security Monitoring and Management
Cisco Self-Defending Network and the Role of
Cisco Security MARS
Cisco Security MARS
Cisco Security MARS Terminology
Cisco Security MARS Technologies
Cisco Security MARS User Interface
Cisco Security MARS Product Portfolio

Lesson 2: Understanding the System Architecture

Cisco Security MARS Software Components
Cisco Security MARS Process Flow Details

Lesson 3: Configuring a Cisco Security MARS Appliance

Initial Cisco Configuration Overview
Scenario: Configuration Tasks
Deployment Planning Guidelines

Lab: Accessing the Cisco Security MARS Appliance

Lesson 4: Adding Reporting and Mitigation Devices

Overview of Reporting and Mitigation Devices
Scenario: Adding a Cisco Reporting Device
and Enabling NetFlow
Data-Enabling Features of Cisco Security
MARS
Integrating Cisco Security MARS with Third-
Party Applications

Lab: Adding Reporting Devices and Enabling NetFlow

Lab: Configuring the Syslog Forwarding Feature

Lesson 5: Viewing the Summary Page

Summary Page Overview
Dashboard
Network Status
My Reports

Lab: Generating Summary Reports

Lesson 6: Managing Rules

Rules Overview
Working with System and User Inspection Rules
Working with Drop Rules
Rule Groups Overview

Lab: Configuring Cisco Security MARS Event Types

Lab: Configuring an Inspection Rule

Lesson 7: Understanding Queries and Reports

Query Page
Scenario: Configuring a Query
Reports Page
Scenario: Configuring a System Report

Lab: Performing a Query and Creating a Custom Report

Lesson 8: Investigating and Mitigating Incidents

Incidents Overview
Incidents
Scenario: Role of Cisco Security MARS in Your
Network
False Positives
Case Management
Scenario: Configuring a Case to Track an
Incident
Configuring Notifications

Case Study: Preventing the W32 Blaster Worm

Lab: Performing Incident Investigation and Mitigation

Lesson 9: Working with User-Defined Log Parser Templates

Overview of User-Defined Log Parser Templates
Scenario: Configuring a Customer Parser

Lab: Configuring the Custom Parser





Implementing Cisco Security Monitoring, Analysis, and Response System

Course Outline

Lesson 10: Integrating with Cisco Security Manager

Overview of Cisco Security Manager Policy Table Lookup
Scenario: Invoking Cisco Security Manager Policy Table Lookup from Cisco Security MARS

Lab: Performing Cisco Security Manager Policy Lookup

Lesson 11: Managing and Administering the System

Management Overview
Overview of System Maintenance Tasks
IPS Signature Dynamic Update Settings
Upgrading the Cisco Security MARS Appliance Software
Migrating Data from Cisco Security MARS 4.3.x to 5.3.x

Lab: Reviewing the CLI and Upgrading the Device Version

Lab: Configuring IPS Auto Signature Download

Lab: Configuring AAA RADIUS Authentication, Account Locking, and Session Timeout

Lab: Retrieving Raw Messages

Lesson 12: Troubleshooting and Optimizing Cisco Security MARS

Hardware Installation Issues
Device Configuration Issues
Global Controller-to-Local Controller Communications
Sizing Cisco Security MARS Deployment
Tuning Cisco Security MARS
Securing Cisco Security MARS

Lesson 13: Using the Cisco Security MARS Global Controller

Cisco Security MARS Global Controller Overview
Configuring the Cisco Security MARS Global Controller
Summary Tab
Incidents
Queries and Reports
Rules
Management
System Maintenance



Learning
Solutions