



CHAPTER 2

Security Threat Mitigation (STM) Task Flow Overview

A reasoned approach to employing Cisco Security Monitoring, Analysis, and Response System (MARS) requires that you firmly grasp the objectives you have in mind and the policies by which you'll accomplish them. This chapter first provides basic lists of [Policy Objectives, page 2-1](#) for security, monitoring, mitigation, and remediation and shows how they should each be considered part of a single comprehensive approach. Such a set of explicit policies acts as a comprehensive foundation and enables the application of specific measures.

The chapter then describes two project phases and task flows that you should follow when you deploy MARS as a security threat mitigation (STM) system in your network. These include:

- Provisioning (see [Checklist for Provisioning Phase, page 2-3](#)).
- Monitoring (see [Checklist for Monitoring Phase, page 2-9](#)).

Finally, this chapter concludes with a discussion of [Appliance-side Tuning Guidelines, page 2-15](#), and provides two worksheets that you can use:

- A [Device Inventory Worksheet, page 2-16](#)
- A [User Role Worksheet, page 2-18](#)

Policy Objectives

This section contains the following topics:

- [Security Policy Objectives, page 2-1](#)
- [Monitoring Policy Objectives, page 2-2](#)
- [Mitigation Policy Objectives, page 2-2](#)
- [Remediation Policy Objectives, page 2-2](#)
- [Cisco Security Wheel, page 2-3](#)

Security Policy Objectives

Your security policy should:

- Identify security objectives for your organization.
- Document the resources to protect.

- Identify the network infrastructure with current maps and inventories.
- Identify the critical resources (such as research and development, finance, and human resources) that require extra protection.

Monitoring Policy Objectives

Your monitoring policy should:

- Identify the expected administrative traffic flows across your network, including user, source, destination, services, and hours of operation.
- Identify expected network traffic for security probing and vulnerability testing, including user, source, destination, services, and hours of operation.
- Identify the network infrastructure able to provide audit data in “network proximity” to the critical resources.
- Identify the various event logging levels available from the devices and hosts in the network infrastructure.
- Identify the devices and techniques used to investigate

Mitigation Policy Objectives

Your mitigation policy should:

- Identify the choke points on your network relative to the critical resources.
- Define your process for documenting mitigated attacks on layer 2 and layer 3 devices.
- Define your process for documenting mitigated attacks at the host and application layer.
- Resolve corporate ownership issues among network operations, security operations, host owners, and application owners on shared hosts.
- Identify your policy for notifying security response teams and remediation teams.
- Identify vendor detection tool prioritization process, such as IOS IPS Dynamic Attack Mitigation (DAM).
- Identify how you want to block detected attacks: block them temporarily or permanently, block them using MARS-generated rules, using custom rules defined by security operations team, etc.

Remediation Policy Objectives

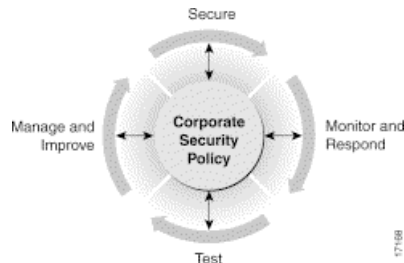
Your remediation policy should:

- Identify the responses to detected but unmitigated attacks for each type of node in your network.
- Identify tool vendor update policies to ensure proper remediation of hosts and applications.
- Identify the policies and procedures for isolating infected legacy hosts where remediation options are unavailable. These procedures may include restoring from backups or network isolation.

Cisco Security Wheel

Your policies, and the objectives they comprise, become the hub of the Cisco Security Wheel, (Figure 2-1).

Figure 2-1 Cisco Security Wheel



The spokes of the Cisco Security Wheel represent network security as a continual process consisting of four steps:

1. Secure your system.
2. Monitor the network for violations and attacks against your security policy and respond to them.
3. Test the effectiveness of the security safeguards in place.
4. Manage and improve corporate security.

You should perform all four steps continually, and you should consider each of them when you create and update your corporate security policy.

Checklist for Provisioning Phase

Provisioning deals with planning, setting up, and configuring the hardware, software, and networks that actually provide access to the data and network resources for the MARS Appliance. This phase takes place after you successfully complete the installation, which is detailed in the [Cisco Security MARS Initial Configuration and Upgrade Guide](#).

The following checklist describes the tasks required to understand the decision-making process and the basic flow required to provision MARS in the most productive manner. Each step might contain several substeps; the steps and substeps should be performed in order. The checklist contains references to the specific procedures used to perform each task.

Step 1 Inventory and review possible reporting devices, mitigation devices, and supporting devices.

- **Reporting devices**—provide logs about user and network activities as well as device status and configuration.
- **Mitigation devices**—can be used to respond to detected attacks. They also act as reporting devices.
- **Supporting devices**—provide network services to reporting devices, mitigation devices, or a MARS Appliance.

