

Course Content

The Cisco Security Monitoring Analysis and Response System (CS-MARS) 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 mitigation features. In knowing the topology of a network, CS-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. CS-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. CS-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 CS-MARS and CS-Manager provide a unified management solution for monitoring and provisioning.

Course Objectives

Upon completing this course, you will be able to meet these objectives:

- 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

Working with User-Defined Log Parser Templates

Integrating with Cisco Security Manager

Managing and Administering the System

Troubleshooting and Optimizing Cisco Security MARS

Using the Cisco Security MARS Global Controller

Course Review