

## Implementing Cisco SecurityMonitoring : Analysis and Response System

Duration: 2 Days Course Code: MARS

### Overview:

This 2 day hands on Instructor led course is designed to give delegates a better understanding of the Cisco Security Mitigation and Response System (CS MARS) family of high performance, scalable appliances for threat management, monitoring and mitigation, thus enabling customers to make more effective use of network and security devices by combining network intelligence, context correlation, vector analysis, anomaly detection, hotspot identification and automated mitigation capabilities. CS MARS solutions empower customers to readily and accurately identify, manage and eliminate network attacks and maintain network compliance.

### Target Audience:

Engineers who support sales of Cisco security product solutions Cisco channel partners and customers who sell, implement, and maintain secure networks

### Objectives:

- 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 informationConfigure 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 behaviorProvide an overview of Cisco Security MARS Global Controller

### Prerequisites:

All delegates should have a working knowledge of:

- Fundamental Knowledge of Implementing Network Security
- CCSP or Security CQS
- Working knowledge of Routing and Switching / CCNA

### Testing and Certification

Recommended as preparation for exam(s):

- None Specified

## Follow-on-Courses:

- NAC – Network Admission ControlCANAC – Implementing Network Appliance (Cisco Clean Access)
- 

### Content:

Cisco Security MARS Overview and STM Task Flow

- Introducing Cisco Security MARS
- Understanding STM Task Flow

Cisco Security MARS Configuration

- Configuring Reporting and Mitigation Devices
- Adding Cisco Security and Network Devices into the Cisco Security MARS Appliance
- Adding Security and Network Devices from Other Vendors into the Cisco Security MARS Appliance

Working with User Defined Log Parser Templates

- Network Summary
- Case Management
- Incident Investigation

Sending Notifications

- Cisco Security MARS Rules
  - Cisco Security MARS Management
  - System Maintenance
  - Cisco Security MARS Global Controller
- 

### Further Information:

For More information, or to book your course, please call us on 353-1-814 8200

[info@globalknowledge.ie](mailto:info@globalknowledge.ie)

[www.globalknowledge.ie](http://www.globalknowledge.ie)

Global Knowledge, 3rd Floor Jervis House, Millennium Walkway, Dublin 1