EMERALD Development Project

December 2000
Acknowledgments:

DARPA ITO
DARPA ISO

EMERALD(TM) *Alert Management Interface*

System Design Laboratory

SRI International

Release Date: December 6, 2000

User's Guide, Version 1.2

EMERALD(TM)

`(Event Monitoring Enabling Responses to Anomalous Live Disturbances)`

**© copyright 1997-2000 SRI International
This is an UNPUBLISHED work of SRI International
and is not to be used, copied or disclosed except
as provided in the Software Distribution Agreement
with SRI International.
EMERALD is a Trademark of
SRI International**

EMERALD Development Team

EMERALD@sdl.sri.com

Steve Cheung (PI), Martin Fong, Ulf Lindqvist (PI), Phillip Porras (PI), Keith Skinner, Alfonso Valdes (PI),
Magnus Almgren, Mike Frandsen, Peter Neumann, Sandy Smith, Lynn Voss

© 2000 SRI International 333 Ravenswood Avenue Menlo Park, CA 94025-3493
SRI International is a nonprofit corporation.

Introduction

EMERALD provides a unique graphical user interface (GUI) for managing alerts produced by EMERALD sensors. Using this interface, you can view individual alerts, manage incident handling reports, print reports, forward reports via email, and view recommendations on responding to attacks. This alert management interface provides a session history that allows the security administrator to maintain a record of which alerts have and have not been acted upon. Administrators can also associate incident handling notes with each alert record to document information gathered during an investigation of the alert. The GUI provides four views. The main view displays alerts reported by the EMERALD sensors, with the most recent alerts listed at the top. The table view lists alerts in a tabular format, and allows the user to sort by any of the table columns merely by linking on the desired column. The table configuration view enables the user to control specific aspects of the tabular display. The status view gives the status of the monitors that are communicating with the interface.

Pull-down Menus

At the top of the window in each view is a pull-down menu bar consisting of five menus: File, View, Tools, Advanced, and Help.

FILE Menu: The File menu contains two options: Open (optional) and Exit. Open is used to start reading from another log file of attack data. Exit closes down the GUI. When exiting, three options are available: Just Exit, Exit and remove this History, and Exit and Remove All Histories. Just Exit closes down the GUI without deleting the persistent history files of this alert log on the disk. Exit and Remove This History shuts down the GUI and deletes any persistent files associated with the currently read attack data, but not the original attack data file itself. Exit and Remove All Histories closes down the GUI and deletes all persistent files associated with running the GUI for all attack data read, but does not delete the original attack data files themselves.

View Menu: The View menu provides six options. The first four allow the user to select which view is displayed: main, table, table configuration, or status. The contents of the various views are discussed in more detail in the sections that follow.

The next menu item, Do IP-Name Lookup, toggles the Main View window between displaying host IP addresses in Internet dot notation or symbolic names.