Identifying which devices on your network to monitor depends on multiple factors, including their placement, the reporting they can provide relative to other devices on the same network segment, and the level of operation that you want to achieve from your MARS Appliance.

When considering which devices to declare as reporting devices and mitigation devices, be sure you know what data is provided to MARS by those devices. Simply adding all possible devices does not guarantee the best monitoring and mitigation strategy. Deliberate selection of the devices can reduce the MARS workload, resulting in improved detection and mitigation times, as well as improved detection of false positives.

As MARS only considers monitored devices, you should take care in identifying which devices to monitor. The following are only a few examples of considerations you should make when identifying devices:

- Consider the types of logs and data available from reporting devices on specific network segments, and select those logs that provide the most complete picture of the activity on your network.
- Identify mitigation devices at natural chokepoints across each segment in your network. You are more likely to stop an attack if these mitigation devices are identified to MARS. When MARS identifies an attack, it studies the topology of your network to identify the best chokepoint; however, it only considers those devices that are monitored.
- Supporting devices can play an important role in the operation of your STM system. Therefore, you should inventory and review the supporting devices on your network, which include e-mail, AAA, DNS, and syslog servers, that will play a role in the envisioned STM system.

Result at Step Completion: The list of devices that you want to monitor is complete. The details of each device include device name, reporting IP address, management IP address, management protocol, administrative account information, and the logging features, levels, and protocols to enable.

For more information, see the following references:

1. [Selecting Devices to Monitor, page 3-2](#)
2. [Levels of Operation, page 3-1](#)
3. Deployment Planning Guidelines, in *Cisco Security MARS Initial Configuration and Upgrade Guide 6.X*.
4. [Device Inventory Worksheet, page 2-16](#)

Step 2 Identify and enable all required traffic flows.

After you identify the devices, you must verify that the network services they use for management, reporting, and notification are permitted along the required traffic flows. Using the detailed [Device Inventory Worksheet, page 2-16](#) identified in the previous task, ensure that the management, logging, and notification traffic between the MARS Appliance and each supporting device, reporting device, and mitigation device is allowed by intermediate gateways.

In addition, network services of supporting devices, such as DNS, e-mail, AAA, and NTP servers, must also be permitted to flow among the MARS Appliance, the supporting devices, and the reporting devices and mitigation devices on your network.

MARS applies the device time to received events only. For all events pulled from devices such as IDS/IPS devices or Windows, MARS uses the reported time as long as that reported time falls within 3600 seconds of the time on the MARS Appliance.



Tip

It is a recommended security practice to have all devices, including MARS Appliances, synchronized to the same time. Also, since the MARS Appliance is an HTTPS server, it uses certificates which require the time, date, and time zone to be set properly. Otherwise, sessions and incidents are stamped incorrectly and you may experience “time out” errors when accessing the web interface.

To limit troubleshooting, you should test each traffic flow from the source network segment to the destination segment. If possible, you should test all device-to-device flows for each protocol to ensure that “best match” versus “first match” semantics of various gateway ACLs do not hinder required traffic flows. As with any security devices on your network, enabled traffic flows should be restricted to the required protocols, ports, and source/destination pairs.

Result at Step Completion: You have verified that all intermediate gateways permit the log, management, and notification traffic between the devices and the MARS Appliance.

For more information, see the following references:

1. [Event Timestamps and Processing](#) in *Top Issues for the Cisco Security Monitoring, Analysis, and Response System*
2. Deployment Planning Guidelines, in [Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X](#).
3. Supporting Devices, in [Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X](#).
4. Required Traffic Flows, in [Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X](#).
5. Specify the Time Settings, in [Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X](#).
6. [Device Inventory Worksheet, page 2-16](#)

Step 3 Bootstrap the reporting devices, mitigation devices, and supporting devices.

For each device identified in the [Device Inventory Worksheet, page 2-16](#) *Device Inventory Worksheet*, you must prepare, or bootstrap, that device to ensure that the desired communications with MARS occur. Bootstrapping a device involves configuring the settings for that device, as determined by its role within the STM system. Perform the following bootstrap tasks as applicable to a device type and its role:

- Enable management of the device by the MARS Appliance for mitigation and access.
- Install an agent that collects the correct logs for MARS Appliance.
- Turn on the correct logging level and logging services.
- Direct the logs to the MARS Appliance or identify the appliance to receive or pull those logs as needed.
- Enable discovery of the device settings.
- Enable the device to receive notifications from the MARS Appliance.

Each device has a different required configuration to ensure that it assumes the role you have envisioned for it in the STM system. As you consider the devices, their expected role in your STM system will correlate directly with the configuration of the tasks listed above. In addition, you identify any restrictions imposed by MARS. For example, MARS may restrict the supported protocols for discovery of a specific device type.

