
REM Operations Guide

The Security Operator Reference Guide

Using your REM System to Secure Your Environment

eEye Digital Security



eEye Digital Security®

Warranty

This document is supplied on an "as is" basis with no warranty and no support.

Limitations of Liability

In no event shall eEye Digital Security be liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained in this document is subject to change without notice.

No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this user guide.

Disclaimer

All brand names and product names used in this document are trademarks, registered trademarks, or trade names of their respective holders. eEye Digital Security is not associated with any other vendors or products mentioned in this document.

This document contains information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of eEye Digital Security.



Preface

eEye Digital Security offers complete enterprise solutions for network vulnerability assessment and remediation, protection against threats and attacks, and data mining and forensics. An enterprise suite may consist of the *Retina Network Security Scanner*, *SecurellS*, or *Blink*, as well as the *REM Security Management Console and Iris*. This user's guide describes the REM components and how they fit into an eEye Digital Security enterprise solution, and offers instructions of how to use the most salient features of REM.

Intended Readers

This guide is intended for network security administrators and managers who are familiar with security concepts, and who have experience in performing administrative tasks.

Assumptions

This guide operates under the following assumptions:

- MS SQL Server has been successfully installed and configured on the same machine on which REM Events Server will be installed, and an instance of a REM database has been created.
- The reader of this guide has the necessary access privileges to perform the tasks described herein.

Conventions Used in this Manual

The following list shows typographic and usage conventions of this guide:

Bold	Bold text represents commands, interface buttons, and dialog names, except when they appear in window examples or the contents of files.
Blue	Blue text indicates a hypertext link to a topic within the manual or a web site.
Monospace	Monospace text represents context specific values including Windows NT path names.
Character underline	Character underline represents the shortcut key or key combination you can press as a command to cause the specified function to occur. For example, if the command is Add Rule , you can press the letter A on your keyboard to display the wizard that you can use to add a rule.

Also, the eEye Digital Security Console is referred to as the eEye Console in this manual.

Related Documents

For additional information regarding REM and other eEye Enterprise Suite components, refer to these documents:

- eEye Retina Design Guide
- eEye Retina User Guide
- eEye Retina Operations Guide
- EVA Product Demonstration Guide
- REM Administration Guide
- REM Management Guide
- REM Deployment Guide
- REM Development Guide
- EVA Installation Guide
- Blink User's Guide
- SecureIIS User's Guide

Additional Resources

eEye Digital Security support may be contacted at 1-866-339-3732 or through this URL:

<http://www.eeye.com/html/Support/Request/index.html>

The eEye Digital Security web site also includes access to forums, live seminars, white papers, as well as an option to subscribe to the eEye Newsletter.



Contents

Preface.....	i
Intended Readers	i
Assumptions.....	i
Conventions Used in this Manual.....	i
Related Documents.....	ii
Additional Resources.....	ii
Introduction	1
REM™ Security Management.....	1
REM Events Server	2
REM™ Events Manager	2
REM Event Client	2
Architectural Overview.....	2
Procedural Overview	3
Getting Started	4
Deployment	4
Operations	4
Management	5
Administration	5
Development.....	5
Overview of REM Events Manager.....	6
Basic Concepts	6
Object Descriptions.....	6
Main Object	7
Threat Management Portal Details	8
Events	10
View Events	11
Search Events	11
Purge Events.....	11
Tasks	12
Reports.....	12
View Reports.....	12

Manage Reports	13
Manage Report Categories	13
Policies	14
Manage Audits	14
Manage Ports	16
Manage Addresses.....	16
Manage Options	17
Manage Jobs	17
Applications	17
Manage Applications	18
Manage Application Categories	18
Rules	19
Users.....	19
Manage Users	19
Manage Scopes	19
Manage User Groups	19
Options.....	20
Viewing and Managing Assets	21
What is an Asset?	21
Examples	21
Viewing and Managing Events	21
What is an Event?.....	21
Blink Enterprise Intrusion Prevention.....	21
Retina Network Security Scanner	22
SecureIIS Web Server Protection	22
Iris Network Traffic Analyzer.....	22
Viewing Events.....	22
Logging into the REM Events Manager	22
Events for Last Thirty Days.....	23
Viewing Events of the Same Severity Level	23
Viewing Event Details	24
Viewing All Events	25
Searching for Events.....	25
Viewing Events of the Same Severity Level.....	25
Assigning and Managing Tasks.....	27
What is a Task?.....	27
Elevating an Event to a Task.....	27
Viewing Tasks	29
Viewing Tasks of the Same Severity Level.....	29
Viewing Task Details	30
Viewing Tasks using the Tasks Object.....	30
Rules	31
Exercise.....	32
Exercise	32
Reports	34
Accessing and Generating Reports	34

Generating a Report	34
Task Reports.....	35
Additional Reports.....	36
Advanced Concepts	37
Policies	37
Manage Audits	37
Modifying an Audit.....	39
Creating an Audit.....	39
Modifying Ports	39
Creating Port Groups	40
Manage Addresses.....	40
Modifying or Deleting Addresses	41
Manage Options	41
Manage Jobs.....	41
Applications.....	41



Introduction

With the explosive growth of e-commerce, online operations, and international connectivity, enterprises have recognized that security processes and the protection of intellectual property are vital components for continued success. Most companies have adopted security policies, and have implemented various technologies to prevent fraud, vandalism, sabotage, and denial of service attacks. Some of the defenses against an attack on networks include firewalls and Intrusion Detection Services (IDS). However, these traditional defenses characteristically have limitations.

For example, a firewall may only stop a packet based on predefined criteria, such as TCP flags, IP addresses, or TCP and UDP ports. Additionally, some firewalls only take into account the packet information contained in headers, and ignore the data within the packets themselves. Finally, because the most common IDS are signature based, only those attacks which the IDS has been programmed to detect will be stopped.

These limitations, however, do not suggest that the traditional defenses ought to be replaced. Rather, eEye Digital Security, with its enterprise solutions, proposes to complement, and not replace, firewalls and IDS. The key to the eEye Digital Security approach is being proactive as opposed to being reactive.

REM™ Security Management

In the past, IT Security Managers may have had a considerable amount of time, possibly months, to remediate against known vulnerabilities in their networks. However, as e-commerce and online computing have become more sophisticated and complex, so too have hackers and cyber-vandals. Today, the remediation window has decreased dramatically, and IT Security personnel often must scramble in response to vulnerabilities, threats, and attacks.

The REM Security Management Platform, when deployed with any of eEye's enterprise solutions, enables network security managers to:

- Create an inventory of all assets.
- Audit the assets and evaluate results of the audit.
- Delegate tasks and, if necessary, remediate against vulnerabilities.
- Generate Reports.
- Perform a risk analysis.

With the REM Security Management Platform, network security personnel are able to plan, audit, assign tasks, remediate, and generate reports from a centralized location.

The REM Security Management Platform consists of the Events Server, the Events Manager, and the REM Event Client. These REM components centralize the management, remediation and prevention of vulnerabilities, threats and attacks.

REM Events Server

The REM™ Events Server provides a secure virtual network for transferring predefined security events from eEye product engines, such as Retina, Blink, or SecureIIS. These eEye engines are deployed on remote machines across an enterprise to a centralized SQL database. The REM Events Server is scalable to transfer large amounts of data, and functions as a hub between the REM database and REM Event Clients. Each event created by an REM Event Client is sent via a secured connection to the REM Event Server, which in turn processes the event and inserts it into the REM database.

REM™ Events Manager

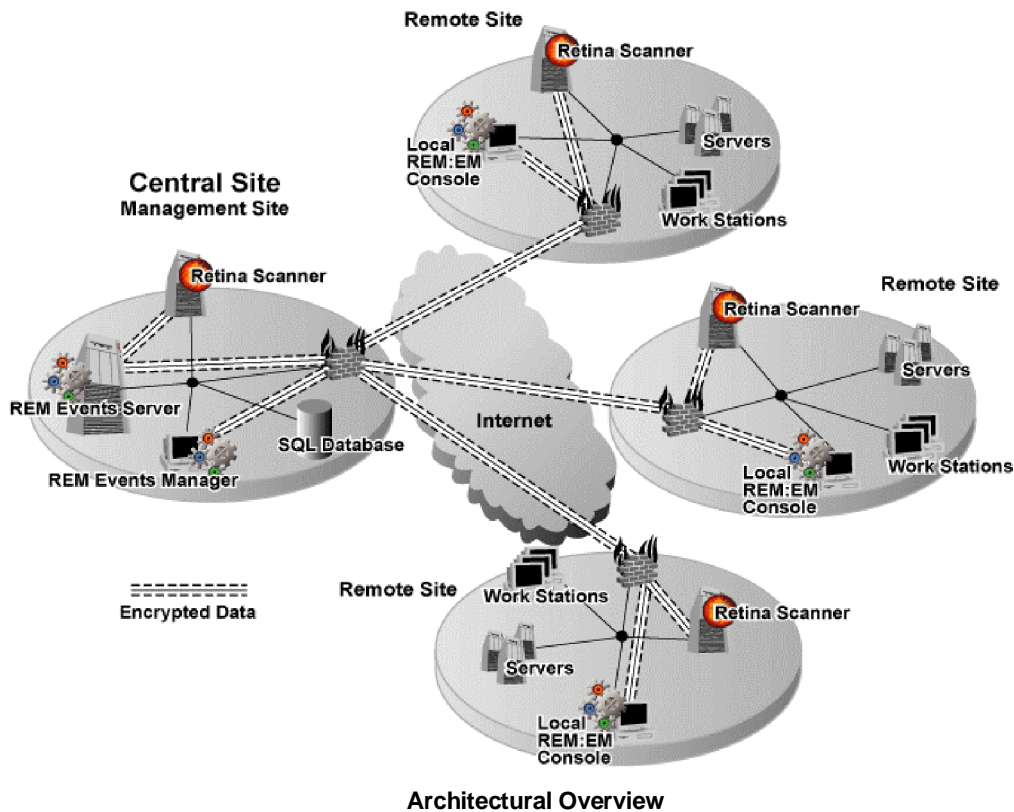
The REM Events Manager, a web-based interface, is a consolidated enterprise-level command center for monitoring, administering, and reporting on all eEye engines. The Events Manager provides diagnostics data that enables IT personnel to proactively identify vulnerabilities and threats, and quickly resolve them across the entire enterprise. The interface also includes a number of useful reporting options that may be customized for specific organizational needs.

REM Event Client

The REM Event Client functions as a bridge between the REM Event Server and other eEye products. It accepts REM messages, and securely relays them to the REM Event Server.

Architectural Overview

In a typical enterprise implementation, multiple eEye engines (such as the Retina Scanner, Blink, or SecureIIS) are installed at various remote sites. In turn, each remote site would include a REM Events Manager, and the REM Events Client would be installed on each work station connected to the LAN at the site. The Retina Scanner at each site scans all work stations and servers, and the resulting data is securely transferred to the REM Events Server at the central site via the REM Events Client. The central site will also include a Retina Scanner, an REM Events Manager, and the SQL Database where the transferred data is stored. The illustration below illustrates the typical enterprise implementation.