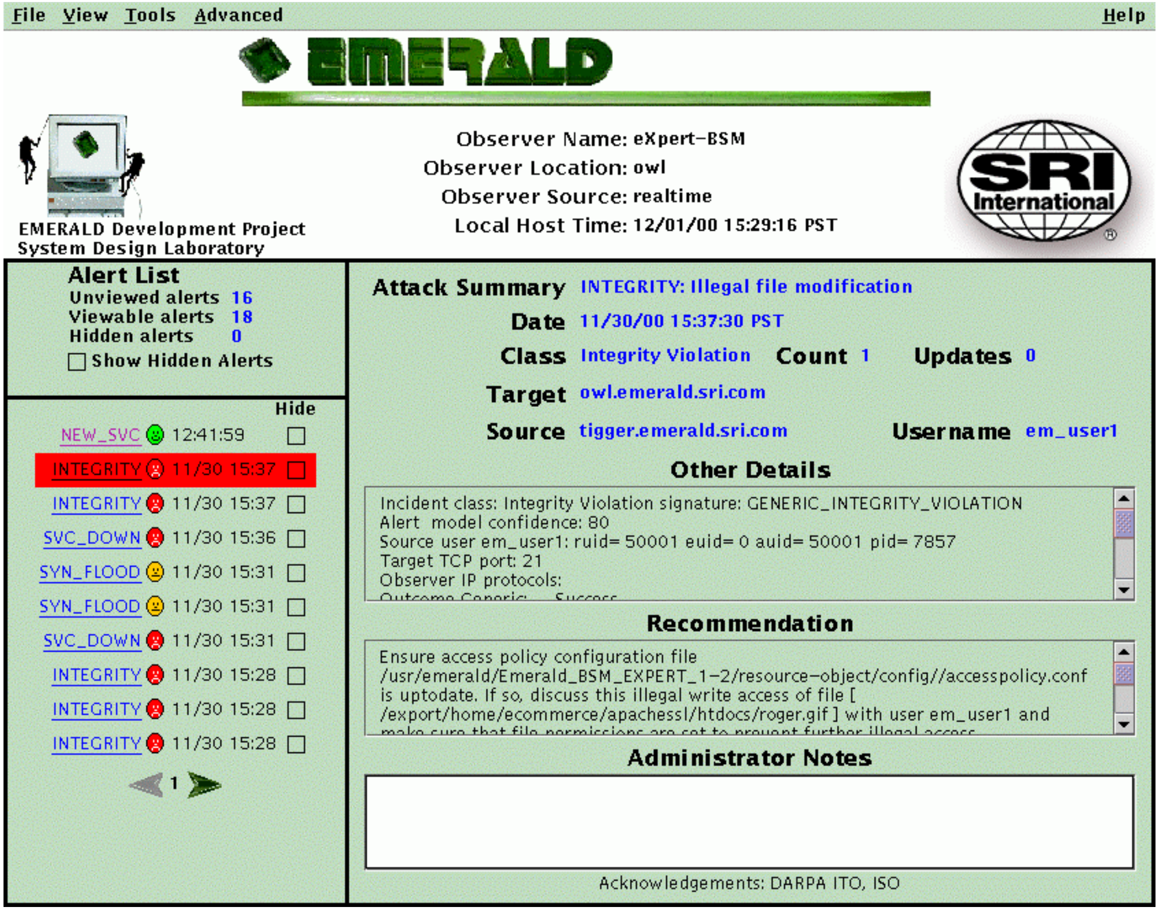
The TimeZone item allows you to select from 32 distinct timezone formats for displaying alert timestamps. Selecting this item causes a selection menu with these 32 timezone names to appear.

Tools Menu: The Tools menu has four options: Email, Print, Respond, and Search. Email brings up the currently selected alert description in a new window and allows the GUI operator to send an email message off to any valid email address. Email is described in more detail near the end of this document. Print sends the currently selected alert to the default installed printer connected to your computer, if one exists. If no printer is installed or properly configured this feature does not work. Currently, the Respond and Search features are not implemented.

Advanced Menu: The Advanced menu has three options: All Alerts , Email Preferences, and Auto-Hide. All Alerts has three options: Set Viewed marks all the currently available alerts as viewed, thus displaying them with purple text; Set Hide hides all alerts in the Alert List as described below; Auto-Hide provides filtering criteria that allow you to specify whether incoming alerts should automatically be hidden. Using the Auto-Hide feature, one can filter incoming alerts by alert name, observer name, or by severity level. Email Preferences has two options: Set Sender allows the user to configure who is operating the GUI and thus who is sending the email; Set SMTP Server allows the operator to set a new mail server if the one set in the ".config" file is not valid.

Help Menu: The Help menu has two options: Using Alert Viewer provides a brief description of this alert management interface, and About shows the current EMERALD copyright information.

EMERALD Alert Manager Main View



EMERALD Development Project
System Design Laboratory

Observer Name: eXpert-BSM
Observer Location: owl
Observer Source: realtime
Local Host Time: 12/01/00 15:29:16 PST

Alert List

Unviewed alerts	16
Viewable alerts	18
Hidden alerts	0

□ Show Hidden Alerts

			Hide
NEW_SVC	●	12:41:59	□
INTEGRITY	●	11/30 15:37	□
INTEGRITY	●	11/30 15:37	□
SVC_DOWN	●	11/30 15:36	□
SYN_FLOOD	●	11/30 15:31	□
SYN_FLOOD	●	11/30 15:31	□
SVC_DOWN	●	11/30 15:31	□
INTEGRITY	●	11/30 15:28	□
INTEGRITY	●	11/30 15:28	□
INTEGRITY	●	11/30 15:28	□

◀ 1 ▶

Attack Summary INTEGRITY: Illegal file modification
Date 11/30/00 15:37:30 PST
Class Integrity Violation Count 1 Updates 0
Target owl.emerald.sri.com
Source tigger.emerald.sri.com Username em_user1