Result at Step Completion: The correct logging levels are enabled on the reporting devices and mitigation devices. The MARS Appliance can receive or pull any necessary logs from those devices, and it can retrieve configuration settings and push ACLS to the supported mitigation devices. Any devices that require notification of detected attacks are configured to receive such notifications from the MARS Appliance. Although the MARS Appliance picks up and stores the events it receives, it does not inspect them until the reporting devices and mitigation devices are defined and activated in web interface.

**Tip**

Any events published by a device to MARS prior to adding and activating the device in the web interface can be queried using the reporting IP address of the device as a match criterion. This technique can be useful for verifying that the device is properly bootstrapped.

For more information, see the following references:

1. [Device Inventory Worksheet, page 2-16](#)
2. [Supported Reporting and Mitigation Devices](#)
3. Bootstrap Summary Table in the [Configuring Reporting and Mitigation Devices in MARS](#) chapter of the *Device Configuration Guide for Cisco Security MARS, Release 6.x*.
4. The log settings sections of the user guides for your reporting devices and mitigation devices

Step 4 Define the devices in MARS.

After you identify and bootstrap the reporting devices and mitigation devices and enable the required traffic flows, you must represent those devices in MARS, which uses this information to communicate with the devices. You can do this by adding individual devices in the web interface or by importing a comma separated value (CSV) file, which can define the required settings for basic device types and give you a headstart on defining the more complicated devices. In addition, you can use topology discovery to automatically discover reporting devices and mitigation devices and later go back to provide additional detail.

For most device types, you must determine what access protocol to use for device discovery. The selection of this protocol determines what type of data you can discover and whether you can perform mitigation. Understanding the options helps you develop a consistent approach in compliance with your corporate policies.

How you choose to add the devices depends on the number of devices on your network and whether there are CSV device keywords for the devices that you want to add. In addition, device types that use agents, modules, or sensors are defined in multiple steps, where you first define the base host or device, and then add the modules, sensors, and agents to the base device. For example, if you want to add an IPS module to a Cisco ASA device, you must first define the Cisco ASA device and then define the IPS module as a component of that device. In addition, many applications that are not dedicated appliances require that you first define the host (generic, Windows, Unix, or Linux) on which that application runs before you can associate the application with that host.

After you add the devices, you must activate them by clicking Activate on any page in the web interface.

To display all devices that are either added incorrectly or not activated in MARS, you can define one of two queries:

- Select “Unknown Reporting Device” in the Devices field. This query returns the events only for those devices that are reporting events that do not match one of the reporting IPs defined in MARS. When MARS receives events, it first determines whether the IP from which the events are received matches one of reporting IPs identified in the Reporting and Monitor Devices page. Only if MARS finds a match does it attempt to parse the events. Therefore, if the Reporting IP is defined incorrectly for a reporting device, the events from that device are not parsed. This query essentially identifies events that are not parsed.
- Select the “Unknown Device Event Type” in the Events field. This query returns events from known devices where, for some reason, the event is not parsed by MARS (for example, if the MARS signature list is not current with the device event lists), and it returns events reported by unknown devices.

These queries are a recommended good practice after adding the devices, especially when using a CSV seedfile or SNMP discovery. For both queries, if you are looking for a specific reporting IP address, enter that address in the Keyword field to filter the results down to those that include that IP address.

Result at Step Completion: All reporting devices and mitigation devices are defined and activated in MARS. When the devices are bootstrapped and defined in MARS, MARS begins to inspect the logs received from the devices. Until the devices are added in MARS, MARS picks up and stores the events it receives without inspecting them.

For more information, see the following references:

1. [Device Inventory Worksheet, page 2-16](#)
2. [Selecting the Access Type, page 3-10](#)
3. [Configuring Reporting and Mitigation Devices in MARS](#) chapter of *Device Configuration Guide for Cisco Security MARS, Release 6.x*.
4. [Supported Reporting and Mitigation Devices](#) (CSV Keyword column)
5. [Verifying Connectivity with the Reporting and Mitigation Devices, page 3-16](#)
6. [Activate the Reporting and Mitigation Devices, page 3-17](#)

Step 5 Configure global data collection settings and schedules in MARS.