Procedural Overview

Vulnerabilities and threats are most likely to be discovered in the following:

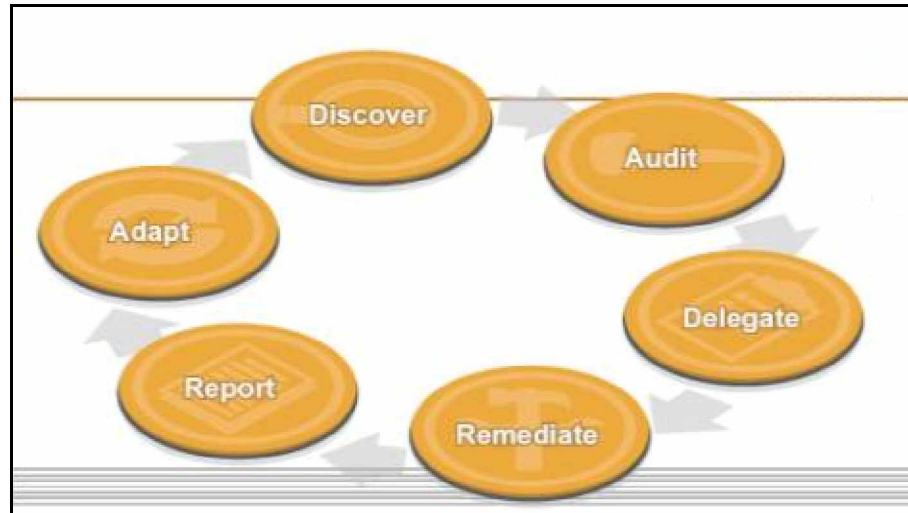
- New Operating Systems
- New Applications
- New Hardware
- Improperly configured systems or network devices.

Even though manufacturers and vendors may provide patches, service packs, or PROM flashes to address vulnerabilities or security threats, the window of opportunity for remediation is decreasing dramatically. Additionally, not all vulnerabilities are known. IT personnel must take a proactive stance against vulnerabilities and security threats. As such, an eEye Digital Security Enterprise solution, comprised of an eEye engine and REM, offers tools to accomplish the following tasks:

- **Audit and Discover**
During this phase, the IT Security Manager makes an inventory of devices and services. With a completed inventory, vulnerabilities are more readily discovered and assessed. Finally, a means of sending alerts and notifications can be established.
- **Delegation and Remediation**
In this phase of the process, incidents are assessed and given an identification number, resources are allocated, and tasks are assigned to the appropriate personnel. Alternatively, through the implementation of rules, tasks may be automatically assigned or remediation may be automated. Finally, a rule may be implemented to verify remediation.
- **Analysis and Adaptation**

Here, IT administrator and managers may generate reports and analyze data. If personnel notice certain security and vulnerability trends, they may implement new policies or modify existing policies and thus manage resources more efficiently.

The following diagram illustrates a model of the network security management processes:



Procedural Overview

In the above illustration, network security managers are able to determine which assets are running which applications. Additionally, the managers are able to identify areas of high risk, and consequently they may more effectively allocate resources to those areas and assign tasks. Finally, network security managers can more efficiently control the remediation process as the progress of initiatives are tracked and areas of non-compliance of security policies are readily identified.

Getting Started

The previous sections provided a glimpse into the REM Security Management Platform, and how it fits into the eEye approach to providing enterprise security solutions. The deployment, operations, and management of the REM Security Management Platform consist of various steps. eEye Digital Security provides reference material to assist users, managers, and developers in each step.

Deployment

This first step involves the assessment of the environment within an enterprise, and the installation and configuration of REM. The purpose of this step is to address all of the issues for a first-time installation and configuration, so that the enterprise is up and running as quickly as possible. The step is discussed fully in the *REM Deployment Guide*.

Operations

After REM has been successfully installed and configured, users should be able to utilize the REM Event Manager in an efficient manner. There will be basic tasks that the user will perform on a daily basis. The procedures for completing these tasks are described in the *REM Operations Guide*.

Management

As is often the case, needs and environments within an enterprise change. For example, new employees may require access to REM, or the roles and duties of current employees may change. Furthermore, assets within the enterprise may be added or reconfigured. To address these changes, REM includes a variety of management tools. These are explained in detail in the *REM Management Guide*, which is intended for network security managers and administrators.

Administration

At this point, the installation, configuration, and basic management of a REM Deployment have been addressed by the previous steps. However, it is critical to maximize the returns from the investment in a network security solution. For example, a network security manager may need to implement a system of metrics to gauge system performance. In addition, a manager may want to evaluate employee performance. Finally, tasks such as performing backups or generating reports may need to be done on a routine basis. These administrative tasks are discussed in the *REM Administration Guide*.

Development

In many cases, it may be necessary to automate certain operations, or to integrate with existing applications. The *REM Development Guide* provides instructions to developers and programmers on how to integrate with third-party applications, and how to automate certain processes.

Overview of REM Events Manager

This chapter provides an overview of the Web-based REM Events Manager, which allows for enterprise-wide management and remediation of network vulnerabilities, attacks, and threats. Because this chapter is an overview, all of the objects in the web interface are described. However, it should be noted that some users will not have access or see some of the objects described. Only users with full access, generally those with Administrator privileges, will see all of the objects.

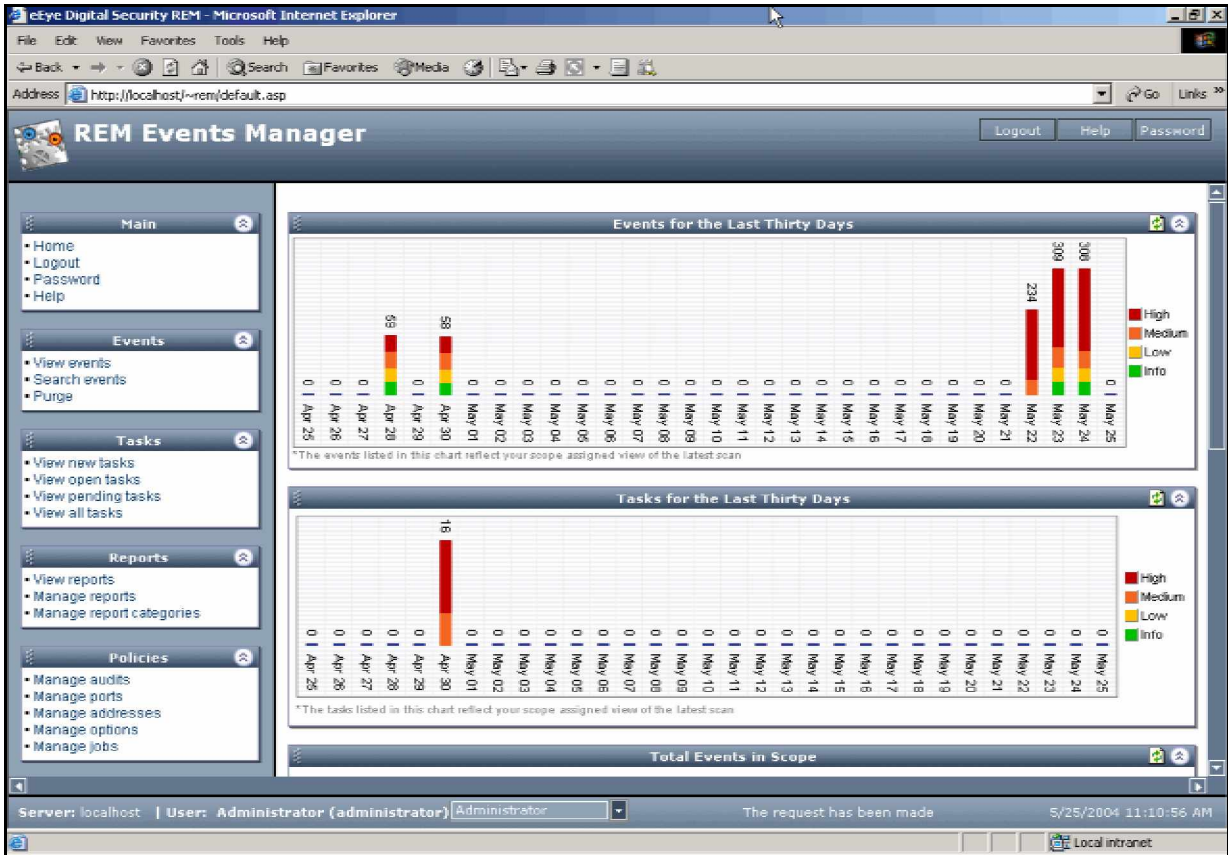
Basic Concepts

The REM Events Manager operates independently from any one specific eEye Digital Security engine. The Events Manager receives data from any one of the eEye engines, including SecurellS, Blink, and Retina. The Event Manager, in turn, classifies the data it receives as an “event,” which the network security manager, or other authorized user, is able to assess, manage, and remediate.

As a result, and by design, the Event Manager serves as a threat management portal because it consolidates all events, regardless of the source (Blink, SecurellS, Retina), and enables the network security manager to plan, implement, and review remediation activities. As a “Threat Management Portal,” the Events Manager displays critical information regarding the current state of network security in an enterprise. Specific features and functions of the Event Manager are discussed later in this document.



Object Descriptions

After an authorized user logs into the Events Manager, the Home page, also referred to as a Threat Management Portal, opens in a web browser. The view for a user will vary, depending on the permissions granted and the user group to which the user belongs. For the purposes of discussion, the view shown in the **following figure** is based on a user who has complete access. Users and User Groups are discussed later in this chapter, and specific details are provided in the *REM Management Guide*.



Events Manager Threat Management Portal

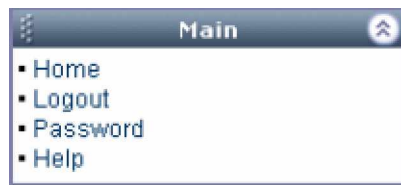
The left portion of the Threat Management Portal are objects that contain links to information that is displayed in the main window of the browser, which also contains links and objects.

Objects can be expanded or collapsed by clicking on the down arrow  or up arrow , respectively.

Descriptions and functionality of the objects are described in the following sections.

Main Object

This object contains the default page for the Events Manager, also referred to as the Threat Management Portal, when it initially opens. The Main object also has access to the Online Help, Password change options, and logging out.



Events Manager Object

Clicking **Home** returns the user to the Threat Management Portal. Note that Logout, Password, and Help may also be accessed in the upper right of the browser.



Logout, Help, and Password

Threat Management Portal Details

The Threat Management Portal displays important information regarding events and tasks within a range of IP addresses on a network. This information provides a snapshot of the network security. Note that not all users will have the same view of the Threat Management Portal.