Other Details

```
Incident class: Integrity Violation signature: GENERIC_INTEGRITY_VIOLATION
Alert  model confidence: 80
Source user em_user1: ruid= 50001 euid= 0 auid= 50001 pid= 7857
Target TCP port: 21
Observer IP protocols:
Outcome Generic:     Success
```

Recommendation

Ensure access policy configuration file /usr/emerald/Emerald_BSM_EXPERT_1-2/resource-object/config//accesspolicy.conf is uptodate. If so, discuss this illegal write access of file [/export/home/ecommerce/apachessl/htdocs/roger.gif] with user em_user1 and make sure that file permissions are set to prevent further illegal access

Administrator Notes

Acknowledgements: DARPA ITO, ISO

The main view is the one that will be displayed most of the time in normal operation. It consists of panels for title, alert list, alert description, and administrator notes. These are further described below.

Title Panel:

The Title panel is the top horizontal panel of the Main View window, and contains the alert management interface title with the EMERALD and SRI International logos. In the middle of the Title panel are four fields: Observer Name, Observer Location, Local Host Time, and Observer Source. Local Host Time is the current time on the host running the GUI updated every second. The other three fields are present only when an alert in the alert list is highlighted (the procedure to select an alert is explained below).

Alert List Panel:

The Alert List panel is on the far left of the GUI below the title panel described above. In the top box of the alert list is the number of unviewed, viewable, and hidden alerts. An alert is considered unviewed until the user selects it from the list of alerts below and has the alert's information displayed in the bottom right panel or until the user chooses Set Viewed from the Advanced menu. Viewable alerts are alerts that do not have their associated hidden flag set. Below the number of hidden alerts is a checkbox labeled: Show Hidden Alerts. If this is checked, all alerts that have been previously hidden are added to the list of alerts in the panel below. If this is not checked, only alerts which have not been hidden are displayed in the list below. In the space below the Show Hidden Alerts checkbox is room for a message which is not always visible. This message (in red font when visible) displays the number of alerts that have arrived into the GUI since the user last selected an alert for viewing. This message allows the user to keep track of new alerts when the GUI is left unattended. Below the alert list is a series of tabs containing the actual alerts. Each alert appears on a separate line that contains the alert name, a severity icon, and the timestamp indicating when the alert was generated. To select an alert, click on either the attack name or the severity icon. Once an alert is selected, its row is highlighted with a red box and its information is displayed in the Alert Description panel. As alerts are selected, their names change in color from blue to purple, similar to the color scheme of most web browsers.

The severity icon represents four possible levels of severity for alerts:

- Informative - Green smiley face
- Warning - Yellow face
- Severe Warning - Orange face
- Attack - Red frowning face

By default, the Alert List panel will display up to ten alerts. Two arrow buttons at the bottom of this panel are provided to switch between alert sets. The number between the two arrow buttons indicates the page number of the current Alert List panel. The arrow buttons are "grayed out" when there no additional alerts to view.

To the right of each alert is a checkbox that allows the user to optionally hide the corresponding alert. Hidden alerts are not displayed unless the Show Hidden Alerts checkbox is checked.

Alert Description Panel (center panel displaying alert content)

When one of the alerts is selected in the alert list describe above, this panel is filled out with the information present in the currently selected alert. At the top of this panel are the Attack Summary, Date, Class, Count, Update, Victim, Attacker, and Username fields. The Attack Summary line contains the name of the attack followed by a colon and a short description of the attack. The Date line contains the starting time of the attack. If the attack spanned a period of time, it also contains the ending time of the attack. The Class field contains the class name of the attack (typically, an attack class encompasses a number of specific attack signatures). The Count represents the number of individual occurrences of the malicious phenomena encountered by the intrusion detection tool. The Update field represents the number of updates to the particular alert that have been received by the Alert Management Interface. EMERALD sensors have the ability to produce multiple alerts regarding a single intrusion incident, providing additional information during the duration of an attack. These alerts are associated under a single reporting *thread*; this common thread is recognized and alert entries are automatically updated or overwritten in the Alert Management Interface.