After you add the devices, you can enable the rich data collection features of MARS, which include:

- **Dynamic vulnerability scanning.** When MARS detects an attack, it can probe the network to determine the likely success and severity of the attack. To allow this data collection in response to detected attacks, you must enable the feature and identify which networks to analyze.
- **NetFlow data collection.** NetFlow data enables MARS to identify anomalies by profiling typical data flows across your network, allowing MARS to detect day-zero attacks, including worm outbreaks. Statistical profiling takes between four days and two weeks for a MARS Appliance to complete. When the profiles are developed, MARS begins detecting anomalous traffic flows and creates incidents in response to them. To configure NetFlow data collection, you must configure those devices that can generate NetFlow traffic, and you must configure MARS to listen on a shared community string.
- **Layer 3 topology discovery.** A process-intensive operation that discovers the layer 3 network devices (that is, those devices operating at the IP layer). This layer 3 data is used to determine the attack path vector and to populate the Topology graphs. You can define the schedule for updating this information.
- **Layer 2 device discovery.** This feature allows MARS to determine the attack path vector and to identify attacking hosts and targets by MAC address, which eliminates confusion caused by attacks that spoof IP addresses. This feature is typically configured when adding a switch and enabling mitigation.

There are also several device types from which MARS periodically pulls data. For such devices, you can define the intervals at which the event logs are retrieved and processed. These update features are as follows:

- **Windows event logs.** You can set the frequency by which MARS pulls audit trail records from Windows hosts and servers. This setting is global for all such hosts and has a default value of five minutes.
- **Oracle event logs.** You can set the frequency by which MARS pulls audit trail records from Oracle database servers. This setting is global for all such servers and has a default value of five minutes.
- **Monitored device update scheduler.** You can set the frequency by which MARS pulls data from specific reporting devices, such as Qualys QualysGuard, Foundstone Foundscan, and eEye REM. Schedules are set on a per IP address basis.

After you define the settings, you must activate them by clicking **Activate** on any page in the web interface.

Result at Step Completion: The schedules for updating cached data pulled from reporting, mitigation, and supporting devices are defined and activated in MARS. After these settings are defined, MARS can probe the network or pull updates from reporting, mitigation, and supporting devices.

For more information, see the following references:

1. [Data Enabling Features, page 3-18](#)
2. *Windows Event Log Pulling Time Interval* section of the [Device Configuration Guide for Cisco Security MARS, Release 6.x](#)
3. [Layer 2 Discovery and Mitigation, page 3-19](#)
4. *Configure Interval for Pulling Oracle Event Logs* section of the [Device Configuration Guide for Cisco Security MARS, Release 6.x](#)
5. [Networks for Dynamic Vulnerability Scanning, page 3-19](#)
6. [Understanding NetFlow Anomaly Detection, page 3-20](#)
7. [Discovering Your Network: Layer 3 Topology Discovery, page 3-27](#)
8. [Scheduling Topology Updates, page 3-30](#)

Step 6 Populate vulnerability assessment information for supporting devices and network assets.

Vulnerability assessment information describes specific hosts on your network. You can detail this information for any host, whether it is a host representing a reporting device, a mitigation device, or an important asset on your network.

This information identifies the operating system, patch levels, and the network services that run on the host.

After you define the hosts, you must activate them by clicking **Activate** on any page in the web interface.

Result at Step Completion: MARS understands more about the hosts on your network and the services that they run.

For more information, see the following references:

1. [Host and Device Identification and Detail Strategies, page 3-27](#)
2. [Device Inventory Worksheet, page 2-16](#)
3. [IP Management, page 6-3](#)
4. [Service Management, page 6-8](#)

Step 7 Monitor and tune event generation and processing.

As with all monitoring applications, tuning log generation and event processing is key to technical accuracy and performance. You can use two methods to tune which events are processed by MARS:

- **Device-side tuning**—This method involves restricting event generation at the device level. MARS never receives events that are not relevant to security or device status. It also involves eliminating superfluous, duplicate data reported by multiple devices on the network, as well as eliminating those events that can be reproduced by reports or queries in MARS, such as traffic summary syslogs.
- **Appliance-side tuning**—This method involves identifying events received by the MARS Appliance that represent normal or planned network activity. You define drop rules to prevent MARS from processing such events as part of potential security incidents. When defining such drop rules, you should be as precise in the definition as possible, for example, identify the source of expected ping sweeps by an IP address within an expected time period, which is much more difficult to spoof as it requires explicit knowledge of your network and administrative practices. You can further qualify the rules using a combination of seven conditions: source, destination, service type, event type, time range, reporting device, and event severity. You must choose whether to drop the event entirely or to drop it and log it to the database, where it can be used by queries and reports.

**Note**

Drop rules do not prevent MARS from storing the event data; they simply prevent the appliance from processing the events. Events affected by drop rules can still appear a query as they are being stored on the appliance. You are still storing them; just not processing them for inspection rules. Therefore, if appliance storage considerations are an issue, we recommend using device-side tuning.

**Note**

For releases 4.2.3 and earlier of MARS, you cannot define drop rules for a NetFlow-based event. For these releases, tuning of NetFlow events must be performed on the reporting device.

