



**Course Title:** Implementing Cisco Security, Monitoring, Analysis and Response System (MARS)  
**Duration:** 2 days

### Certification

This course is a part of the CCSP and completes course material for the exam **642-544 MARS**

### Objectives

After completing this course the delegate will be able to:

- Describe the Cisco Security MARS solution, features, and functions in relation to the issues of security incidents and security information in an enterprise network
- Explain the task flows that you should follow when you deploy Cisco Security MARS as an STM system in your network
- Cover the basic physical installation process of Cisco Security MARS software and hardware appliances and navigate the web-based administrator console
- Add Cisco security and network devices into the Cisco Security MARS appliance
- Add security and network devices from other vendors into the Cisco Security MARS appliance
- Discuss NetFlow and the DTM features of the Cisco Security MARS appliance
- Provide an overview of log parser templates
- Use the management features in the Cisco Security MARS appliance to assign event, addressing, service, and user information, configure hardware maintenance tasks such as viewing the audit trail, data archiving, hot swapping hard drives, and upgrading software on Cisco Security MARS appliance
- Describe the Cisco Security MARS user interface and Summary page to get an overview of the network
- Describe the case management features that can capture, combine, and preserve user-selected Cisco Security MARS data within a specialized report called a case
- Configure security devices to generate interesting events that constitute an attack scenario and have Cisco Security MARS collect the interesting events for incident investigation
- Discuss attack mitigation and false-positive confirmation in the context of the Cisco Security MARS appliance
- Configure the Cisco Security MARS appliance to perform incident investigation and attack mitigation
- Explain how to create, view and save a long-duration query and reports on the Cisco Security MARS appliance
- Configure the Cisco Security MARS appliance to send an alert
- Describe and configure a rule (or rules) that detect interesting patterns of network activity and other anomalous network behavior providing an overview of Cisco Security MARS Global Controller

### Pre-Requisites

- Cisco Certified Networking Associate (CCNA)
- Fundamental Knowledge of Implementing Network Security

### Content

- Cisco Security MARS Overview and STM Task Flow
- Cisco Security MARS Configuration
- Cisco Security MARS Incident Investigation
- Incident Investigation
- Sending Notifications
- Cisco Security MARS Rules and Management