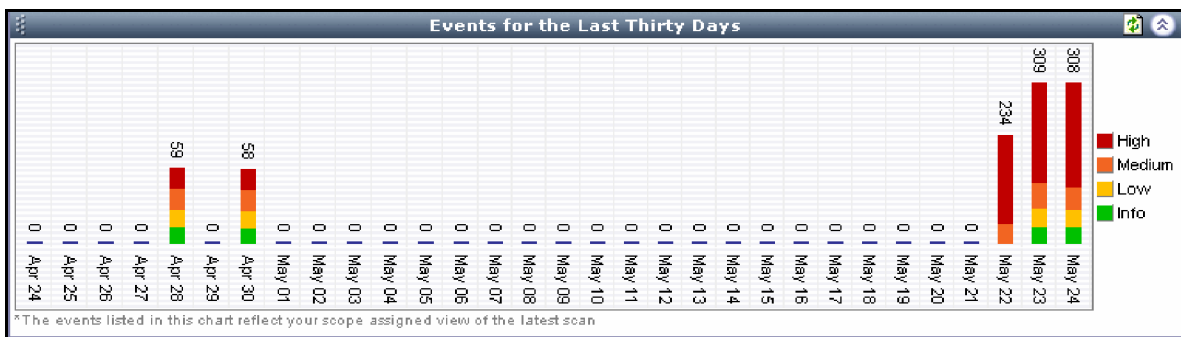
Events and tasks are color-coded to indicate the severity level, with **Red** = “High,” **Orange** = “Medium,” **Yellow** = “Low,” and **Green** = “Informational.”






REM Color Codes

The information contained within separate objects on the Home page are as follows:

- Events for Last 30 Days



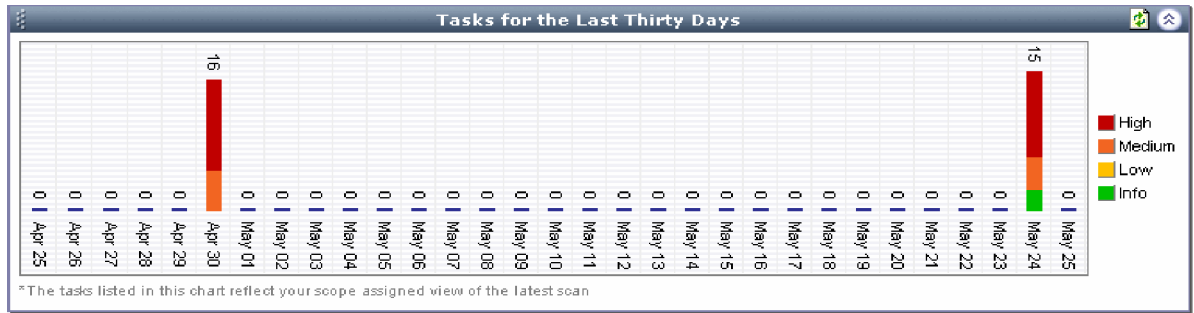
Events for Last 30 Days

The source of the events displayed here can be Retina, SecureIIS, or Blink. Also, note that events are displayed with corresponding, color-coded severity levels to aid in identifying and assessing the event. As with other objects, this graph may be collapsed, expanded, or refreshed by clicking on   or 

- Tasks for Last 30 Days

The information displayed here is in reference to events that have been assigned to a user or a group within the last 30 days.

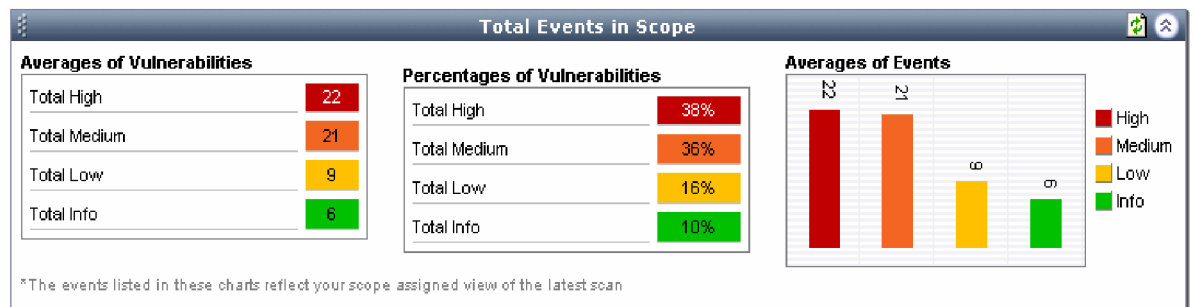
Tasks for Last 30 Days



- Total Events in Scope

The information displayed here provides a count of the total number of events within the scope to which the given user has access. A scope is, in its simplest terms, a collection of IP addresses on the network.

Total Events in Scope

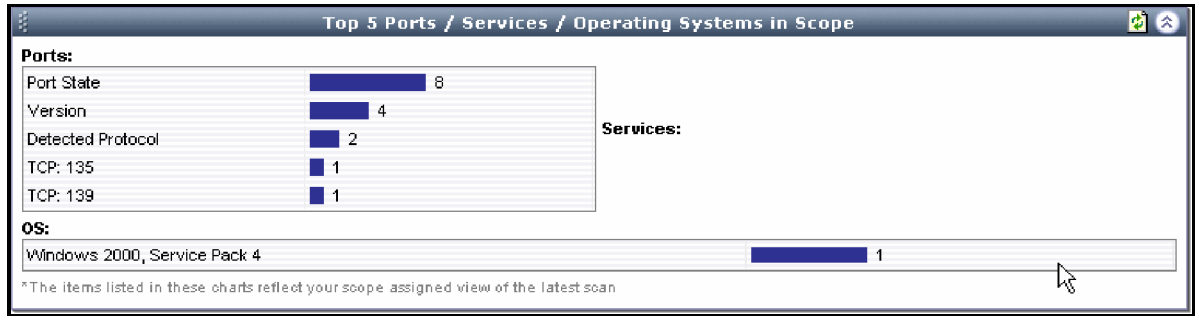


The Total Events in Scope object displays averages per host (IP address) of vulnerabilities and events. That is, if the scope includes three IP Addresses, and the total number of vulnerabilities are sixty-six, then the average vulnerability per host would be twenty-two. The average number of events is determined in the same manner. The averages are also displayed in color codes to reveal the level of severity. Finally, the percentages of the levels of severity are also displayed. That is, if 22 of the 66 vulnerabilities are rated as “High,” then 33 percent of the vulnerabilities are rated as “High.”

- Top Five Port/Services/Operating Systems in Scope

This object displays details about the Ports, Services, and Operating Systems that are in use within the Scope of IP Addresses.

Top 5 Port / Services / Operating Systems in Scope



- Task Grid

This object displays the total number of tasks (events that have been assigned to a user or group), as well to whom or to which group the task has been assigned. In addition, the status (New, Open, Pending, Closed) and the severity level of each task is shown.

Task Grid

Users:	New					Open					Pending					Closed					
	Total	High	Med	Low	Info	Total	High	Med	Low	Info	Total	High	Med	Low	Info	Total	High	Med	Low	Info	
administrator	2	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
stephen	3	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

- Events by Category

This object displays the total number of events, but categorizes them by type. For example, the event may be related to a Database, IP Services, an Anti-Virus application, or Web Services. Figure, "Events by Category," on page 10 shows all of the categories.

Events by Category

Event Category	Total	High	Medium	Low	Info
Accounts	18	0	8	8	0
Anti-Virus	1	0	0	0	1
Database	26	19	7	0	0
IP Services	1	0	1	0	0
Mail Servers	2	0	1	0	1
Miscellaneous	2	2	0	0	0
NetBIOS	2	1	1	0	0
Registry	4	0	3	1	0
Web Servers	2	0	0	0	2

Events

The **Events** object contains links for viewing, searching for, and purging events.

Events Manager Events Object



View Events

Clicking the **View events** link displays a list of all events, including all severity levels, in the REM database.

View Events

Type	Severity	Date	Machine	Application	Name
Warning	Medium	4/30/2004 12:05:00 PM	smartinez	Retina	TCP:25 - SMTP Relaying
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 sp_MSscopyscript comm...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 malformed 0x08 packe...
Warning	Medium	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 Resolution Service d...
Warning	Medium	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 sp_MSscopyscript SQL ...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 xp_SetSQLSecurity bu...

The list of events includes information that indicates the Type (for example, Warning, Information), Severity (Medium, High, Low), Date, Machine, the Application (Retina, Blink, SecureIIS), and Name (brief description of the Event). Additional details about an event in the list are accessible by clicking on that event. (See "Viewing and Managing Events" on page 21).

Search Events

This link allow users to search for events based on such criteria as the application source, severity level, and date. In addition, specific text can be used as part of the search.

Search Events

 A screenshot of a "Search Events" dialog box. It has a title bar with a maximize button. The main area contains:

- "Enter search criteria below." followed by a text input field.
- "Search all fields for:" followed by another text input field.
- "Include these scanner applications:" followed by a list of checkboxes: Retina, Iris, Blink, and SecureIIS.
- "Include these severities:" followed by a list of checkboxes: High, Medium, Low, and Information.
- "Date range (start):" followed by three dropdown menus for day, month, and year.
- "Date range (end):" followed by three dropdown menus for day, month, and year.
- At the bottom right, there are "OK" and "Cancel" buttons.

Purge Events

This link will delete all events from the REM database, and should only be used when necessary.

Tasks

This object contains links for viewing tasks.

Tasks



You can choose to view all tasks, or only those that have a status of **New**, **Open**, or **Pending**. Figure displays a view of all tasks.

View All Tasks

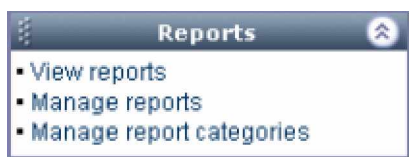
	Severity	Status	Date	Machine	Application	Event	Name
	Medium	Closed	4/30/2004 12:05:00 PM	smartinez	Retina	RET-SCAN-002	TCP:25 - SMTP Relaying
	High	New	4/30/2004 12:05:00 PM	smartinez	Retina	RET-SCAN-002	SQL 2000 sp_MSscopyscript comm...
	High	New	4/30/2004 12:05:00 PM	smartinez	Retina	RET-SCAN-002	SQL 2000 xp_SetSQLSecurity bu...
	High	Pending	4/30/2004 12:05:00 PM	smartinez	Retina	RET-SCAN-002	SQL 2000 xp_proxiedmetadata b...
	High	New	4/30/2004 12:05:00 PM	smartinez	Retina	RET-SCAN-002	SQL 2000 xp_peekqueue buffer ...
	High	Open	4/30/2004 12:05:00 PM	smartinez	Retina	RET-SCAN-002	SQL 2000 xp_updatecolvbm buff...
	High	Closed	4/30/2004 12:05:00 PM	smartinez	Retina	RET-SCAN-002	SQL 2000 xp_showcolv buffer o...

This view is similar to View Events (see Figure , “View Events,” on page 11). However, there is also a **Status** column showing which tasks are **Closed**, **New**, **Open**, and **Pending**. Details about a particular task can be viewed by clicking on that task. See “Assigning and Managing Tasks” on page 27 for more information about tasks.