Tuning is an ongoing task to improve the identification of attacks, report quality surrounding truly suspicious activities, and the overall performance and accuracy of your STM solution. It involves a detailed study of traffic, which can be conducted and refined by evaluating the events that are coming into the appliance on a device-by-device basis.

**Tip**

In a lab network environment, use a MARS Appliance to study generated events and tuning options on an individual device type basis. By documenting your requirements in a controlled environment, you can eliminate much of the production network tuning by establishing valuable device-side tuning standards for each monitoring device type.

Result at Step Completion: The events being processed by the MARS Appliance are restricted to those that provide value to the STM system.

For more information, see the following references:

1. [Appliance-side Tuning Guidelines, page 2-15](#)
2. *Configuring Logging Policies on Firewall Devices* in the [Managing Firewall Devices](#) chapter of the *User Guide for Cisco Security Manager 3.2.1*

Checklist for Monitoring Phase

After you complete the provisioning phase, you must configure MARS to help you realize your broader security goals and requirements. During the monitoring phase, your primary goal is to effectively realize your monitoring, mitigation, and remediation policies. This phase involves defining the strategies, rules, reports, and other settings required to achieve this goal.

**Note**

You must prepare MARS to closely adhere to your corporate security policy before you begin monitoring traffic flows, as you must be prepared to react to detected attacks.

The following checklist describes the tasks required to understand the decision-making process and the basic flow required to operate MARS in the most productive manner. Each step might contain several substeps; the steps and substeps should be performed in order. The checklist contains references to the specific procedures used to perform each task.

Step 1

Develop monitoring, notification, mitigation, remediation, and audit strategies.

These strategies are concerned less with desired traffic flows and generated events and focus more on what to do after MARS Appliance processes that data. These strategies are at the heart of how you will use MARS to protect your network, taking into account the short- and long-term requirements of monitoring and forensic analysis, as well as how to stop ongoing attacks and clean infected hosts. These strategies encompass not only your expected interaction with MARS, but the expectations of your reporting devices as well. Essentially, they identify the roles, tasks, and data requirements that you anticipate so that you can map events, rules, queries, and reports to those roles that provide the data required by the identified tasks.

As with any security system, we recommend that users be assigned the lowest-level privilege required to perform their job. Admin-level privileges should be reserved for administrators of the MARS Appliance.

Result at Step Completion: You have identified the users and roles required to effectively respond to detected attacks and device issues. You have defined clear guidance for responding to notifications and understand the information requirements of those such notifications and the expected format and delivery methods to be used.

For more information, see the following references:

1. [Strategies for Monitoring, Notification, Mitigation, Remediation, and Audit, page 2-14](#)
2. [Chapter 10, “Case Management”s](#)
3. [User Management, page 6-11](#)
4. [Promoting Global User Roles on Local Controller, page 6-16](#)
5. [User Role Worksheet, page 2-18](#)

Step 2 Define the notification services.

This task prepares the notification services of MARS to notify your mitigation and remediation personnel and take other required actions. In MARS, notification services have three building blocks:

- **User accounts**—Represent users who will receive reports or notifications or who will access the web interface for the purpose of monitoring or mitigation. Users can receive notifications in the form of e-mail, pager messages, or Short Message Service (SMS) messages. Users are assigned to one of four roles, admin, security analyst, operator, notification only, which determines their access privileges in the web interface.
- **Devices**—Represent those devices that will receive notifications in the form of an SNMP message, a syslog message, or in the case of an IOS IPS device, a DAM message (equivalent to a shun). For more on defining devices, refer to [Checklist for Provisioning Phase, page 2-3](#).
- **Actions**—Actions are defined within inspection rules, and they represent the notifying action. Depending on the target of the notification, a user or a device, your action can provide guidance to your staff or instruct your devices to log or block an attack.

Within MARS, any person or device that is expected to receive a notification must be identified in the system. Therefore, the first step is to define user accounts that map to the users or groups who must be notified based on specific event settings (see [User Role Worksheet, page 2-18](#)). You must also identify the devices that need to be notified or that need to take some action (see [Device Inventory Worksheet, page 2-16](#)).

The next step is to define the notification service settings (actions), which can be one or more of e-mail, page, SMS, SNMP, Syslog, or Dynamic Attack Mitigation. Each of these settings includes the contact information and a message that you can define for each type of notification.

There is not a separate interface for defining these settings. To define the notification service settings, you must edit an existing inspection rule and add new Action definitions. After you define these settings, they are available to all inspection rules.

Result at Step Completion: All required personnel have been identified in MARS so that rules and reports can be customized to notify the correct personnel.