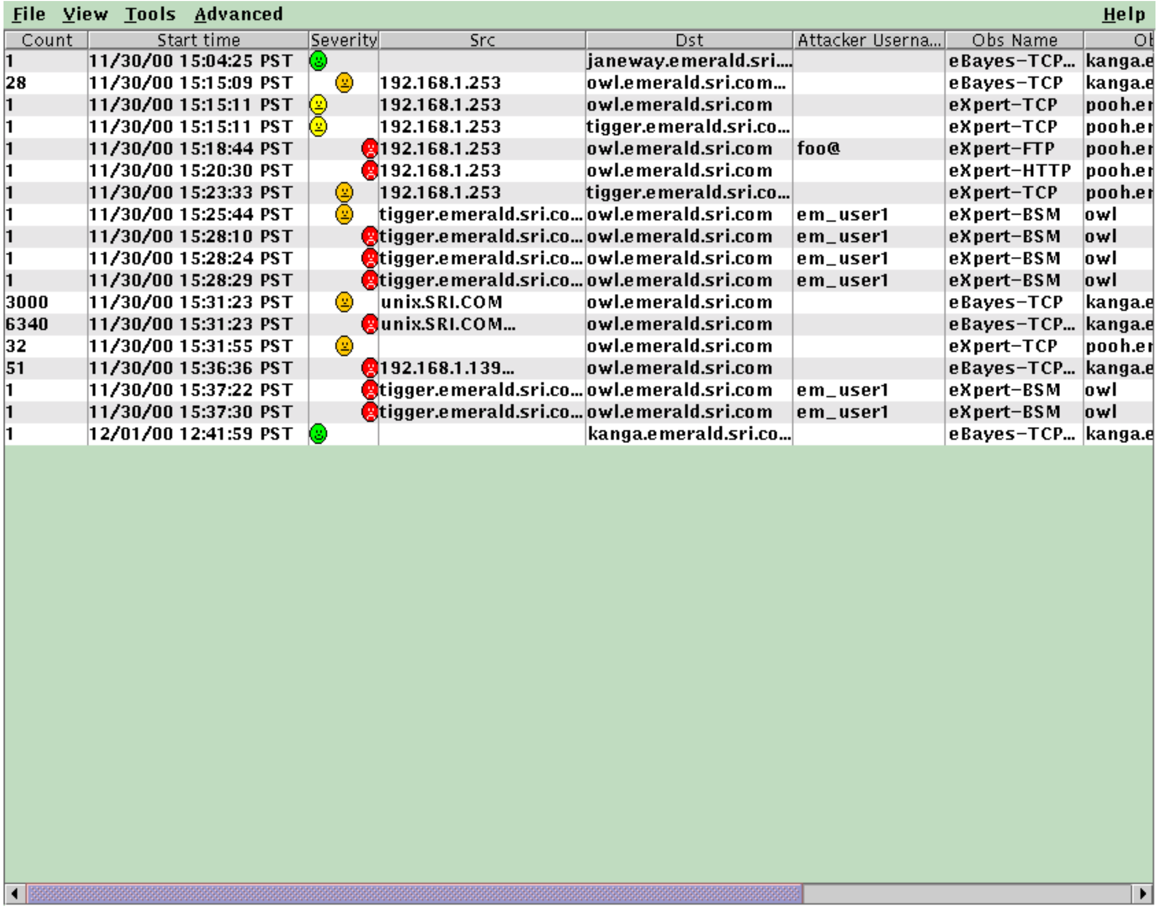
Victim shows the host name of the computer being attacked or the IP address (use the View menu Do IP-Name Lookup feature to toggle between IP and symbolic host name displays). If multiple computers were attacked then the host name is followed by the string "…". Attacker shows the host name of the computer that initiated this attack if known, otherwise "Unavailable" is displayed. The Username field contains the attacker's username, if known.

The "Other Details" section displays all other information known about the alert depending on the attack type and sensor. The attacker's ruid, euid, auid, or pid information is displayed, if available. If the attacker's command or parent command are known, they are displayed. If the alert pertains to an execution event, its arguments are shown. If the attack involves manipulation of a resource, the resource pathname and owner are shown.

Below the "Other Details" section is the "Recommendation" section. This section contains text explaining optimal countermeasures that should be performed to counter the intrusive activity.

At the bottom of the Alert Description panel is the "Administrator Notes" area. This section provides an area to record incident handling notes associated with the alert investigation. These notes are stored in a history file associated with the alert report, providing a permanent record of annotations that may be shared with the security staff as EMERALD reports are processed.