Reports

This object contains links to all available reports, as well as to options for managing reports and categories.

Reports



View Reports

This link displays all available reports. The default view categorizes these reports.

View Reports

Home > View Reports
 Below is a list of all reports found in REM's database.

Categorized | [Uncategorized](#)

Event reports (10)

Application, Task Status, Severity
Assigned To, Task Due Date, Status
Date of Event, Assigned To, Task Status
Last Updated, Assigned To, Severity
Machine Name, Severity, Task Status
Severity, Date, Task Status
Severity, Machine Name, Task Status
Task Due Date, Status, Severity
Task Status, Workgroup, Severity
Workgroup, Date, Task Status

Retina specific (18)

SecureIIS specific (7)

Task Reports (3)



test (1)

Categorized | [Uncategorized](#)

39 reports found.

Reports are listed by category. The reports can be displayed in alphabetical order, instead of by category, by clicking the **Uncategorized** link in the upper right. Conversely, the reports can be grouped according to category by clicking on the **Categorized** link.

The number of reports in each category are indicated in parentheses. For example, the Retina Specific category contains 18 reports. A particular report can be scheduled by clicking that report.

As with other objects in the Events Manager, the report categories can be expanded or collapsed by clicking on the down arrow  or up arrow . For example, the **Event reports** category in Figure is expanded while the **Retina specific** category is collapsed.

Manage Reports

The Manage Reports link is similar the View Reports link. However, this link enables users to add a new report.

Manage Report Categories

The Manage Categories link displays a list of report categories and the number of reports they each contain. Users can add a new category, or delete or rename an existing category.

Manage Categories

Home > Categories
 Below is a list of categories.

[Add New](#)

Manage Application Categories	
Group	# of Items
Event reports	10
Retina specific	18
SecureIIS specific	7
Task Reports	3
Test	1

5 categorie(s) found.

Policies

This object provides tools for defining audit parameters for an eEye scan engine.

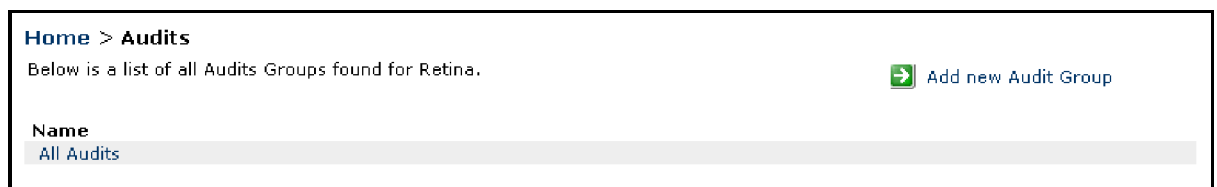
Policies



Manage Audits

This link displays a list of all Audit groups for an eEye scan engine. From this list, a user can select an existing audit group and modify it, or create a new audit group.

Manage Audits



As shown in the Figure above, the example shows only one audit group called "All Audits." At this point, a user can add a new Audit Group by clicking the link in the upper right, or click All Audits to modify it.

"Audit Group List of Vulnerability Checks" Figure on page 15 shows of list of vulnerabilities categories that an eEye scan engine can use. The vulnerabilities are grouped into over twenty categories, including CGI Scripts, Database, DNS Services, FTP Servers, IP Services, CHAM, and many others.

Audit Group List of Vulnerability Checks

Home > Audits
 Retina audits define the list of vulnerability checks used by the Retina scanner.

Name:

- Accounts
- CGI Scripts
- Database
- DNS Services
- DoS
- FTP Servers
- IP Services
- Mail Servers
- NetBIOS
- Registry
- Remote Access
- RPC Services
- Service Control
- SNMP Servers
- SSH Servers
- Web Servers
- Wireless
- Anti-Virus
- Windows
- Backdoors
- CHAM
- Miscellaneous

A particular category of vulnerabilities can be expanded by clicking on the plus sign (+). Conversely, a category may be collapsed by clicking on the minus sign (-). In the “Vulnerability Checklist” Figure on page 15, the CGI Script category has been expanded.

Vulnerability Checklist

Home > Audits
 Retina audits define the list of vulnerability checks used by the Retina scanner.

Name:

- Accounts
- CGI Scripts

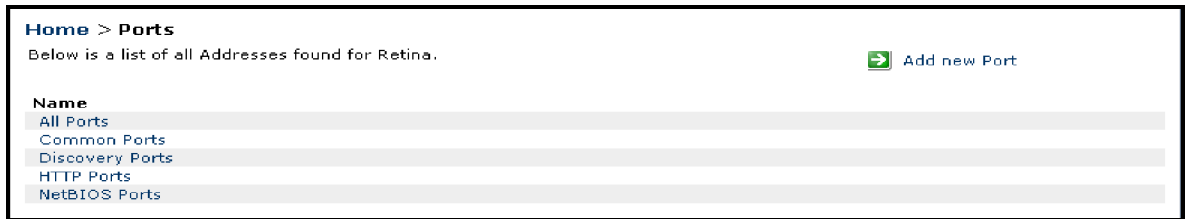
<input type="checkbox"/>	High	CGI - Aglimpse	CGI Scripts	2026	CVE-1999-0147
<input type="checkbox"/>	High	CGI - AnyForm2	CGI Scripts	719	CVE-1999-0066
<input type="checkbox"/>	High	CGI - Websendmail	CGI Scripts	2077	CVE-1999-0196
<input type="checkbox"/>	Medium	CGI - Www-sql	CGI Scripts		
<input type="checkbox"/>	Medium	EZMail 2000 - Order.log	CGI Scripts	2055	CAN-1999-0609
<input type="checkbox"/>	Medium	PDG Shopping Cart - Config File	CGI Scripts		
<input type="checkbox"/>	Medium	PDG Shopping Cart - Order.log	CGI Scripts	2021	CVE-1999-0608
<input type="checkbox"/>	Medium	QuikStore - Admin Password	CGI Scripts	1983	CAN-1999-0607
<input type="checkbox"/>	Medium	WebCart - Config File	CGI Scripts		CAN-1999-0610
<input type="checkbox"/>	Medium	WebCart - Orders File	CGI Scripts		CAN-1999-0610
<input type="checkbox"/>	Medium	WebStore - Order.log	CGI Scripts	2021	CAN-1999-0604
<input type="checkbox"/>	High	CGI - Args.bat	CGI Scripts		
<input type="checkbox"/>	Medium	CGI - Bdir.htr	CGI Scripts		

From here, a user can add any or all of the vulnerabilities from the category to the Audit group that is being created or modified. Clicking the **Check All** button enables all of the parameters, while the **Uncheck All** button disables all of the parameters. The **Reverse** button is similar to an “undo” command, which returns the window to its previous state. Finally, a user can delete or save an Audit Group, or cancel out to return to the previous screen. More details about Audits are discussed in Chapter 7 “Advanced Concepts” on page 37.

Manage Ports

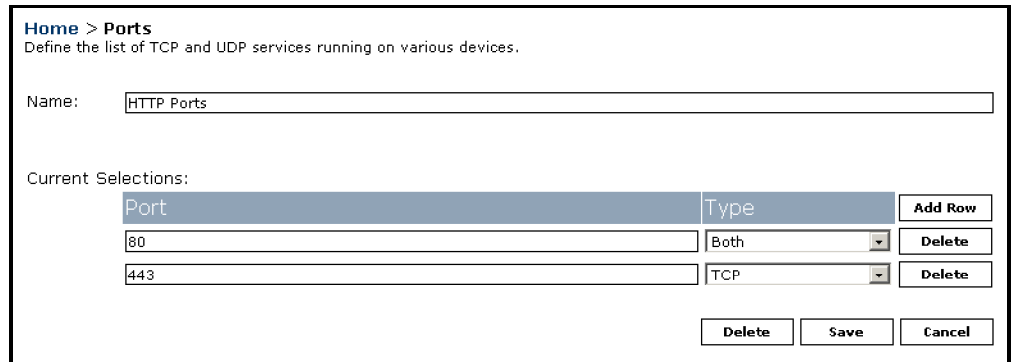
This link displays a list of ports defined for an eEye scan engine. Figure shows a list of port groups that have been defined for this example implementation.

Manage Ports



From this window, a user can either select an existing port group, or create a new port group. Each port group defines the relevant port numbers and whether the corresponding port type is UDP, TCP, or both. Figure , below defines two port numbers.

Ports Example



From here, the user can add or delete port numbers, or change the port type for an existing port number.

Manage Addresses

This link displays a list of addresses that define machines, devices, and IP addresses to be audited by an eEye scan engine. From this list, a user can select an existing address to modify, or create a new one. Figure shows an example of how an address is defined.

Address Example

Home > Addresses
Addresses define the machines, devices and IP addresses to be audited by Retina.

Name:

IP Ranges:

The IP ranges can be a single range, as shown in the previous example, or a set of several ranges, which may be manually entered. Alternatively, clicking the **Wizard** button accesses a wizard through which IP ranges may be added, modified, or deleted. In addition, the wizard will confirm that the address ranges are valid.

Manage Options

This link provides options for defining environment and performance variables for an eEye scan engine.

Manage Options

Home > Options
Define the Retina performance and environment preferences.

General

Create Log File

Opsec

Enable

Audit Level

Server

Port

As shown in Figure , a user can specify whether or not to create a log file, the Server name, the port number, and the level of severity (for example, Info, Low, Medium, High).

Manage Jobs

This link enables users to schedule a scan. The job is defined by specifying the eEye scan engine to use, the Audit Groups, Port Groups, Addresses, the time, frequency (daily, weekly, once per month), and other options such as forced scans, reverse DNS, Tracerouting, and so on.

Applications

This object allows users to specify applications and associate them with an eEye engine. These applications may be grouped into categories.

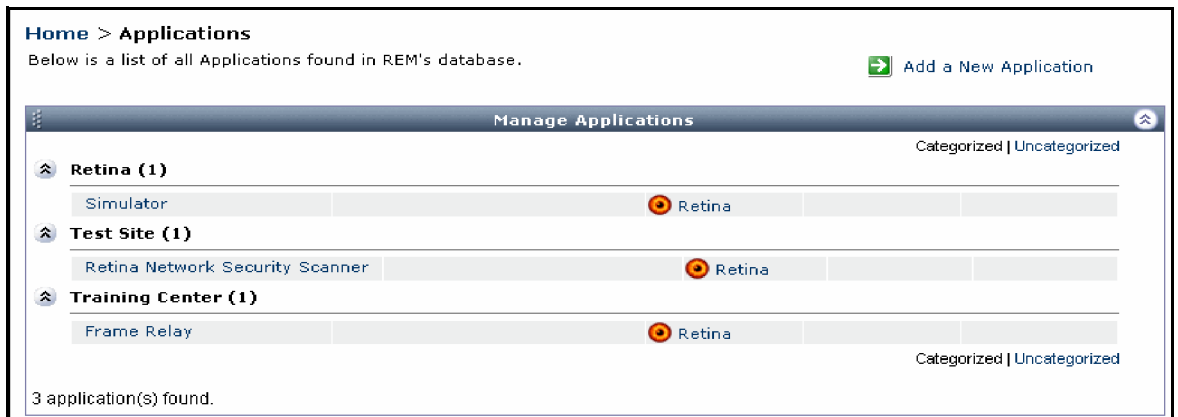
Applications



Manage Applications

This link displays a list of applications in the REM database.