For more information, see the following references:

1. [User Management, page 6-11](#)
2. [Adding or Removing a User from a Custom User Group, page 6-15](#)
3. [IP Management, page 6-3](#)
4. “Adding Reporting and Mitigation Devices” found in the [Configuring Reporting and Mitigation Devices in MARS](#) chapter of *Device Configuration Guide for Cisco Security MARS, Release 6.x*
5. [Forwarding Alert Data to 3rd -Party Syslog and SNMP Servers, page 3-39](#)
6. [MARS MIB Format, page 3-42](#)
7. [Inspection Rules, page 4-4](#)
8. [Working with System and User Inspection Rules, page 4-14](#)
9. [Setting Alerts, page 4-21](#)
10. [Chapter 5, “Alerts and Incident Notifications”](#)

Step 3 Define custom inspection rules and refine system inspection rules.

Inspection rules correlate events from disparate devices into meaningful sessions that reflect the end-to-end activities of an attack or other network session. By identifying the end-to-end view of attacks, MARS is better able to identify mitigation points in your network. However, you can define inspection rules to accomplish different goals: identification of an attack is just one possible goal. Other example goals might include identifying use of priority assets, assessing network health, or refining your network configuration based on usage analysis.

MARS ships with over 100 system inspection rules; however, you may find that you cannot identify those sessions that are important to your corporate policies. For example, if you want to monitor the use of a custom or unsupported application, you can either define a new inspection rule that monitors traffic between a selected source and destination using a known protocol and port pair, or define a custom log parser that uniquely processes the events generated by that application to expose the data within the event that you want to track. Monitoring a known protocol port pair can provide summary data, such as number of sessions, where a custom log parser can enable detailed inspection of aspects of the traffic, such as resource utilization or failed logging attempts. To define a custom parser, you must know the message format used by that appliance, and it must be published to MARS in clear text.

Organizing the rules that you create into meaningful groups helps clarify your purpose and improve the learnability of the system. As you consider your specific goals, you should define a rule group (and a corresponding report group) to help you refine the strategies you identified in [Step 1](#), above. Because rules can be members of multiple groups, you do not have to worry about creating multiple rules to address the same issue. The groups are merely available to help you organize your work and allow you to focus on one strategy at a time.

Result at Step Completion: Any custom inspection rules are developed and existing inspection rules are configured to provide proper notification in compliance with your corporate policies. Any custom log parser and inspection rules are defined that enable the audit of the traffic flows of home-grown or unsupported applications or protocols.

For more information, see the following references:

1. [Rule and Report Groups, page 4-22](#)
2. [Event Management, page 6-2](#)
3. [IP Management, page 6-3](#)

4. [Service Management, page 6-8](#)
5. [User Management, page 6-11](#)
6. [Inspection Rules, page 4-4](#)
7. [Working with System and User Inspection Rules, page 4-14](#)
8. [Setting Alerts, page 4-21](#)
9. [Chapter 5, “Alerts and Incident Notifications”](#)

Step 4 Define custom queries and reports.

Queries and reports are forensic analysis tools. They help you analyze historical data and enable you to identify trends over longer periods of time than the real-time monitoring features of MARS. The relationship between queries and reports is essentially that queries are on-demand, refined inspections of data as defined by a report template. Reports are scheduled to run periodically, enabling you to define the periods and frequencies that you want to inspect on an ongoing basis. Queries allow you to narrow or broaden your search based on a report template by filtering the search criteria. While MARS provides many predefined report templates, you can define new report templates that focus on the incidents and events important to fulfilling your policies. This feature can be especially useful for adhering to compliance reporting requirements, as you can define a report, schedule it to be generated, and store the results as part of your audit records.

As with overall access, you can restrict the ability to run or view reports and queries based on user role. Such safeguards can reduce accidental tampering with schedule reports by other users of the system. In addition, you can configure your report templates so that users are notified of the report. Typically, e-mail is the primary method used for report notification, but all notification methods are supported.

Result at Step Completion: The report templates required to realize your forensic analysis and audit goals are defined and assigned to user roles according to your least privilege policies. Any report groups that facilitate access or division of reports and queries among your staff are defined.

For more information, see the following references:

1. [Chapter 8, “Queries and Reports”](#)
2. [Select Query Criteria, page 8-7](#)
3. [Batch Query Operations, page 8-14](#)
4. [Reports, page 8-26](#)
5. [Report Creation, page 8-29](#)

Step 5 Monitor network and security activity.

This task encompasses monitoring your network for attacks or issues and responding to them. How users interact with MARS depends on their role and your organization’s operational guidelines. For users who are expected to use the web interface to monitor traffic in near real-time, this task requires an in-depth understanding of the data that is correlated and displayed, as well as when and how to respond to suspicious or anomalous behavior.

MARS provides two interfaces to network and security activity: the Summary tab and the Query/Reports tab. Each interface provides different views and tools to help you understand what is happening on your network.

