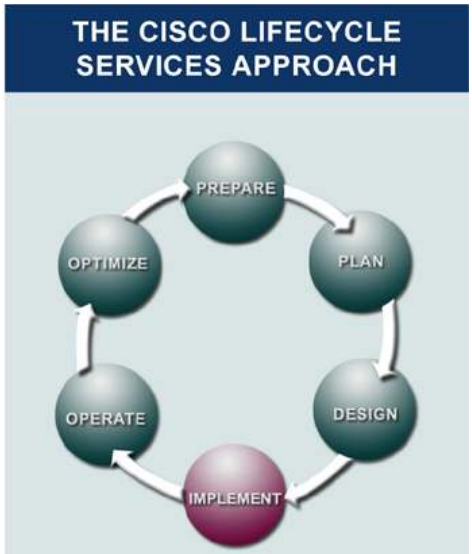
Cisco Security Monitoring, Analysis, and Response System Implementation Service



The unique Cisco lifecycle approach to services defines the requisite activities at each phase of the network lifecycle to help ensure service excellence. With a collaborative delivery methodology that joins the forces of Cisco, our skilled network of partners, and our customers, we achieve the best results.

Network Lifecycle Phases

- **Prepare**—Develop a business case for a technology investment
- **Plan**—Assess readiness to support proposed solution
- **Design**—Create a detailed design to address business and technical requirements
- **Implement**—Deploy new technology
- **Operate**—Maintain network health through day-to-day operations
- **Optimize**—Achieve operational excellence through ongoing improvements

Empowers organizations to identify, manage, and minimize network attacks and maintain compliance

Service Overview

As your business faces more sophisticated Internet attacks, information security practices must evolve from basic perimeter defenses to a defense-in-depth model, in which multiple countermeasures are layered throughout your network infrastructure. However, although multilayer defenses are necessary, they also increase the complexity of managing network security and make it more difficult to effectively identify and mitigate threats and meet compliance requirements.

The Cisco® Security Monitoring, Analysis, and Response System (MARS) is an inclusive security information management solution that synthesizes security data from the network to help your network personnel more effectively identify, manage, and counter security threats. The solution gains intelligence from the network and from security devices deployed in your network, and uses sophisticated event correlation and validation to help administrators more rapidly validate threats, subvert security incidents, and maintain compliance.

Implementing Cisco Security MARS can be a complex process. To function effectively, the solution must be carefully deployed, configured, tuned, and integrated into the network infrastructure. In addition, Cisco Security MARS uses a policy-based approach to blocking security attacks, so your organization's business and security policies must be integrated into the solution from the beginning.

The Cisco Security MARS Implementation Service, designed for large enterprises, provides the expert network analysis, planning, design, and implementation assistance your organization needs to design and deploy an effective Cisco Security MARS solution. Applying extensive practical experience, knowledge of the latest risk mitigation techniques, and specialized tools and methodologies, Cisco security experts can help your organization rapidly deploy an effective in-depth network defense that speeds attack response and resolution.

Validate Threats, Subvert Security Incidents, and Maintain Compliance

Through the Cisco Security MARS Implementation Service, Cisco security consultants help your organization deploy a solution that integrates with your existing network infrastructure, intrusion detection solutions, and endpoint security (Table 1). Employing a consistent and proven methodology for implementing the Cisco Security MARS solution, Cisco experts provide the following services to help ensure the deployment is a success:

- **Cisco Security MARS readiness assessment**—Cisco network engineers analyze Cisco Security MARS deployment requirements and assess the readiness of your network devices, operations, and architecture to support the solution. In addition to identifying components that do not support Cisco Security MARS capabilities, security engineers determine if your network topology supports a scaled deployment and deliver an impact analysis detailing requirements for redundancy, scalability, and hardware and software upgrades.
- **Cisco Security MARS limited deployment**—Cisco network security engineers install and configure a limited deployment solution, allowing your IT staff to test and gain experience with the Cisco Security MARS solution. This limited deployment can be deployed in a lab or production environment, and begins the development of system rules and reports customized to your organization's environment.
- **Cisco Security MARS design development**—Cisco consultants assist in developing a detailed design for integrating Cisco Security MARS into your network infrastructure. Working with your IT staff, design engineers develop the overall strategy and plan for the Cisco Security MARS solution, providing an in-depth analysis of the technical, procedural, and resource requirements for a corporatewide deployment. Cisco consultants also provide a design specification that defines the network topology and configuration recommendations for the Cisco Security MARS appliance, network devices, Cisco Secure Access Control System (ACS), management software, and endpoint software such as the Cisco Security Agent.
- **Cisco Security MARS implementation engineering**—The Cisco Security MARS solution must be carefully deployed, configured, and integrated into the network infrastructure, so Cisco security engineers support your organization through a customized full-scale implementation. Cisco consultants work with your IT staff to develop detailed deployment plans for installation, configuration, integration, and management. After the plans are completed, Cisco security engineers deliver onsite support for installation of the Security MARS appliance, setup of device integration, and configuration of reports and incident management. Once in production deployment, Cisco engineers assist in optimizing custom rules and reports and document all system rules and deployment procedures, including received events, false positive tuning, report configuration, alert notification procedures, and data archiving and backup and restore.