Manage Applications

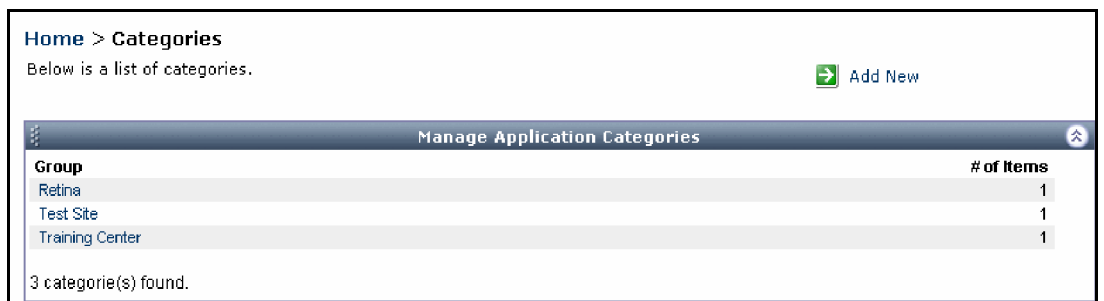


From the Manage Applications window, a user can add a new application, or select an existing one and modify it. In the previous example, there are three application categories, with one application in each, as indicated by the number in parentheses. For example, the Test Site category contains the Retina Network Security Scanner application. Optionally, the applications can be viewed uncategorized when the **Uncategorized** link in the upper-right is clicked, in which case the applications are listed in alphabetical order.

Manage Application Categories

This link displays a list of existing Application Categories, which assist network security personnel in organization.

Manage Application Categories



From this window, a user can add a new application category, or select an existing category and rename it.

Rules

The Rules object contains only one link, Manage Rules. A rule enables users and managers to automatically assign tasks to a user or a group, or delete tasks, based on specific criteria, such as the machine name, the application source (Blink, Retina, SecureIIS), and the severity level.

The Manage Rules link displays a list of existing rules, and enables users to create a new rule, or select an existing one and modify it.

More details about Rules are discussed in “Assigning and Managing Tasks” on page 27.

Users

This object enables managers and others with the proper level of permission to create user IDs, passwords, and groups, and to define scopes.

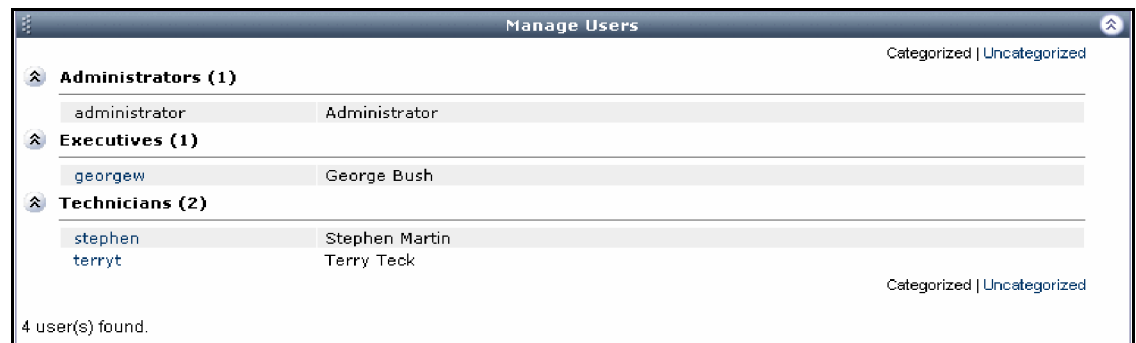
Users



Manage Users

This link displays a list of authorized users, organized by the user groups that they belong to.

Manage Users



From this window, users, or those with proper permissions, can modify the profile of an existing user, or create a new User ID. The list of users can be viewed in alphabetical order by clicking the **Uncategorized** link.

Manage Scopes

Scopes define an IP address range to be used by an eEye scan engine. The Manage Scopes link displays a list of existing scopes, from which a user can modify the IP address range of an existing scope, or create a new scope.

Manage User Groups

This link displays a list of existing user groups, and enables managers and users with proper permissions to create new user groups or modify an existing user group.

Manage User Groups

Manage User Groups	
Group	# of Users
Administrators	1
Executives	1
Technicians	2
3 groups found.	

This window displays the user groups and the number of users within each user group. When a new User Group is created, it is assigned a scope to which members of the group will have access. Therefore, the usual process is to create a scope, then assign it to a new or existing user group. In addition, users IDs may be created and assigned to a group.

Similarly, existing user groups can have additional scopes assigned to them, or have scopes removed from them. Details about users, scopes, and groups are discussed in the *REM Management Guide*.

Options

This object enables administrators and managers to define password policies, such as expiration date, password length, and whether or not passwords must contain letters and numbers. In addition, managers and administrators are able to define which User Groups have access to which objects. For example, a **Technician** user group can only have access to the **Events**, **Tasks**, **Reports**, and **Rules** objects. Details about how to use Options are discussed in the *REM Management Guide*.

Home > Options
Define the Retina performance and environment preferences.

General	
Create Log File	False
REM	
Enable Logging	True
Audit Level	Info
Enable Port	True
Enable Share	True
Enable Machine	True
Enable User	True
Enable Service	True
Enable General	True
Opsec	
Enable	False
Audit Level	Info
Server	
Port	
Performance	
Simultaneous Scans (1-255)	24
Adaptive Scan Speed	5 - Fastest
Reliability	
Ping Timeout (1-255 seconds)	3
Data Timeout (1-255 seconds)	3

Viewing and Managing Events

This chapter discusses how Events are viewed and managed in REM Events Manager. Part of the discussion takes into consideration how REM fits into the eEye product architecture.

What is an Event?

An event is a piece of information that the Events Server receives from a REM Client application, such as Retina, Blink, Iris, or SecureIIS. The information contains data regarding different assets, including routers, switches, servers, ports, IP addresses, wireless devices, individual machines, and peripheral devices.

The data, in turn, reflects an event that is informational or of a varying degree of severity. For example:

- An *informational* event could be a visitor to a web site who does not log in.
- A *low severity* event may occur when a machine on the network has autorun enabled on the CD-ROM drive.
- A *medium* level event may occur when an Administrator's password does not have an expiration date.
- A *high severity* event is one where the absence of a Service Pack installation makes it possible for an attacker to exploit a function by passing a long parameter.

The following sections discuss various eEye Digital Security engines, and how REM interacts with each of them. More specifically, the types of events that REM may receive from each engine is discussed.

Blink Enterprise Intrusion Prevention

Blink is host-based and scans the host machine against a vulnerability database that is updated daily. After Blink completes a scan, REM is alerted to such events as misconfigurations or uninstalled patches.

There is often a gap between the time that a vulnerability is known and when a patch or fix may be implemented. To address this issue, Blink uses a database of attack signatures to alert REM of a potential attack.

Finally, unknown vulnerabilities may be detected by Blink through intelligent protocol analysis, which enables the reconstruction of network traffic. In this manner, REM will be alerted to attacks in progress. At the same time, Blink will block the attack and log this intrusion prevention event with REM.

In all of these scenarios, Blink alerts REM to any vulnerability or attack, as well as any remediation against the relevant vulnerability or attack. These do not constitute an exhaustive list of Blink's capabilities. Rather, these are some examples of the types of events REM may receive from Blink.

Retina Network Security Scanner

While Blink is host-based, Retina is server-based, which enables a scan of all devices on a network. Retina performs a scan against a list of known vulnerabilities that is updated daily. The scanning technology itself is also updated and downloaded at the beginning of each Retina Session.

During each scanning session, Retina alerts REM to any vulnerabilities it discovers in reference to specific machines, IP addresses, ports, and applications.

In addition to the vulnerability database, Retina enables the creation of customized audits so that REM can be alerted to such events as anti-virus deployments, machine configurations, application installations, and version control.

Finally, Retina updates the REM database with corrective actions and fixes for those events that require them.

SecureIIS Web Server Protection

SecureIIS addresses the vulnerabilities of Microsoft Internet Information Services. Between the time that IIS vulnerabilities are detected and when Microsoft issues a patch, SecureIIS inspects all web server traffic and alerts REM to any known or unknown attacks.

Presently, SecureIIS is available as a stand-alone application. However, future releases of SecureIIS will be bundled with Blink.

Iris Network Traffic Analyzer

Iris analyzes all network traffic, and sends events to REM that pinpoint the source of security breaches and performance problems. When the Iris automated filters are set up appropriately, REM can receive events of network traffic that contain specified MAC or IP addresses, unacceptable words, or web sites.

Viewing Events

To view events, a user will need the following:

- Valid username and password
- Access to the REM database
- A completed scan by an eEye engine to populate the REM database with events.

Logging into the REM Events Manager

The REM Events Manager can be accessed by launching it through the Windows Program Manager, or by typing in the web address of the virtual directory. (The default is <http://localhost/~rem/>.)

When the Events Manager is initially launched, the user is prompted to enter a User Name and Password.

Login Dialog

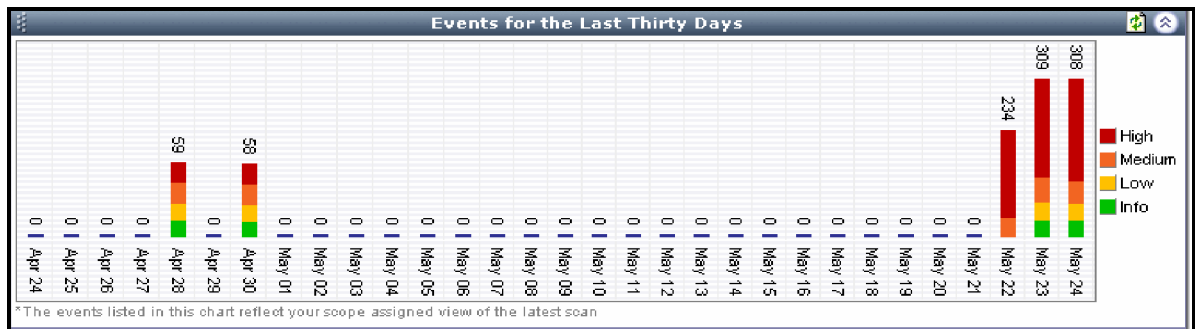


After successfully logging in, the Threat Management Portal displays. The actual objects and options available to any user will depend upon the User Group to which he or she belongs, and the access rights the user has.

Events for Last Thirty Days

The Threat Management Portal provides several methods for a user to view events. The events that can be viewed will be limited to the scope of the User Group that a user belongs to.