The Summary tab focuses on near real-time events, whereas the Query/Reports tab focuses on historical, forensic analysis as described in the next task of this checklist. The Summary tab organizes priority views of your network activity, displaying hot spot diagrams, recent events, charts of incidents, and a topology diagram, identifying recent activities.

When you identify an incident that requires further investigation or mitigation, you can investigate the incident to determine whether it is a false positive or block attack using MARS. If you have choke points operating at layer 2, primarily switches, MARS will identify the appropriate device, provide recommended CLI changes, and allow you to push these changes to the device. If the choke point is a layer 3 device, MARS recommends CLI changes that you can copy and paste into an administrative session with the identified choke point.

In this manner, you can monitor your network for suspicious behavior and respond to any detections.

Result at Step Completion: Users understand the views and tools required to monitor, verify, and mitigate attacks on the network.

For more information, see the following references:

1. [Chapter 7, “Network Summary”](#)
2. [Chapter 9, “Incident Investigation and Mitigation”](#)
3. [False Positive Confirmation, page 9-7](#)
4. [Rule and Report Groups, page 4-22](#)
5. [Using Event Groups, page 6-2](#)
6. [Chapter 10, “Case Management”](#)
7. [The False Positive Page, page 9-9](#)
8. [Retrieving Raw Messages, page 13-3](#)

Step 6 Monitor system and network health.

The STM system is more than your MARS Appliance; it includes all reporting devices and mitigation devices and any MARS Appliances. When assessing the health of the system, you should monitor the health of each of these devices. You can monitor your system health by using inspection rules that generate notifications for anomalous behavior, by generating system health queries and reports, and by manually reviewing the system logs of MARS.

MARS provides reports about use of common resources, including CPU, bandwidth, and memory. To simplify the monitoring of system health, you can define a report group that organizes these reports into a meaningful collection. You can also restrict the presentation of those reports and queries to specific user roles.

Because reports can be scheduled, you can notify the appropriate users each time the report is updated.



Tip

If you cannot view the resource usage of a reporting device, verify that you have enabled the Monitor Resource Usage option as part of that device definition in Admin > System Configuration > Security and Monitored Devices. For the list of devices that can be configured to provide this data, see [Configuring Device Resource Usage Data, page 3-32](#).

MARS also includes detailed logs about the status of the appliance itself, as well as several command-line utilities that present status on the health of the appliance.

Result at Step Completion: The users responsible for monitoring the system and network health understand the tools and reports provided by MARS to perform these functions.

For more information, see the following references:

1. [Rule and Report Groups, page 4-22](#)
2. [Rule and Report Group Overview, page 4-22](#)
3. [Configuring Device Resource Usage Data, page 3-32](#)

4. *pnstatus* command in [Cisco Security MARS Command Reference, 6.X](#)
5. *pnlog* command in [Cisco Security MARS Command Reference, 6.X](#)
6. [Setting Runtime Logging Levels, page 13-1](#)
7. [Viewing the MARS Backend Log Files, page 13-2](#)
8. [Viewing the Audit Trail, page 13-2](#)
9. [Retrieving Raw Messages, page 13-3](#)

Step 7 Tune MARS processing.

Tuning, which is an ongoing activity for any monitoring application, involves refining the sensitivity and accuracy of event processing. In MARS, you can do any of the following to effect such changes:

- Use drop rules to enable or disable the processing of events by MARS.



Note For releases 4.2.3 and earlier of MARS, you cannot define drop rules for a NetFlow-based event. For these releases, tuning of NetFlow events must be performed on the reporting device.

- Turn on or off event generation at the device.
- Identify selected incidents as false positives.
- Tune inspection rules to include or exclude specific networks, hosts, services, reporting devices, or traffic flows.
- Tune the inspection of traffic by device type, such as IPS and IDS, refining the rule set they use to generate events.
- Add or remove reporting devices to alter the reported event set or to provide supporting data that can be used to improve the self-tuning features of MARS, such as false positives, OS fingerprinting, and vulnerability assessment.
- Describe the expected behavior on your network by describing the assets, services, and vulnerability assessment information. The more details MARS knows about your network, the better it can assess the incoming events.

Result at Step Completion: The events being processed by the MARS Appliance are restricted or expanded to encompass those that provide the most value to the STM system.

For more information, see the following references:

1. [Appliance-side Tuning Guidelines, page 2-15](#)
 2. [Working with Drop Rules, page 4-18](#)
 3. [False Positive Confirmation, page 9-7](#)
 4. [Selecting Devices to Monitor, page 3-2](#)
-

Strategies for Monitoring, Notification, Mitigation, Remediation, and Audit

STM requires the close coordination of multiple strategies in support of your corporate security policies:

- Monitoring involves the study of network activities and device status to identify anomalous activities or behavior.
- Notification involves alerting those parties responsible for responding to detected anomalies with the information necessary to respond.
- Mitigation involves responding to suspicious activity to prevent the spread of anomalies across your network.
- Remediation involves responding to successful exploits to clean infected hosts on your network.
- Audit involves logging and reporting activities that have taken place during other tasks. The goal of audit is to provide an account the activities and responses to support compliance audits and trend analysis.

