For Security Analysts

NOTE: Assumption: necessary filters have built for your system.

Getting Started – Active Views Tab

In the Active Views tab, you can monitor events as they happen, performing queries on these events. You can monitor them in a table form or through a 3-D graphical representation. To get a Real-Time events started:

1. Click Active Views > Create an Active View, click the Filter down arrow, select a filter and click Select. Click Finish. To display just a 3-D graph, click the Display Events down arrow and select No.
2. To further filter your event table, right-click in the graph area and select properties. Here you can filter in certain types of events similar to when creating a filter. For instance, you can select to only view events that contain the word web in the event name field. This option is not permanent. You change this filter at any time.

Getting Started – Event Query Sample Scenario

During monitoring, you see numerous telnet attempts from source IP 189.168.10.22. Telnet attempts could be an attack. Telnet potentially allows an attacker to remotely connect to a remote computer as if they were locally connected. This can lead to unauthorized configuration changes, installation of programs, viruses, etc.

For Event Query to determine how often this possible attacker has attempted a telnet, you can setup a filter to query for this particular attacker. For example, you know the following: source IP is 189.168.10.22, destination IP is 172.16.10.10, Severity is 5, Event Name is Attempted_telnet and Sensor Type is H (Host Intrusion Detection). Do the following:

1. Click the Event Query button (magnifying glass icon) and click the Filter field down arrow.
2. Click Add, enter a filter name of "telnet SIP 189_168_10_22". In the field below the Filter Name, enter:
   - SourceIP = 189.168.10.22
   - EventName = Attempted_telnet
   - Match if, select (and)
   - Severity = 5
   - SensorType = H
   - DestinationIP = 172.16.10.10
3. Click Save. Highlight your filter and click Select.
4. Enter your time period of interest, click the search button (magnifying glass icon). The results of your query will appear. If you want to see how often in general this user is attempting telneting, remove DestinationIP, SensorType and Severity from your filter. The results will show all the destinationIPs this user is attempting to telnet to.

If any of your events are correlated events (SensorType = C or W), you can right-click > View Trigger Events to find what events triggered that correlated event.

NOTE: Another event of interest could be excessive FTP events. This can also be a remote connection, allowing for transferring, copying and deleting of files.

Below is a short list of attacks of interest. Types of attacks is an extensive list. For more information about network/host attacks, there are many resources available (i.e., books and the internet) that explain different types of attacks in detail.

- SYN Flood
- ICMP and UDP Flood
- Packet Sniffing
- Denial of Service
- Smurf and Fraggle
- Dictionary Attack

For Report Analysts

NOTE: Assumption: your Security Administrator has configured your Crystal Enterprise web server and published a list of available reports.

Getting Started – Analysis Tab

The Analysis tab allows for historical reporting. Historical and vulnerability reports are published on a Crystal web server, these run directly against the e-Security database. These reports can be useful to track and investigate activity over a large time frame, for instance a week or a month. These reports can also be used as a high level reporting method to your supervisors. If your reporting web server is installed, look in the navigator bar to see what reports are available.

For example, lets say you are responsible for generating reports to upper management within your organization. Chances are you will run a Top 10 report. There is a Top 10 Source to Destination IP Pairs on hosts names, ports, IPs and users. To run this report, do the following:

1. Expand Top 10 and highlight Top 10 Source to Destination IP Pairs Summary. Click the Create Reports button (magnifying glass).
2. Enter esecrpt as the username (for SQL Authenication or Oracle) or your Windows Authentication Report user name and enter your password.
3. Under Report Type, select Weekly Report (select Specific Date Range if you want enter a specific date range). Other reports may have additional parameters such as resource name and severity range.
4. Click View Report. You can export this file as a Word, PDF, rtf, Excel or as a Crystal Report.

Getting Started – Event Query

Similar to the Security Analyst, if you have an event or events of interest within your reports, you can run an Event Query under the Analysis tab. To run a query, highlight Historical Events > Historical Event Queries and click the Create Reports button. For more information, see Event Query Sample Scenario under the Security Analysts section.

Getting Started – Correlated Event Query

Correlation is the process of analyzing security events to identify potential relationships between two or more events. Correlation allows quick association of priority attacks based on common elements of event data.

If from your Event Query you find a correlated event of interest, you can query that correlated event as to what events triggered that correlated event. Right-click on a correlated event and select View Trigger Events.

For Administrators

Getting Started – Basic Correlation

For a brief explanation on what correlation is, see Getting Started – Correlated Event Query under Report Analyst.