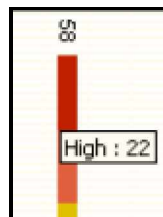
Events for the Last Thirty Days



Viewing Events of the Same Severity Level

In the *Events for the Last Thirty Days* object, users can view the details of all events for a given severity level. For instance, in the above example, the bar graph for April 30 shows that there are 22 events with a “High” severity level.

Cursor Display



Double-clicking on the red code, from the example Figure on page 24, displays all 22 high severity level events in a new window.

High Level Events Example

Home > Events

Below is a list of all events found in REM's database.

Type	Severity	Date	Machine	Application	Name
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 sp_MSscopyscript comm...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 malformed 0x08 packe...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 xp_Set5QLSecurity bu...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 xp_proxiedmetadata b...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 xp_printstatements b...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 xp_peekqueue buffer ...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 xp_updatecolvbm buff...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 xp_showcolv buffer o...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 xp_enumresultset buf...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 authentication buffe...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 xp_displayparamstnt ...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 text formatting func...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 DBCC SourceDB buffer...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 Agent jobs privilege...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 Resolution Service b...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 OLE DB provider name...
Warning	High	4/30/2004 12:05:00 PM	smartinez	Retina	SQL 2000 multiple XP buffer o...
Warning	High	4/30/2004 12:04:59 PM	smartinez	Retina	SQL 2000 password encryption ...
Warning	High	4/30/2004 12:04:59 PM	smartinez	Retina	SQL 2000 Resolution Service O...
Warning	High	4/30/2004 12:04:56 PM	smartinez	Retina	Internet Explorer 6 SP1 Cumul...
Warning	High	4/30/2004 12:04:56 PM	smartinez	Retina	Null Session
Warning	High	4/30/2004 12:04:56 PM	smartinez	Retina	Windows DirectX MIDI heap cor...

Page 1 of 1 Go

22 events found.

Viewing Event Details

From this window, users can obtain details about a specific event by clicking on it.

Event Detail Example

Home > Events

Below are the details of the event. Elevate event to task

EventView

Machine Information

Date: 4/30/2004 12:05:00 PM **Source IP:** 192.168.2.184

Machine: smartinez **User:** SYSTEM

Operating System: Microsoft Windows 2000 Server v 5.0 Service Pack 4 (Build 2195)

Event Information

Name: SQL 2000 xp_printstatements buffer overflow

Subject: 192.168.002.184 (smartinez.eCompany.gov)

ID: RET-SCAN-002 **Type:** Warning

Severity: 9 **Category:** Audits - Database

Description: Microsoft SQL Server 2000 (pre-SP) is susceptible to a buffer overflow in the srv_paraminfo function that can be triggered by indirectly passing a long parameter to the function via the xp_printstatements extended stored procedure. An attacker can expl

BUGTRAQ ID: 2041

CVE ID: CAN-2000-1086

How To Fix: Install the latest SQL Server 2000 Service Pack.

URL1: [Download the latest SQL 2000 Service Pack](#)

URL2: [Microsoft Knowledge Base Article Q280380](#)

URL3: MS00-092

Workgroup Information

Application Information

<< Back

From the Event View, users can obtain more details about the event, go to a specific site to download a patch or fix, or elevate the event to a Task. Details about task are in Chapter 5 “Assigning and Managing Tasks” on page 27.

Viewing All Events

The previous sections essentially demonstrated how to view events for the same severity level. However, by clicking on **View events** in the **Events** object, all events, regardless of the severity, can be displayed in a single list. When these events are displayed, details of a particular event can be viewed by clicking on a particular event.

Searching for Events

The **Search events** link in the Events object can be used to search for events based on the following criteria:

- Descriptive text
- Application
- Severity level
- Date range

Search Events

Viewing Events of the Same Severity Level

The following procedure demonstrates how to view events of the same severity level, and how to obtain details about a specific event. It is assumed that a REM database is already installed, and that an eEye engine has been written data into the database.

1. Log in to REM Events Manager to open the Threat Management Portal. If you are already logged in and are on a different page, click **Home** in the **Main** object to open the Threat Management Portal.
2. In the **Events for the Last Thirty Days** object, double-click on Medium severity-level (orange color-coded) events for a particular day. If none exist, click on green color-coded events.
3. Take note of the number of these events.
4. Click one of these events to view details about the event.
5. Click **View events** in the **Events** object.
6. Take note of the total number of events, and the different severity levels (High, Medium, Information).

7. In the **Name** column, make a note of a word or phrase, such as "SQL," NetBIOS," "Printer," or any other word or phrase that appears in that column.
8. Under the **Application** column, make a note of the application, such as Retina, Blink, or other eEye engine that may appear in that column.
9. Click **Search Events** in the **Events** object.
10. Enter the word or phrase you noted in Step 8, click the corresponding checkbox of the Application you noted in Step 9, select any or all of the security levels (leaving these checkboxes unchecked results in a search for all security levels), and enter the date range for the previous 30 days, including today's date.
11. Click **OK**.
12. Take note of the search results.
13. Click **Home** to return to the Threat Management Portal.



Assigning and Managing Tasks

This chapter discusses the concept of Tasks, and how they are assigned and managed. Rules for automating the assignment and management of tasks will also be addressed.

What is a Task?

A task is simply an Event that requires remediation activity by a user, and which has been assigned to a user or group to complete that activity. When an event requires intervention or remediation, it is said to be elevated to a “Task.”

Elevating an Event to a Task

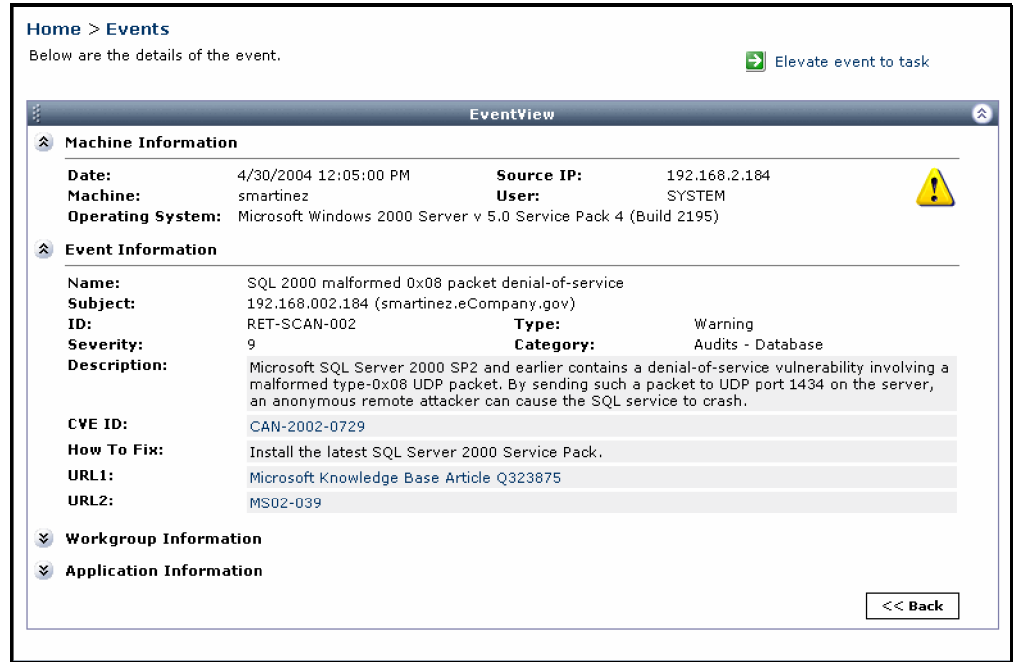
The previous chapter demonstrated how viewing events and their details is simple. This section explains the process for elevating an event to a task, and assigning it to a user or group.

The Threat Management Portal displays tasks that have been assigned to the presently logged in user. The portal also displays events that fall within the scope assigned to the user group of which the present user is a member.

A user with the proper permissions can elevate an event to a task. The event to elevate may be based on its severity level. In such a case, the user may display a list of events for the same severity level from the “Events for the last Thirty Days” object (as shown in “Viewing Events of the Same Severity Level” on page 25), and then select a specific event. Alternatively, an event can be selected from a list of all events, after selecting **View events** from the **Events** object, as shown in the “View Events” on page 11.

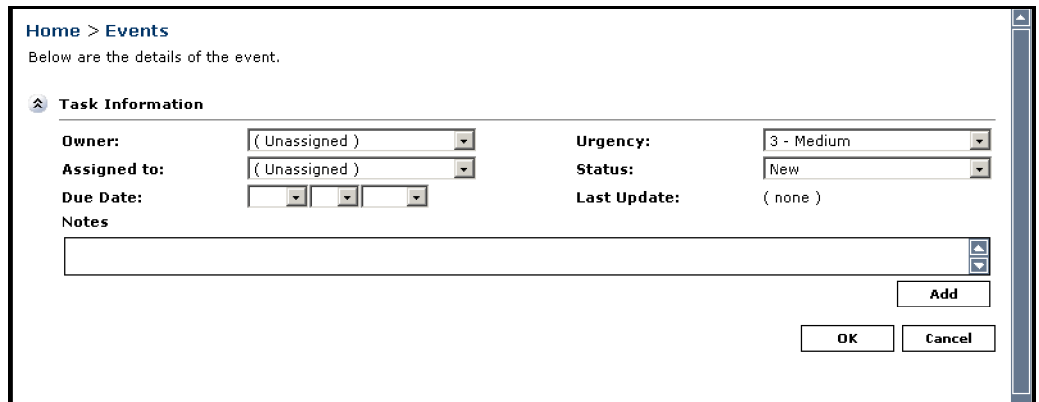
After selecting an event to display its details, the user has the option of elevating the event to a task.

Event Details

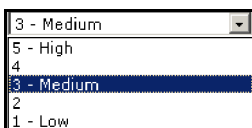


From this window, the user can click **Elevate event to task** in the upper-right corner, which displays the following window:

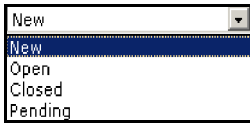
Elevate Event to Task



In this window, specify the values for the fields using the corresponding drop-down lists. The names that are available in the **Owner** and **Assigned to** drop-down lists are system specific for the users that have been defined within REM. Specify the **Due Date** as necessary, and insert notes if desired. The **Urgency** drop-down list ranges from 1 (Low) to 5 (High), as shown below:



The **Status** drop-down list includes **New**, **Open**, **Closed**, and **Pending**.



The status defaults to **New** when an event is initially elevated to a task. Later, the user to whom the task is assigned may change the status, to either **Open**, **Pending**, or **Closed**, as appropriate.