The first decision you must make is who will be responsible for mitigation at the selected choke points. Often, organizations separate specialized security devices from the core network infrastructure devices along organizational divisions. As an example, two separate teams, security operations and network operations, may be responsible for different network components or different policies on shared devices. Before you roll MARS out on your network, ownership of a strategies for mitigation must be clearly defined in according with your corporate policies.

When it comes to a mitigation strategy, two options exist:

- You can rely on MARS to identify the choke point and accept the recommended CLI changes to block the detected attack.
- You can issue notifications and incident details to a responsible party who can evaluate the MARS recommendations, but ultimately that party will make the final decision about where and how to stop the detected attack.

Regardless of the option you choose, you should develop guidelines on how long an attack should be blocked, how to investigate an internal attack so that you can clean them, who is responsible for updating the policies after the required quarantine period, and how records of such events should be maintained for audit compliance (for example, is the case management feature of MARS tied to your ticket integration system?).

Next, you should make a distinction in the type of monitoring that you should perform: system monitoring versus security monitoring. *System monitoring* involves monitoring not only the status of the MARS Appliance but also the health and status of the reporting devices and mitigation devices that MARS manages. *Security monitoring* focuses on network and security activity.

For both types of monitoring, you must decide what predefined and custom queries and reports are required, the processes for evaluating and responding to the data they reveal, and guidelines on using the case management features of MARS to manage the responses and track changes.

The last phase involves determining who should be notified when specific incidents are detected. For example, who is notified of device status incidents versus security-related incidents. You must identify your mitigation and remediation personnel, identify those responsible for monitoring (across organizations if necessary), and determine how notifications are to be generated and what they should look like. This involves selecting among methods, including SMS, pager alert, and e-mail, as well as whether the notifications are based on incidents, queries, or reports.

Appliance-side Tuning Guidelines

Tuning on the MARS Appliance focuses on not inspecting traffic that is received from the reporting devices. Two primary techniques exist for appliance-side tuning:

- **Drop rules**—This technique involves dropping all events that match specific criteria received from a reporting device. This technique is the fastest and the least refined. As part of defining a drop rule, you can also specify whether to retain the event log in or simply discard it. The advantage of drop rules is that they events are not processed by any inspection rules, which speeds up the processing of the appliance by reducing the potential workload.



Note For releases 4.2.3 and earlier of MARS, you cannot define drop rules for a NetFlow-based event. For these releases, tuning of NetFlow events must be performed on the reporting device.

- **Removing devices from inspection**—This technique involves removing a device from inspection rules. This technique is specific to the events that trigger a specific type of alarm. The advantage of this technique is that it does not drop all events that match specific criteria received from a reporting device. In other words, your focus is on reducing a specific false positive rather than all incidents that are fired based on the events. In addition, the events are retained so that you can review them using queries and reports.

When using either of these techniques, remember that when you add or modify a rule, you must click Activate before the changes take effect.

Device Inventory Worksheet

The device inventory worksheet will help you collect the required information about the devices on your network. It includes the following information:

- **Device name**—Identifies the well-known name of the device. Typically, this name is the DNS name of the device. MARS uses this name in the topology graph, reports, and events.
- **Reporting IP address**—Identifies the IP address assigned to the network interface from which MARS will be receiving events. This address is used by MARS to map back to the device name and to uniquely identify messages and events originating from the device.
- **Management IP address**—Identifies the IP address assigned to the network interface to which MARS connects to discover the configuration settings for the device.
- **Username/password**—Identifies the account that has the correct authorization to connect to the management IP address and read or write information based on the role in the network. For reporting devices, this account must have privileges sufficient for MARS to read the existing configuration. For mitigation devices, specifically layer 2 switches, this account can enable MARS to publish actual CLI changes to the device to block detected attacks.
- **Role in system/segment**—Identifies whether this device is a reporting device or a mitigation device. It can also identify supporting devices, such as DNS and e-mail servers. In addition, the role should take into account this device's expected importance relative to the network segment, specifically relative to the other devices on the same segment. You can qualify this segment-level role using terms that fit your overall monitoring strategy, such as primary source, second opinion, attack identification, false positive assessment, session data, and endpoint/MAC address identification. Understanding the role that a device can or should play at a network segment level helps prioritize the required and tunable log settings.
- **Required protocols**—Identifies the protocols that this device uses to operate. The primary focus is on the management protocols, notification protocols, and protocols used to publish audit events.