EMERALD Alert Manager Table View

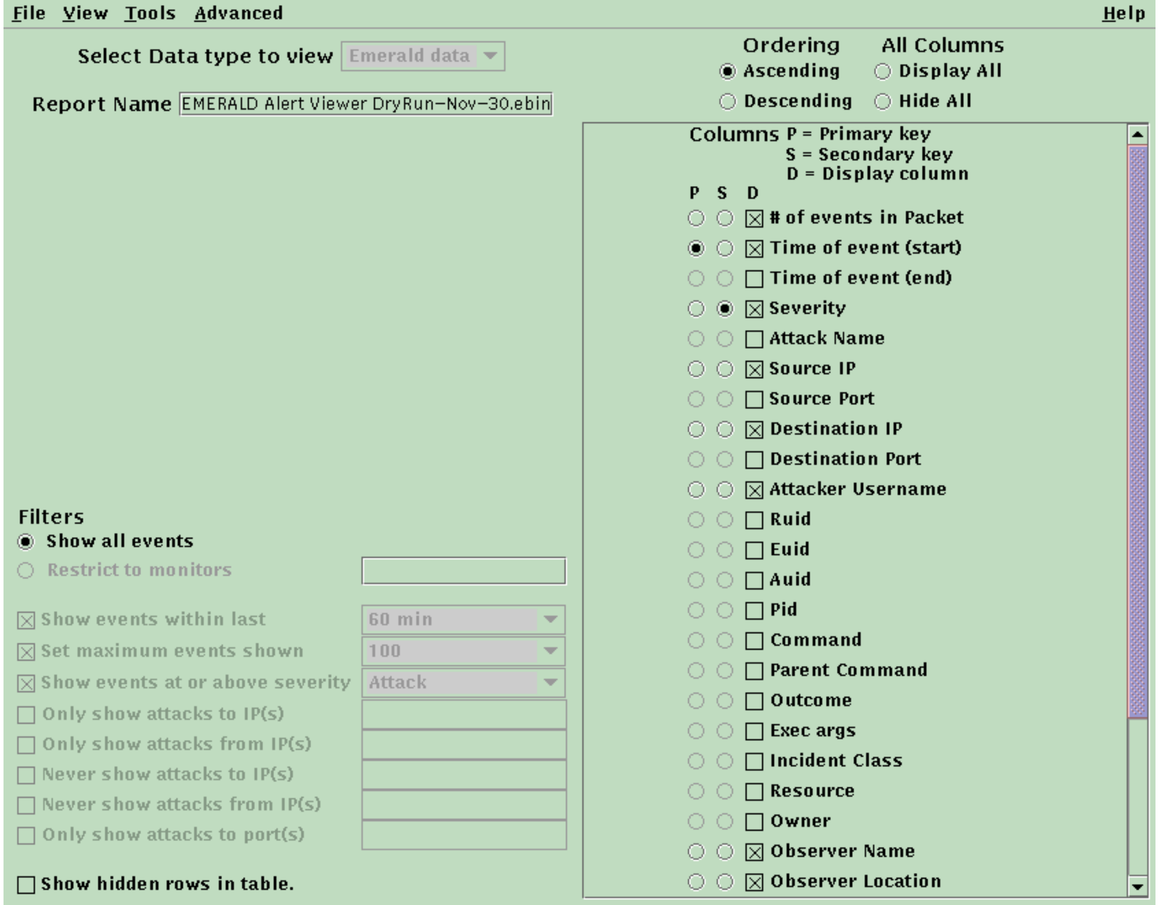


Count	Start time	Severity	Src	Dst	Attacker Userna...	Obs Name	Ol
1	11/30/00 15:04:25 PST	🟢		janeway.emerald.sri....		eBayes-TCP...	kanga.e
28	11/30/00 15:15:09 PST	🟠	192.168.1.253	owl.emerald.sri.com...		eBayes-TCP	kanga.e
1	11/30/00 15:15:11 PST	🟡	192.168.1.253	owl.emerald.sri.com		eXpert-TCP	pooh.er
1	11/30/00 15:15:11 PST	🟡	192.168.1.253	tigger.emerald.sri.co...		eXpert-TCP	pooh.er
1	11/30/00 15:18:44 PST	🔴	192.168.1.253	owl.emerald.sri.com	foo@	eXpert-FTP	pooh.er
1	11/30/00 15:20:30 PST	🔴	192.168.1.253	owl.emerald.sri.com		eXpert-HTTP	pooh.er
1	11/30/00 15:23:33 PST	🟠	192.168.1.253	tigger.emerald.sri.co...		eXpert-TCP	pooh.er
1	11/30/00 15:25:44 PST	🟠	tigger.emerald.sri.co...	owl.emerald.sri.com	em_user1	eXpert-BSM	owl
1	11/30/00 15:28:10 PST	🔴	tigger.emerald.sri.co...	owl.emerald.sri.com	em_user1	eXpert-BSM	owl
1	11/30/00 15:28:24 PST	🔴	tigger.emerald.sri.co...	owl.emerald.sri.com	em_user1	eXpert-BSM	owl
1	11/30/00 15:28:29 PST	🔴	tigger.emerald.sri.co...	owl.emerald.sri.com	em_user1	eXpert-BSM	owl
3000	11/30/00 15:31:23 PST	🟠	unix.SRI.COM	owl.emerald.sri.com		eBayes-TCP	kanga.e
6340	11/30/00 15:31:23 PST	🔴	unix.SRI.COM...	owl.emerald.sri.com		eBayes-TCP...	kanga.e
32	11/30/00 15:31:55 PST	🟠		owl.emerald.sri.com		eXpert-TCP	pooh.er
51	11/30/00 15:36:36 PST	🔴	192.168.1.139...	owl.emerald.sri.com		eBayes-TCP...	kanga.e
1	11/30/00 15:37:22 PST	🔴	tigger.emerald.sri.co...	owl.emerald.sri.com	em_user1	eXpert-BSM	owl
1	11/30/00 15:37:30 PST	🔴	tigger.emerald.sri.co...	owl.emerald.sri.com	em_user1	eXpert-BSM	owl
1	12/01/00 12:41:59 PST	🟢		kanga.emerald.sri.co...		eBayes-TCP...	kanga.e