Viewing Tasks

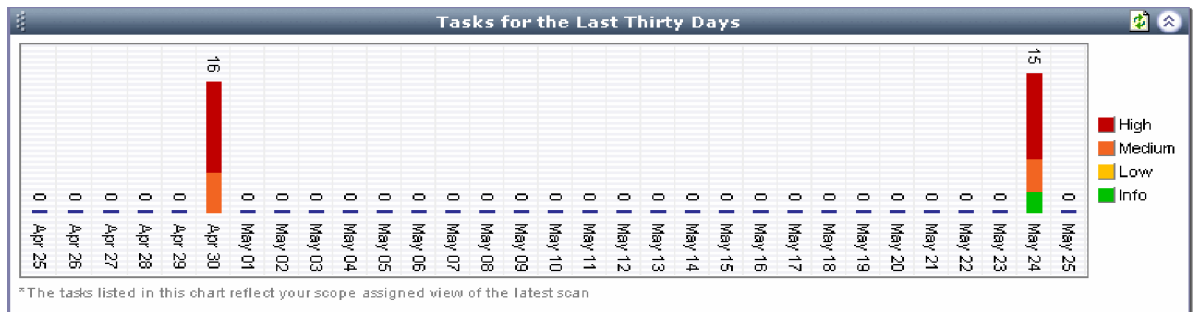
A user can view a task by either of the following methods:

- Viewing Tasks of Same Severity Level
- Viewing Tasks through the Tasks Object

Viewing Tasks of the Same Severity Level

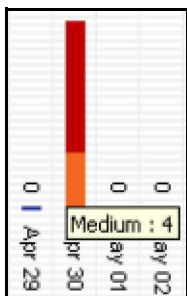
When a user first logs into the REM Events Manager, among the objects that they may view is “Tasks for Last Thirty Days,” which is displayed in the Threat Management Portal.

Tasks for Last 30 Days



The tasks shown here are those that fall within the Scope assigned to the User Group of which the user is a member. A user can view tasks of a given severity level, on a particular due date, by placing the cursor over the corresponding area on the color-coded graph. For example, placing the cursor over the orange color for April 30 shows that there were four tasks of medium severity that were due, as shown in the “Viewing Tasks of Same Severity Level” Figure on page 30.

Displaying Number of Tasks of Same Severity Level



The user can then double-click to display these medium level tasks.

Viewing Tasks of Same Severity Level

Home > Tasks
Below is a list of all tasks found in REM's database.

Severity	Status	Date	Machine	Application	Event	Name
⚠ Medium	Pending	4/30/2004 2:34:05 PM	QA017	SecureIIS	SIIS-FLT-01	File Not Found
⚠ Medium	Open	4/30/2004 2:34:05 PM	QA017	SecureIIS	SIIS-FLT-01	File Not Found
⚠ Medium	Closed	4/30/2004 2:33:17 PM	QA017	SecureIIS	SIIS-FLT-01	File Not Found
⚠ Medium	Closed	4/30/2004 2:32:48 PM	QA017	SecureIIS	SIIS-FLT-01	File Not Found

In this example, the user can see that two of the tasks are closed, one is pending, and another is open. This example shows how to view tasks of the same severity level for a specific due date. The same can be done for other dates and other severity levels. Further, details about a particular task can be viewed.

Viewing Task Details

To view details of a task, click on a specific task from the displayed list. The list of tasks may be those displayed through the Tasks Object (see the section "Viewing Tasks using the Tasks Object" on page 31), or those of the same severity level (as explained in the previous section). For example, in the "Tasks" Figure on page 31, double-clicking the Open task displays the details for that task, as shown in the "View All Tasks" Figure on page 31.

Task Details

Home > Tasks
Below are the task details.

EventView

Machine Information

Date: 4/30/2004 2:34:05 PM **Source IP:** 127.0.0.1
Machine: QA017 **User:** SYSTEM
Operating System: Microsoft Windows 2000 Server v 5.0 Service Pack 3 (Build 2195)

Task Information

Owner: Administrator **Urgency:** 3 - Medium
Assigned to: Stephen Martin **Status:** Open
Due Date: Apr 30, 2004 **Last Update:** New
New
Open
Closed
Pending

Notes

5/25/2004 1:42:53 PM - Administrator
Status changed to Open.

5/25/2004 1:32:37 PM - Administrator
Status changed to New. Assigned to Administrator.

Add

Event Information
Workgroup Information
Application Information

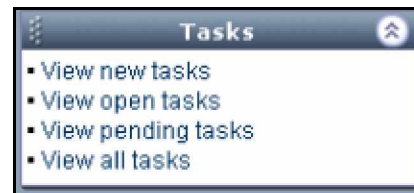
OK **Cancel**

From here, the user can obtain more information or change the status of the task.

Viewing Tasks using the Tasks Object

The **Tasks** object on the left portion of the Threat Management Portal includes links for viewing tasks.

Tasks



All tasks can be displayed, or only those that have a status of **New**, **Open**, or **Pending**. For example, a task recently elevated from an event would be displayed as a new task. Figure shows a view of all tasks.

View All Tasks

Severity	Status	Date	Machine	Application	Event	Name
Medium	Closed	4/30/2004 12:05:00 PM	smartinez	Retina	RET-SCAN-002	TCP:25 - SMTP Relaying
High	New	4/30/2004 12:05:00 PM	smartinez	Retina	RET-SCAN-002	SQL 2000 sp_Mscopyscript comm...
High	New	4/30/2004 12:05:00 PM	smartinez	Retina	RET-SCAN-002	SQL 2000 xp_SetSQLSecurity bu...
High	Pending	4/30/2004 12:05:00 PM	smartinez	Retina	RET-SCAN-002	SQL 2000 xp_proxiedmetadata b...
High	New	4/30/2004 12:05:00 PM	smartinez	Retina	RET-SCAN-002	SQL 2000 xp_peekqueue buffer ...
High	Open	4/30/2004 12:05:00 PM	smartinez	Retina	RET-SCAN-002	SQL 2000 xp_updatecolvbm buff...
High	Closed	4/30/2004 12:05:00 PM	smartinez	Retina	RET-SCAN-002	SQL 2000 xp_showcolv buffer o...

From here, the user can view the details of a task by highlighting and double-clicking it. The details, and the options available to the user, will be similar to those shown in the “Task Details” Figure on page 30.

Rules

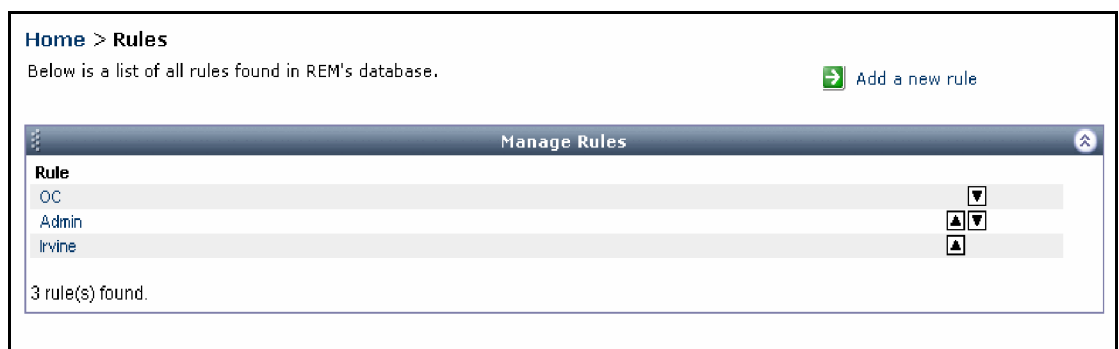
The section “Elevating an Event to a Task” on page 27 discusses how to manually elevate an event to a task, and then assign that task to a user or user group. However, REM contains a tool by which this process can be automated.

Tasks



Clicking **Manage rules** in the **Rules** object displays the following window:

Manage Rules Window



From here, depending on whether or not the user has the proper access privileges, the user can modify an existing rule or create a new rule.

- To modify an existing rule, click on the rule to be modified.
- To create a new rule, click **Add a new rule**.

In either case, the following window displays, in which the user can modify a rule or specify the parameters for a new one.

Specifying Parameters for a Rule

The screenshot shows a web interface for managing rules. At the top, it says "Home > Rules" and "Below is a list of all rules found in REM's database." Below this is a "Manage Rules" dialog box. The dialog has the following fields:

- Rule name: QA Testing
- Action: assign task to
- Target: Technicians (group)
- WHEN**
- Machine Name = QA017
- Application = Retina
- Severity = 6 (Medium)
- Rule: assign task to 'Technicians' when source.host = 'QA017' and agent.id = 'Retina' and severity = '6'

At the bottom of the dialog are three buttons: "Delete", "OK", and "Cancel".

In this window, the user can specify or modify the Rule Name, the action to take (assign or delete), the Target (user or user group), the machine name, the application (Retina, Blink, Iris, SecurellS), and the severity level.

Exercise

This section includes a simple exercise that will help familiarize users with basic procedures for managing tasks.

Exercise

This exercise demonstrates how to elevate an event to a task.

1. Log in to REM Events Manager
2. Click **View events** in the **Events** object.
3. Double-click an event to display its details.
4. Click the **Elevate to a task** link.
5. Fill in the fields as required. A user may claim ownership, and assign the task to himself or to another user or group.

Depending on the user's access permissions, the user may not be able to view all tasks unless:

- The user is an administrator
- The task has been assigned to them, or to their user group

- The user is the owner of the task.
6. Click **Add**, and then click **OK** to return to the list of events.
 7. Click the **View new tasks** link in the **Tasks** object.
 8. In the list of new tasks, highlight and double-click the task to display its details.
 9. Change the status from **New** to either **Open** or **Pending**.
 10. Click **OK**.
 11. Click **View all tasks** to see the task with the changed status.

Reports

This chapter discusses how to access the various reporting options in the REM Events Manager, and how these reports can assist network security personnel in planning, auditing, analyzing, and implementing security policies. A typical REM implementation has a default of at least forty reports available, depending on the number of eEye applications that send data to the REM database. In addition, network security administrators can add reports. Consequently, due to the variation and number of reports available for different installations, this section will not address all of the reports that can be accessed through the REM Events Manager.

Accessing and Generating Reports

As mentioned briefly in Chapter 2, REM offers a variety of reporting tools. These reporting tools can be easily accessed using either the **View reports** or **Manage reports** links in the **Reports** object.

- The **View reports** link is used for generating or scheduling a report.
- The **Manage reports** link is used for modifying an existing report or creating a new one.

However, the ability to create new reports or modify an existing report is dependent upon the user's access permissions.

Generating a Report

The reports that can be generated are based on the following categories:

- Application specific (Retina, Blink, SecureIIS)
- Events
- Tasks
- Any other category created by the network security administrator, or a REM user with administrator privileges

To generate a report, do the following:

1. Click **View reports** in the **Reports** object.
2. Select the desired report from any of the report categories.
3. Depending on the type of report selected, specify the relevant criteria, such as machine name, IP Address, Scope, or Task Status.
4. To schedule a report at a specific time and date, click **Schedule**. Additional options allow for generating a report only one time, or on a daily, weekly, or monthly basis.

- To generate the report, click **OK**.