In reference to the telnet scenario under Security Analyst – Event Query Sample Scenario, a Basic Correlation Rule can be created that will trigger a correlated event when 4 telnet attempts are done in a 10 second period. To create this correlation rule:

1. Go to the Admin tab and highlight Correlation Rules in the navigation bar. Create a new folder and place your rule in it. This done through a right-click option.
2. Highlight Basic Correlation, enter a name and click Next. In the next pane, click the down arrow and select Filter Manager. Click the Selected Filter down arrow and in the Filter Selection pane, click Add. Enter the following:
   - Name: telnet_attempt_189_168_10_22
   - Description: telnet attempt 189.168.10.22
   - SourceIP = 189.168.10.22
   - EventName = Attempted_telnet
   - select And
   - Severity = 5
   - SensorType = H
   - DestinationIP = 172.16.10.10
3. Click Save. Highlight your filter and click Select.
4. Click Next, enter the value of 4 for when condition is met and 10 seconds in the Threshold Grouping Criteria pane. Click Next.
5. In the Correlated Events and Actions pane, change the severity level to 2 (click the down arrow). Click Finish.
6. To deploy this rule, highlight Correlation Engine Manager in the Navigation pane, highlight a correlation engine, right-click > Deploy Rules. In the Deploy rules pane, find your rule and check mark it. Click OK. Ensure that your Correlation Engine and Correlation Rule have a green check marks indicating that they are enabled. This is done by right-clicking.
7. Under the Active Views tab, create a Active Views Events window using the correlation filter you created and when the telnet is attempted 4 or more times in a 10 second period, a correlated event will trigger. Right-click on the correlated event and select View Trigger Events to see how many telnet events (could be more than 4) triggered this correlation rule.

The above procedure can be applied to different types of events. For example, the above could be applied to ICMP or UDP. A large number of these protocols could result in a ICMP or UDP flood that could then result in a Denial of Service attack.

Changing Default User Passwords (esecadm, esecrpt, esecdba and esecapp)

For Oracle or MS SQL Authentication:

- esecadm – use the Sentinel Control Center
- esecapp - change it at the Sentinel DB using Enterprise Manager and update all container xml files ($ESEC_HOME/sentinel/config) using the dbconfig command.
- esecdba – change it at the Sentinel DB using Enterprise Manager and update the sdm.connect file using the SDM GUI or command line.
- esecrpt - change it at the Sentinel Database using Enterprise Manager. For MS SQL also change it in the ODBC DSN. For Oracle, no change to Oracle 9i Client.

For Windows Authentication:

All user password changes are done through the Windows Operating System. After changing the password in Windows, you must do the following additional items.

- e-Security Administrator – no change to any files or applications.
- e-Security DB Administrator - If you are running any SDM scheduled tasks, you will need to update the "run as user" property.
- e-Security Application DB User - On your DAS machine, update "log on as" for eSecurity Services. If applicable, also on the DAS machine, update the "run as user" property for all Advisor scheduled tasks.
- e-Security Report User – no change to any files or applications.

symptom: Two incidents get created while creating an incident

possible cause: This issue will arise if two or more Sentinel Servers are running in the same LAN. A machine with Sentinel Server installed should not point to another machine where another instance of Sentinel Server is running.

symptom: login failure due to timeout

possible cause: check your configuration.xml for proper IP address to Sentinel Server (sonic brokerURL, this is in two places).

possible cause: Communication layer (Sonic) is not running. For Unix as user esecadm, run: ps ef | grep –i sonic. If there isn't an instance of Sonic, you can start Sonic by entering /usr/local/bin/startcontainer.sh. For Windows, in the Services Window, start eSecurity Communications.

If you cannot get Sonic Started. *For Windows*, a lock may be present. Go to %ESEC_HOME%\sentinel\scripts and run remove_sonic_lock.bat. Restart Sonic. *For Solaris*, two lock files may be present. Go to $ESEC_HOME/sentinel/scripts and run ./remove_sonic_lock.sh. Restart Sonic.

possible cause: Database password is changed. Use the dbconfig utility to change your password. See the e-Security reference manual for more information.

possible cause: Check if DAS_Query (the process that handles login) is connected to Sonic using the Sonic Management Console.

1. (For Windows) Start > Programs > e-Security > SonicMQ > SonicMQ 6.1 > Management Console. (For Solaris) cd to $ESEC_HOME/ 3rdparty/SonicMQ/MQ6.1/bin and run ./startmc.sh.
2. Use the defaults settings (Domain Name: esecDomain and connection URL: tcp://localhost:10012). Enter esecadm or windows authentication user name and password. Click OK.
3. Click on the "Manage" tab. In the tree on the left, select Containers > esecContainer > esecBroker > Connections. Click on the Identity column to sort by Identity name. If DAS_Query is connected to Sonic, you'll see three DAS_Query's in the list.