The table view represents the alerts in tabular format. Each row of the display corresponds to an alert; the fields within the alert are shown in the columns. The fields are count, start time of the event, severity, source, destination, attacker username, observer (sensor) name, observer location, observer source, attack signature, and a check box to hide the alert. The horizontal and vertical scroll bars at the bottom and right of the display allow the user to scroll to the area of interest.

Not all sensors report all fields; for example, network sensors do not report process identifiers (pid). The rows can be sorted according to a particular field by clicking on the column label at the top of the column. To reverse sort a field, you may right-click on the column header with your mouse. Columns can be re-ordered by clicking on the column header and dragging it to a new location. The complete list of customizable fields is available in the table configuration view.

Table Configuration View



Select Data type to view: Emerald data

Report Name: EMERALD Alert Viewer DryRun–Nov–30.ebin

Ordering
● Ascending
○ Descending

All Columns
○ Display All
○ Hide All

Columns P = Primary key
S = Secondary key
D = Display column

P	S	D	
○	○	☒	# of events in Packet
●	○	☒	Time of event (start)
○	○	□	Time of event (end)
○	●	☒	Severity
○	○	□	Attack Name
○	○	☒	Source IP
○	○	□	Source Port
○	○	☒	Destination IP
○	○	□	Destination Port
○	○	☒	Attacker Username
○	○	□	Ruid
○	○	□	Euid
○	○	□	Auid
○	○	□	Pid
○	○	□	Command
○	○	□	Parent Command
○	○	□	Outcome
○	○	□	Exec args
○	○	□	Incident Class
○	○	□	Resource
○	○	□	Owner
○	○	☒	Observer Name
○	○	☒	Observer Location