Task Reports

The most common types of reports that a typical user would generate are those related to tasks. A default REM installation contains the following task reports:

- Task Grid
- Tasks assigned to a specific user
- Tasks owned by the user, but assigned to other users

Task Reports

The reports can be accessed by clicking the corresponding link.

The Task Grid report displays a list of tasks and their corresponding status, according to individual users and user groups.

Task Grid Report

Task Grid																				
Tasks:	New					Open					Pending					Closed				
Users:	Total	High	Med	Low	Info	Total	High	Med	Low	Info	Total	High	Med	Low	Info	Total	High	Med	Low	Info
administrator	2	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
stephen	3	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

The “Tasks assigned to you” and “Tasks you own that are assigned to another user or group” reports provide details for tasks as indicated by their report name.

Additional Reports

The following table contains a list of categories with the corresponding reports contained in each.

Category	Name of Report
Event Reports	Application, Task Status Severity Assigned To, Task Due Date, Status Date of Event, Assigned To, Task Status Last Updated, Assigned To, Severity Machine Name, Severity, Task Status Severity, Date, Task Status Severity, Machine Name, Task Status Task Due Date, Status, Severity Task Status, Workgroup, Severity Workgroup, Date, Task Status
Retina specific	Executive report Retina audit report by IP Retina audit report by name Retina audit report by scan Retina audits delta report by IP Retina audits delta report by name Retina port delta report by IP Retina port delta report by machine name Retina service delta report by IP Retina service delta report by machine name Retina share delta report by IP Retina share delta report by machine name Retina user delta report by IP Retina user delta report by machine name Top 20 operating systems Top 20 ports Top 20 services Top 20 users
SecureIIS specific	Executive report Top 20 404 errors Top 20 attack categories Top 20 attacked scripts Top 20 attacked servers Top 20 attacking IPs Top 20 HTTP method violations
Blink Specific	TBD

Advanced Concepts

This chapter discusses how to use the Policies and Applications components in the REM Events Manager. This discussion can be useful in circumstances where an enterprise consists of several locations that are spread out over a large geographical area. In such situations, a local office may have a local network manager who may need to perform some of the tasks described in this chapter. A more detailed description of these tasks is available in the *REM Administration Guide*.

Policies

The **Policies** object contains several links for controlling the results of an eEye engine scan. For example, it may be necessary to limit the results to the detection of certain kinds of CGI scripts or other known vulnerabilities. In addition, the results may be limited to events related to ports or IP addresses. Finally, a scan may be scheduled for specific IP address ranges or ports at a specific time or date.

The **Policies** object contains these links:

- Manage audits
- Manage ports
- Manage addresses
- Manage options
- Manage jobs

Policies



Manage Audits

An audit may be defined as a list of events, or potential vulnerabilities or threats that are categorized by type. For example, some vulnerabilities may be CGI scripts, others may protocol-based, and others may be application based.

The types of audits and the corresponding categories are dependent upon the eEye engine that is installed. For example, Retina includes the categories shown in the Figure below.

Retina Vulnerability Checklist

- Accounts
- CGI Scripts
- Database
- DNS Services
- DoS
- FTP Servers
- IP Services
- Mail Servers
- NetBIOS
- Registry
- Remote Access
- RPC Services
- Service Control
- SNMP Servers
- SSH Servers
- Web Servers
- Wireless
- Anti-Virus
- Windows
- Backdoors
- CHAM
- Miscellaneous
- User

Each category includes a list of the known vulnerabilities that are stored in the REM database. A category may be expanded by clicking on the plus sign (+). For example, Accounts includes numerous items related to user names, passwords, and activities related to accounts, as shown in the Figure below.

Example of Accounts Vulnerability List

Accounts				
<input checked="" type="checkbox"/>	Low	Anonymous Policy Password - NT4	Accounts	87
<input checked="" type="checkbox"/>	Low	Cached Logon Credentials	Accounts	
<input checked="" type="checkbox"/>	Low	Cannot Change Password	Accounts	
<input checked="" type="checkbox"/>	Medium	Default Administrator Account	Accounts	CAN-1999-0585
<input checked="" type="checkbox"/>	Low	Last Username	Accounts	CAN-1999-0592
<input checked="" type="checkbox"/>	Medium	Max Password Age	Accounts	CAN-1999-0535
<input checked="" type="checkbox"/>	Low	Min Password Age	Accounts	CAN-1999-0535
<input checked="" type="checkbox"/>	Medium	Min Password Length	Accounts	CAN-1999-0535
<input checked="" type="checkbox"/>	Medium	Password Does Not Expire	Accounts	CAN-1999-0535
<input checked="" type="checkbox"/>	Low	Password History	Accounts	CAN-1999-0535
<input checked="" type="checkbox"/>	Medium	Service Account Passwords - NT4	Accounts	231
<input checked="" type="checkbox"/>	Info	User Never Logged On	Accounts	
<input checked="" type="checkbox"/>	High	Account password reverse of account	Accounts	CAN-1999-0505 CAN-1999-0518 CAN-1999-0520

Here, the user may select any or all of the vulnerabilities for this category. A user can modify an existing audit, or create a new one.

Modifying an Audit

To modify an audit, complete the following steps:

1. Select **Manage audits** in the **Policies** object.
2. Select an audit to modify from the list that is displayed.
3. Expand the relative categories and check or uncheck items from the list as needed.
4. Click **Save**.

Note: An existing audit can also be deleted simply by selecting **Manage audits**, selecting the desired audit, and then clicking **Delete**.

Creating an Audit

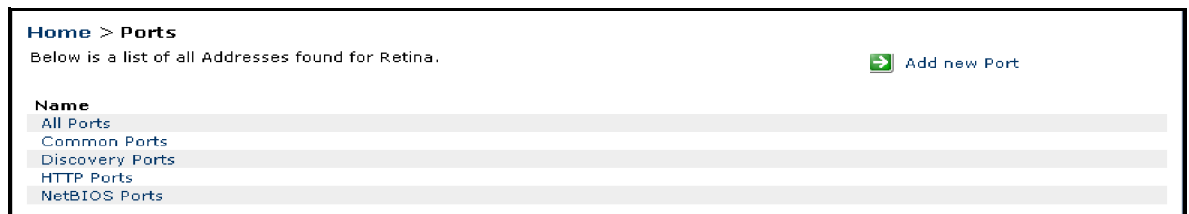
To create an audit, do the following:

1. Select **Manage audits** in the **Policies** object.
2. Select **Add new Audit Group**.
3. Type a name for the new audit.
4. Expand the relative categories and check or uncheck items from the list as needed.
5. Click **Save**.

Manage Ports

The **Manage ports** link in the **Policies** object allows users to categorize UDP and TCP services that are running on various ports. For example, some categories are HTTP or NetBIOS. Clicking **Manage port** displays a list of existing port categories.

Manage Ports



From here, a user can modify an existing port group or add a new one.

Modifying Ports

To modify an existing port group, do the following:

1. Select **Manage ports** in the **Policies** object.
2. Double-click the existing Port group to be modified.
3. If necessary, in the corresponding Port number row, change the port type to **UDP**, **TCP**, or **Both** from the drop-down menu under the **Type** column.
4. If desired, delete a row by clicking **Delete** to the right of the relative row.
5. To add a new port number, click **Add row**, and then type the desired port number (0 to 65535) and type (UDP, TCP, Both).

6. Click **Save**.



An existing port group can also be deleted simply by selecting **Manage ports**, clicking the port group, and then clicking **Delete**.

Creating Port Groups

To create a new port group, do the following:

1. Select **Manage ports** in the **Policies** object.
2. Click **Add new Port**.
3. Type a name for this port.
4. Specify the port number and the port type.
5. To add a new port number, click **Add row**, and then enter the desired port number (0 to 65535) and type (UDP, TCP, Both).
6. Repeat as necessary.
7. Click **Save**.

Manage Addresses

This link allows users to specify the range of IP Addresses to include in an eEye engine scan. For example, it may be necessary to limit the range of IP addresses by an office location, or by a department.

To specify a range of IP addresses, do the following:

1. Click **Manage addresses** in the **Policies** object.
2. Click **Add new Address**.
3. Type a name for this range of IP addresses.
4. Specify an IP address, a list of addresses, or a range of addresses.
5. Alternatively, click the **Wizard** button to display the following:

Address Wizard

A screenshot of the 'Address Wizard' dialog box within a Microsoft Internet Explorer browser window titled 'eEye Digital Security - Microsoft Internet Explorer'. The dialog box contains two rows of IP address input fields. The first row is labeled 'From:' and the second row is labeled 'To:'. To the right of the 'To:' row are four buttons: 'Add', 'Exclude', 'Delete', and 'Clear'. Below these input fields is a large empty text area. At the bottom right of the dialog box are 'OK' and 'Cancel' buttons.

In the Wizard, a user can **Add** or **Exclude** an IP address or a range of IP addresses.

6. Exit the Wizard by clicking **OK**.

7. Click **Save**.

Modifying or Deleting Addresses

To modify or delete an IP address range, do the following:

1. Click **Manage addresses**.
2. Select the Address to modify or delete.
3. Manually enter or delete the IP address, addresses or a range of addresses.
4. Alternatively, the Wizard can be used.
5. Click **Save**.

Manage Options

This link enables users to specify whether or not to use the following options:

- Create a log file
- Enable OPSEC, which allows for the following parameters:
 - Severity Level (Info, Low, Medium, High)
 - Server
 - Port

Manage Jobs

This link enables users to schedule a scan using specific parameters, such as Audits, Scan engine, Ports, and IP Address ranges. Further, these jobs can be run one time, or on a daily, weekly, or monthly basis. Finally, the scheduling of the jobs can be modified or deleted.

Applications

The **Applications** object allows users to specify the parameters of an eEye application. For example, a Retina scan engine could be specified by the DNS, or an IP Address. Further, the Path or URL for the application can be specified.

The use of this REM feature is useful when different locations, departments, or machines of a given IP address range have different configurations that are exposed to different possible threats or vulnerabilities. For example, one location may be using Blink and SecurellS to protect against specific types of threats, while another location is using Retina to protect against known vulnerabilities.

The **Applications** object includes the following links:

- Manage applications
This link allows users to add applications, or modify the specifications of an existing application.
- Manage application categories
This link allows the user to organize applications.



Index

A

- Administration 5
- Assets
 - Viewing and Managing 21
- audits
 - creating 39
 - deleting 39
 - modifying 39

B

- Blink
 - reports 36

C

- configuration 4

D

- Deployment 4

E

- elevating event to task
 - rules 27
- Events
 - Viewing and Managing 22

G

- Generating a Report 34

I

- installation 4
- IP address
 - modifying or deleting ranges 41
- IP addresses
 - specifying for a scan 40

M

- manage ports
 - deleting 39
- manual conventions i
- Modifying Ports 39

O

- Operations 4

P

- Policies 37
- Ports
 - modifying 39

R

- REM Deployment Guide 4
- Retina
 - reports 36
- Rules 31

S

- SecureIIS
 - reports 36

T

- Task Reports 36
- Tasks
 - changing status 29