If you don't see DAS_Query in the list, then that means either DAS_Query is not running or it not pointing to the right Sonic broker. Check the configuration.xml file to make sure it's pointing to the right Sonic Broker. Also check the bottom of the configuration.xml to make sure the DAS_Query process's "min_instances" property is set to one ("1"). If it's set to zero, watchdog will not attempt to start DAS_Query. If the configuration.xml file looks fine, check the DAS_Query log file in $ESEC_HOME/sentinel/log for errors.

symptom: problems with license validation during installation (on Windows platform)

possible cause: The HostId that you supplied when you requested a license key is different than the current value by running ./hostid.exe under the utilities directory on the install CD.

If the HostId returned does not match the HostId tied to your license key, you'll need to request another license key for the new HostId. If the HostId's match, try running the following:

1. Under the utilities directory on the install CD, run:

   set PATH=.;%PATH%

   .\softwarekey.exe –check serial_no license_key

If the program returns "Invalid Key" there is most likely a problem with the softwarekey.exe program, contact e-Security Customer Support.

symptom: problems with license validation after installation

possible cause: Check that the HostId that you supplied when you requested a license key is the same as the current value by running ./hostid.exe under the utilities directory on the install CD.

If the HostId returned does not match the HostId tied to your license key, you need to request another license key for the new HostId. If the HostId's match, try running the following:

1. On the command line, (*for Windows*) go to %ESEC_HOME%\utilties and run .\softwarekey.exe or (*for Solaris*) go to $ESEC_HOME/utilities and run ./softwarekey.
2. Select Option 3 to view the Primary Key.

If only "Press Enter to continue ..." is displayed, no Primary key has been entered. Follow the on screen instructions for setting the license key:

If "Invalid Key" is displayed, the Primary Key is invalid. Follow the on screen instructions for setting a new license key.

If the information about your valid key is displayed and if DAS_Query is reporting that it is not licensed to run on your machine, there is a problem with the license validator. Contact e-Security Customer Support.

possible cause: If you have multiple NICs on a machine, the NIC tied to your license must remain in the machine.

For windows, the hostid is determined by getting the list of NICs on the machine, then taking the first NIC in the list and using the last 8 digits of it's MAC address. To rearrange the order of your NICs:

1. Start > Settings > Control Panel, double-click Network and Dial-up Connections. In the menu bar, click Advanced > Advanced Settings...
2. In the Connections area is a list of network connections. This is the order that the hostid.exe gets the NIC cards MAC address. Use the up and down arrows to arrange the order and click OK.

---

symptom: Crystal will not run reports and throws a page server error.

possible cause: Not running the correct version of Crystal and/or running it on a non-supported platform. For Sentinel, Crystal 9 and Crystal 11 (BOE XI) are not forward or backwards compatible.

- Crystal 9 is only supported on Sentinel 5.1 and below and uses a concurrent user license key. In addition, e-Security only supports Crystal 9 on Windows 2000 Server with SP4.
- Crystal 11 (BOE XI) is only supported on Sentinel 5.1.1 and higher and uses a named user license key. In addition, e-Security only supports Crystal 11 (BOE XI) on Windows 2003 Server with SP 1.

Troubleshooting Linux Crystal Server

See the Sentinel Install Guide, Chapter 8, Utilities and Troubleshooting for Crystal BusinessObjects Enterprise™ 11.

---

symptom: In the Analysis and/or Advisor tab, Crystal Report list is not updated after loading new reports through Crystal Publishing Wizard.

possible cause: Reporting Configurations window under the Admin tab has not been updated. Go to the Admin Tab, highlight General Options, click Modify > Refresh (Analysis URL and/or Advisor URL) > Save. Logout of Sentinel Control Center and Log back in.

---

symptom: During Advisor startup, Advisor exits due to detecting an already running Advisor process.

possible cause: Due to an abnormal shutdown, such as a power outage. Go to <Advisor Data Feed Directory>/alert and to <Advisor Data Feed Directory>/attack and delete the .lock file.

NOTE: Location of your Advisor Data Feed Directory can be found in $ESEC_HOME/sentinel/config/alertcontainer.xml or $ESEC_HOME/sentinel/config/attackcontainer.xml under advisor.data.dir.

Useful Log File Directories

- **Sentinel Data Manager**
  $ESEC_HOME/sdm/SDM_*.0.log
- **iTRAC**
  $ESEC_HOME/sentinel/log/
- **Advisor**
  $ESEC_HOME/sentinel/log/
- **Event Insertion (das_binary), Database Queries (das_query) and Active Views (das_rt)**
  $ESEC_HOME/sentinel/log/
- **Agent Manager (service wrapper is agent-manager.log)**
  $ESEC_HOME/wizard/logs/

NOTE: The above UNIX paths are the same for Windows.