Filters
● Show all events
○ Restrict to monitors

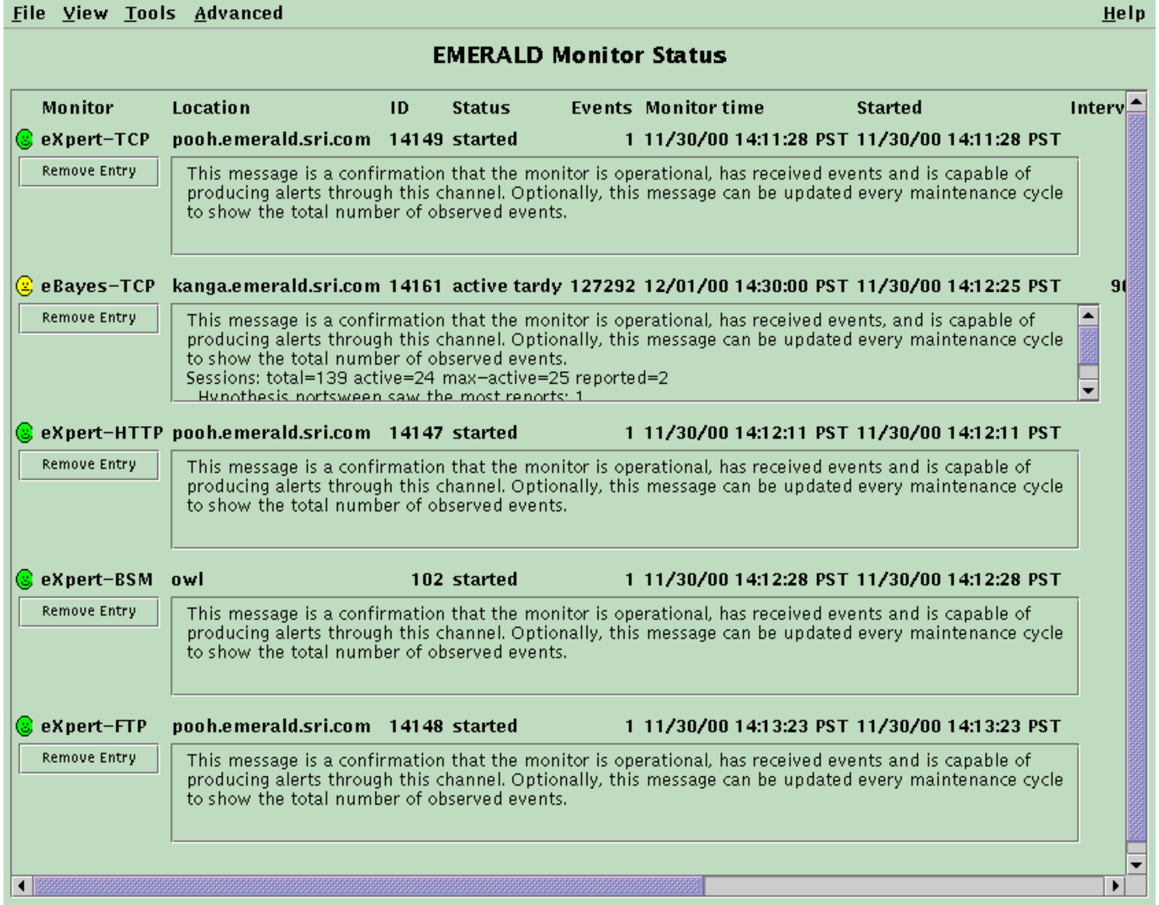
☒ Show events within last: 60 min
☒ Set maximum events shown: 100
☒ Show events at or above severity: Attack
□ Only show attacks to IP(s)
□ Only show attacks from IP(s)
□ Never show attacks to IP(s)
□ Never show attacks from IP(s)
□ Only show attacks to port(s)

□ Show hidden rows in table.

Alert Table Configurations

Selecting Table Configuration, from the View menu allows the GUI operator to customize the look of the table. In the top left corner is the data type to view. Currently only EMERALD Data is allowed so this option is not selectable. In the center-left region is the name of this report. Changing the name in the label will change the title displayed for this EMERALD Alert Viewer window the next time the table is displayed. In the bottom-left corner are various filters for screening which rows should be displayed in the table. Currently the only configurable option is the last one: Show Hidden Rows in Table. If this is selected, all rows are displayed in the table. If it is not selected (default), hidden rows are not displayed in the table. In the upper center region is the Ordering option, which allows ascending and descending ordering. In the upper right corner are the options for displaying or hiding all columns, which select or unselect the Display column checkboxes in the lower right corner. In the lower right corner are the Columns, which can be displayed in the table view. For each column the user can choose whether the column should be displayed or not with the checkbox in the "D" column. Columns are sorted based on both a primary key "P" and a secondary key "S". The primary key should be selected first, which will allow the rows to be ordered by the data in this column. The secondary key should be selected next, which allows the rows to be further sorted by the data in this column when data in the primary key field is equal.

