



5051 Westheimer  
Suite 500  
Houston, Texas 77056  
(713) 871-8411  
866-88-C-TREC  
Fax (713) 622-1915

Class Code: MARS  
Number of Days: 4  
Format: Instructor-Led

## Implementing Cisco Security Monitoring, Analysis and Response System (MARS) Version 3.0

**Course Description:** The Cisco Security Monitoring Analysis and Response System (MARS), a four-day instructor-led course, is part of the Cisco Security Management Suite which provides security monitoring for network security devices and host application made by Cisco or non-Cisco providers. In addition to event correlation and data reduction features found in SIM products, CS-MARS also provides topology awareness and automatic migration features. In knowing the topology of a network, MARS can determine where the attack is originating and apply the appropriate remediation. CS-MARS is a key component in the Cisco Self Defending Network Strategy. MARS exchanges information with CS-Manager to provide a unified security management solution. For example, an administrator can view IPS signatures or the Firewall block/permit syslog messages received from sensors or firewalls. MARS will communicate with CS-Manager and display the IPS signature table or firewall rule table. From there the IPS signature or firewall rule can be modified as necessary. Together MARS and CS-Manager provide a unified management solution for monitoring and provisioning.

**Prerequisites:** The prerequisites for students attending the Cisco Certified Design Associate (CCDA) course are:

- MARS 2.0

**Delivery Method:** Instructor led, group-paced, classroom-delivery learning model with structured hands-on activities.

### Course Objectives

After taking this course, student will be able to:

- Use CS-MARS to monitor security and host application devices
- Know CS-MARS architecture and how CS-MARS process events
- Know how to use archive and restore features
- Use CS-MARS to run/create/customize reports
- Use CS-MARS to investigate an incident and mitigate the security threats
- Use CS-MARS to do customer parser for unknown devices in CS-MARS
- Use CS-MARS to create/customize rules that detects dark net through best practices example
- Know how to tune signature/log level on device side and CS-MARS side

## Course Outline

- Introducing Cisco Security Monitoring, Analysis and Response System
- Understanding the System Architecture
- Configuring a Cisco Security MARS Appliance
- Adding Reporting and Mitigation Devices
- Viewing the Summary Page
- Managing Rules
- Understanding Queries and Reports
- Investigating and Mitigating Incidents