For DBAs

symptom: If you get a message that the Message Bus database is corrupt.

possible cause: For Oracle, the database most likely got corrupted during startup or shutdown. Perform the following:

1. su to root and cd to /etc/rc3.d. Move the S98sentinel to xS98Sentinel and If present, move S99wizard to xS99wizard
2. Reboot. The above will insure that no e-Security processes will start.
3. Login as esecadm and cd to $ESEC_HOME/3rdparty/SonicMQ/MQ6.1
4. Back up the SonicMQDB directory and the Sonic log directory
5. cd to $ESEC_HOME/3rdparty/SonicMQ6.1/MQ6.1/bin
6. Purge the database, run ./dbtool.sh -d a
7. Reload the database, run ./dbtool.sh -c a
8. cd to $ESEC_HOME/3rdparty/hp and start the e-Security processes, run ./hp_startesec
9. Look for errors. Start Wizard (if you have one), run ./hp_startewiz
10. su to root and move xS98sentinel to S98Sentinel and If applicable move xS99wizard to S99wizard.

---

symptom: Database query failing with the following error:

ORA-01502: index 'ESECDBA.EVT_EVT_ID_IDX' or partition of such index is in unusable state

possible cause: Partition operation was performed on a partition that contains data. The local indexes need to be rebuilt. To do so:

1. Connect to SQL*Plus as ESECDBA. At the SQL prompt (SQL>) enter:

   SQL> select p.index_name, p.partition_name from user_ind_partitions p, user_indexes i where p.index_name = i.index_name and p.status <> 'USABLE';

   SQL> alter index <index_name> rebuild partition <partition_name>;

How to ensure your Oracle database is running:

1. Check for processes, enter: 'ps -ef | grep oracle'. You should see multiple processes owned by oracle. If you do not, restart the database.
2. ping the Oracle (ESEC is default, this is your Net8 alias) listener by entering: 'tnsping ESEC'. If it does not, restart the listener as user Oracle (lsnrctl start). See your Oracle documenation for more information and for any errors you may receive.
3. Try to login to the server as esecadm (sqlplus esecadm/<password>@esec). See your Oracle documenation for more information and for any errors you may receive.

Oracle Quick Guide

1. Starting and stopping the database as sysdba in sqlplus:
   - Start
     SQLPlus> startup
   - Shutdown
     SQLPlus> shutdown immediate
2. Listener status/start/stop as user Oracle
   - Status
     lsnrctl status
   - Start
     lsnrctl start
   - Stop
     lsnrctl stop

Best Practice - Also available in the Installation guide is a Best Practices chapter that addresses installation and maintenance best practices. Some specific topics are hardware recommendations, disk array configuration, network configuration, patches, kernels, database analysis, correlation engine and logs.

Technical Assistance

- For Customer Support, email at support@esecurity.net
- For general information, email at info@esecurity.net
- Website: www.esecurity.net
- For 24x7 support, call the customer support desk directly at 800-474-3131

Before Calling Customer Support:

Before calling Customer Support, at a minimum have the following information available:

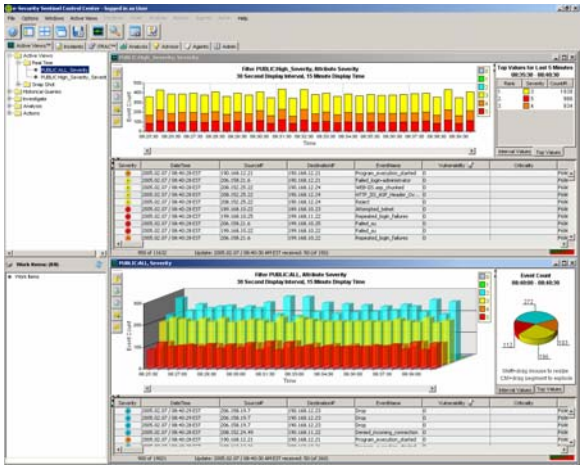
- e-Security version
- Database version
- Configuration
- OS version

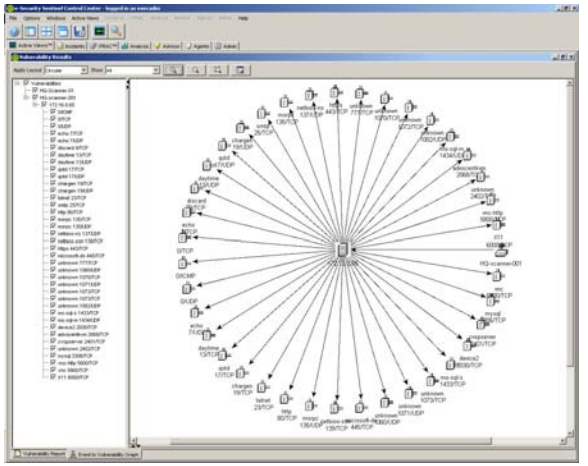
On a per request basis, Customer Support has a utility script that will pipe your configuration information (Solaris only) to a recon.tar file.

e-Security™ v5.1.1

- Windows
- Solaris
- Linux

Quick Reference Guide





March **2006**