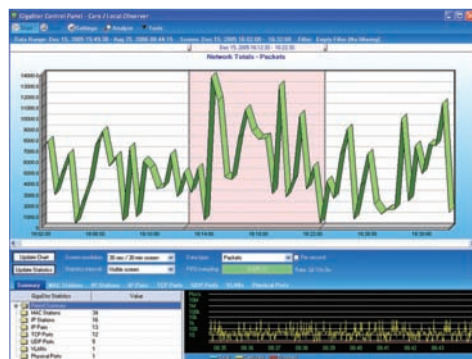


GigaStor lets you reconstruct traffic streams for user sessions and view Web pages, images, and IM and e-mail messages as the end user saw them.



When a time interval has been selected, traffic can be played back or analyzed based on pre-packaged or custom rule sets.

pairs, traffic level, behavioral rules, and most other factors that can reasonably be considered for this kind of task.

Remember that time at 23:49?

The real power of GigaStor emerges when you begin examining the packets you've captured using some of the embedded analysis and replay tools. The analysis takes place in an Observer main window, using a straightforward tabbed interface. In the control panel tab, you get a graphical display of network activity (a rough activity level line graph) with a timeline across the top. You can click on a range of time (from hours down to milliseconds) and run the expert analysis tool on the network traffic. Here you get a detailed breakdown of the traffic contents and you can reconstruct and replay contents, including VoIP calls, certain streaming media types, Web sessions, and instant messaging, allowing you to listen to phone calls and streamed audio and view Web pages and video just as the user heard and saw them. There are some limitations to the playback capabilities, but they're common-sense restrictions. Observer won't, for example, decode SSL tunnels unless

you provide the key.

The expert analysis and session playback are the strongest pieces of GigaStor's forensic and analytical toolbox. With the tools, you can not only see the names and traffic types within packets flowing across the network, you can look inside files that have been transferred and data streams transmitted to see whether the contents are as harmless as the name implies. At this point, a caveat is in order: Although the Observer tools are quite easy to use, they assume that the user is a data security professional. A neophyte parked in front of an Observer window will face a nearly vertical learning curve before becoming proficient in data security. If, on the other hand, you put GigaStor in the hands of competent professionals, they will be able to glean useful information from the Observer interface almost immediately.

Filtering activity

Once you identify the traffic within the capture that interests you, you can become more proactive in gathering additional information. You may set up more targeted filtering, establish traffic capture based on addresses or behavioral rules, set flags, or incrementally move through the conversation packet by packet (if you managed to miss the beginning, end, or exciting climax of the transaction). In the most basic terms, if you know when an incident happened, GigaStor gives you the tools to figure out what the entire incident consisted of.

The tabbed interface is very easy to use, allowing you to stroll through the various capture or gross analysis functions, and then walk the specific tasks within each of those. At each level you can get a great deal of information from the large and small preset tabs. The forensic analysis tab within the Decode and Analysis (Expert Analysis) group uses a preset filtering and behavioral rule set, but you can also upload Snort rules into the tool, change alert settings, and edit specific rules using a built-in editor to fine tune the forensics to your own needs.

The same powerful combination of preset rules and rule-editing capabilities runs throughout the Network Observer's interface. It's a powerful combination of features that lets an admin get started quickly yet still gives the ability to fine tune and customize as time goes on.

Analysis with Observer

Forensics and compliance aren't the only tasks that GigaStor can support. For network engineers more concerned with performance than security, the Observer's Trending Analysis can be quite useful. It's relatively simple to define network, IP address, VLAN, and application traffic to display and analyze across broad trend lines. Once basic network parameters are established, you set a time interval for GigaStor to sample and use to establish the basis for the trend. After the baseline is established, GigaStor resamples at intervals you set to compare against the baseline and show changes.

An appliance that can provide information for both network engineers and security professionals while saving complete network traffic data for as long as a year can be tremendously valuable for performance monitoring, network forensics, and compliance assurance. The multiple uses are a good thing because this won't be the cheapest network appliance you buy. It may, on the other hand, be one of the most cost-effective if it lets you successfully solve even one significant security event. The Observer application won't replace network security training, but like any good tool, it will amplify the impact of your trained staff's knowledge, and that could help them stay a crucial half-step ahead of the bad guys.

— Curtis Franklin Jr.



www.networkinstruments.com
For U.S. inquiries please call
1-800-526-7919

For Europe inquiries please call
+44 (0) 1959 569880

For all other inquiries please call
+1 952 358 3800