EMERALD Alert Manager Status View



EMERALD Monitor Status

```
Monitor      Location               ID     Status        Events  Monitor time            Started                   Interv
eXpert-TCP   pooh.emerald.sri.com   14149  started            1  11/30/00 14:11:28 PST  11/30/00 14:11:28 PST
  This message is a confirmation that the monitor is operational, has received events and is capable of
  producing alerts through this channel. Optionally, this message can be updated every maintenance cycle
  to show the total number of observed events.

eBayes-TCP   kanga.emerald.sri.com  14161  active tardy  127292  12/01/00 14:30:00 PST  11/30/00 14:12:25 PST   9
  This message is a confirmation that the monitor is operational, has received events, and is capable of
  producing alerts through this channel. Optionally, this message can be updated every maintenance cycle
  to show the total number of observed events.
  Sessions: total=139 active=24 max-active=25 reported=2
    Hypothesis nortsween saw the most reports: 1

eXpert-HTTP  pooh.emerald.sri.com   14147  started            1  11/30/00 14:12:11 PST  11/30/00 14:12:11 PST
  This message is a confirmation that the monitor is operational, has received events and is capable of
  producing alerts through this channel. Optionally, this message can be updated every maintenance cycle
  to show the total number of observed events.

eXpert-BSM   owl                      102  started            1  11/30/00 14:12:28 PST  11/30/00 14:12:28 PST
  This message is a confirmation that the monitor is operational, has received events and is capable of
  producing alerts through this channel. Optionally, this message can be updated every maintenance cycle
  to show the total number of observed events.

eXpert-FTP   pooh.emerald.sri.com   14148  started            1  11/30/00 14:13:23 PST  11/30/00 14:13:23 PST
  This message is a confirmation that the monitor is operational, has received events and is capable of
  producing alerts through this channel. Optionally, this message can be updated every maintenance cycle
  to show the total number of observed events.
```

The EMERALD Alert Manager Status View shows all EMERALD monitors that are communicating with this instance of the AMI. For each monitor, the AMI displays the name, the location, the monitor ID, and the status. In this case, we note that eBayes-TCP is active but is tardy with respect to an expected heartbeat message. Its indicator is therefore yellow, indicating a warning condition. In the case above, this is an artifact of batch operation, as the GUI run time is well past the timestamps of the resolver file it is processing. In real time operation, if this warning condition persists, the user should check the status of the affected monitor.

Miscellaneous Features

<u>Printing:</u> Once an alert has been selected and its information is displayed in the bottom right panel, the user can choose to print it to have a hard copy of this information. If the user presses print and the computer running the GUI has a printer installed on it locally or available on the network, the contents of the GUI is printed to that printer. If no printer is installed or properly configured, this feature will not work.

<u>Email:</u> Also, once an alert has been selected, it can be emailed to anyone. For this feature to work properly, the operator must have edited the ".config" file prior to running the GUI. In the ".config" file are two lines one for <u>SMTPServer</u> which must be set to a valid SMTP server. The other line is for <u>MailSender</u> which should be set to the email

address of the person monitoring the GUI but can be set right before the email message is sent. After an alert has been selected, the user can press the Email button in the title panel. A popup will be displayed with a default subject line and a message containing the contents of the GUI's current alert. The To line must be filled in with the email address of the person whom this message should be sent to. The subject and message contents itself are both editable and can be modified or added to prior to pressing the Ok button on the email popup to send the message. If the Cancel button is pressed first, the message is not sent and the user is returned to the original GUI display.

Running the GUI

The AMI typically reads from a file of EMERALD messages. This file can be the output of a live process, or a previously processed file in batch mode. The file is expected to contain EMERALD alert messages. Such files are generated from EMERALD monitors or from a process such as eFunnel.

To invoke the AMI, connect to the appropriate directory and enter

```
./startGUI <EMERALD message file> &
```

To stop the GUI, either select the Exit option from the file menu, or enter the following from the same directory:

```
./ShutdownGUI
```

Alert Names Data Base

In the gui directory there is a file AlertCodeNameDB.txt. This is used to change the text the GUI displays for various signatures, outcomes, and so forth (for example, to translate the displayed text to another language). There are several code to name maps: the incident signature map, the more detailed full incident signature map, the incident class name map, the outcome map, the observer type name map, and the observer stream name map. These may be changed as needed; names that have embedded white space should be enclosed in quotes. The final two sections of the file allow the user to change the default severity map and set a default “autohide” for some alerts. The syntax for these operations is given in the file itself.

Version Status

EMERALD alert manager interface, Version 1.2, December, 2000. See the EMERALD software distribution web page http://www.sdl.sri.com/emerald/releases for further information regarding our follow-on release that will precede the expiration of this release.