Table 1. Cisco Security Monitoring, Analysis, and Response System Implementation Activities, Methodology, and Deliverables

Activities	Methodology and Deliverables
• Analyze Cisco Security MARS deployment goals, objectives, and requirements, including requirements for integrating with existing devices, applications, and systems • Analyze the impact of integrating Cisco Security MARS with existing IT infrastructure, software operations, and security management procedures • Assess your network's readiness to deploy the solution, including the current IT infrastructure, security devices, software operations, and security management procedures • Define the architectural, topological, and functional requirements for the solution • Develop a detailed design of the system, including network diagrams, system rules and reports, and sample software configurations for protocols, policies, and features • Specify hardware and software requirements, including security management tools • Develop an implementation strategy and plan detailing the requirements for solution deployment, integration, and management • Develop the solution testing, installation, integration, management, and maintenance plans • Integrate all devices in the incident management architecture, including routers, switches, firewalls, intrusion prevention systems (IPSs), VPNs, and ACS devices, and set up logging for all reporting devices • Develop the network staging plan, detailing installation and service requirements tasks • Develop the acceptance test plan • Provide custom installation, configuration, testing, tuning, and integration of the solution in a production environment • Perform detailed system tuning and configuration of custom rules for incident management, escalation, and reporting • Optimize report generation and incident management capabilities to help ensure event information is properly analyzed and reported • Acceptance test the solution and analyze system performance and network effect • Provide practical knowledge transfer with staff about the operation and management of the system	**Methodology** • Conduct a kick-off meeting to identify the business objectives for the project, introduce the implementation team, and review major implementation tasks and milestones • Conduct a design workshop to gather business, technical, and operational requirements • Assess the readiness of the network to support Cisco Security MARS • Develop a Cisco Security MARS deployment plan • Develop a Cisco Security MARS Design Specification, including the optimal number and location of Cisco Security MARS appliances and the event monitoring architecture • Travel onsite to perform custom installation, configuration, tuning, and integration of Cisco Security MARS • Document Cisco Security MARS policies and tuning and operational procedures • Deliver maintenance and support documentation • Present an executive summary of the Cisco Security MARS implementation methodology and production deployment **Deliverables** • A Cisco Security MARS Design Specification detailing the topology, feature configuration, device integration, and system rules and report configuration • A Cisco Security MARS Rules Reference Guide documenting devices integrated into the system, device integration, custom system rules, and custom report configurations • An optimized Cisco Security MARS installation in a production environment

Benefits

With the Cisco Security MARS Implementation Service, your organization can:

- More effectively mitigate network security threats by using a sound design and implementation methodology to deploy Cisco Security MARS
- Obtain expert assistance to plan the most strategic and effective placement and configuration for Cisco Security MARS
- Accelerate deployment of Cisco Security MARS by anticipating resource and technical requirements and more effectively planning for required infrastructure changes
- Reduce your operating costs and total cost of network ownership by helping to ensure consistent deployment of security information and event management

- Enhance Cisco Security MARS performance, resiliency, and availability by using the correct set of hardware, software releases, features, and functions
- Improve staff proficiency in managing and operating the Cisco Security MARS solution through continuous knowledge exchange with Cisco experts

Why Cisco

The Cisco Security MARS Implementation Service helps you rapidly deploy a solution to mitigate the risk of network attacks, better manage security information, and aid in compliance activities. This service strengthens your team's ability to meet aggressive deployment schedules while minimizing costly disruptions to the network, and you can draw on Cisco expertise to help improve the reliability, maintainability, and performance of Cisco Security MARS. By helping to ensure the consistent deployment of Cisco Security MARS rules and procedures while strengthening the solution for efficient management and maintenance, the Cisco Lifecycle Services approach can support your efforts to reduce the total cost of ownership of your security infrastructure.

Availability and Ordering

The Cisco Security MARS Implementation Service is available through Cisco and Cisco partners globally. Details may vary by region.

For More Information

For more information about the Cisco Security MARS Implementation Service or the Cisco Lifecycle Services approach, contact your Cisco representative.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA