K2 DEFENDER

ANALYST CONSOLE

Navigation Toolbar

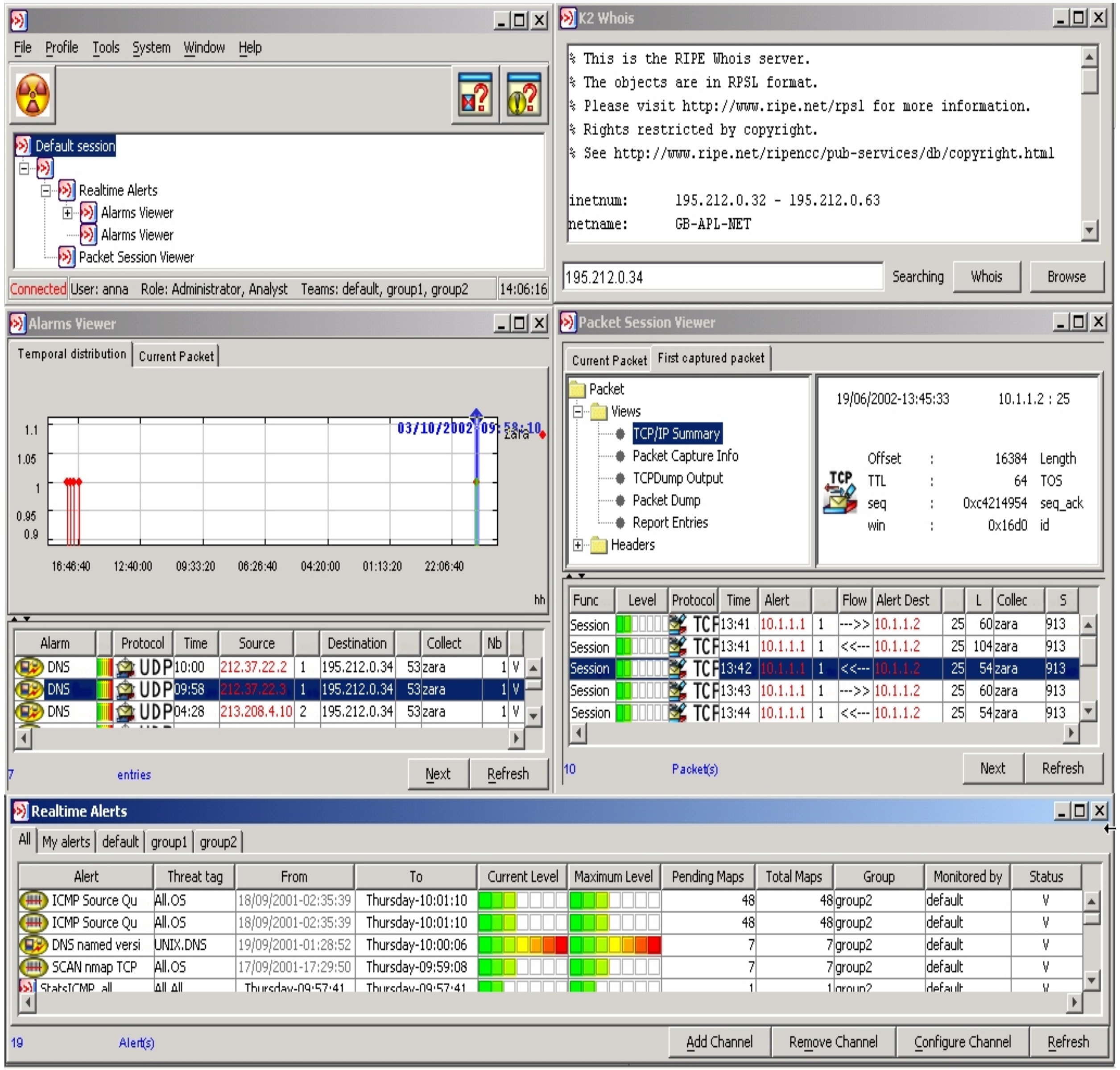
Used to launch and locate all other Analyst Console windows, the toolbar also allows you to save and restore any analysis sessions in progress.

Alarms Viewer

Each Alert is made up of one or more alarms. Double clicking on a real-time alert opens the Alarms window and displays the temporal distribution of alarms being raised on sensors. Detailed information is available down to the packet level.

Temporal Distribution Tab

Giving a birds-eye view of an incident as it occurs on your network, the temporal distribution view enables the security analyst to analyse specific incidents, look for patterns and enable alerts to be grouped. This provides invaluable input to threat assessment.



Connected User: anna Role: Administrator, Analyst Teams: default, group1, group2 14:06:16

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum:      195.212.0.32 - 195.212.0.63
netname:      GB-APL-NET
```

195.212.0.34

Alarm		Protocol	Time	Source		Destination		Collect	Nb	
DNS		UDP	10:00	212.37.22.2	1	195.212.0.34	53	zara	1	V
DNS		UDP	09:58	212.37.22.3	1	195.212.0.34	53	zara	1	V
DNS		UDP	04:28	213.208.4.10	2	195.212.0.34	53	zara	1	V

```
19/06/2002-13:45:33        10.1.1.2 : 25

Offset    :       16384   Length
TTL       :          64   TOS
seq       :  0xc4214954   seq_ack
win       :      0x16d0   id
```

Func	Level	Protocol	Time	Alert		Flow	Alert Dest		L	Collec	S
Session		TCP	13:41	10.1.1.1	1	--->>	10.1.1.2	25	60	zara	913
Session		TCP	13:41	10.1.1.1	1	<<---	10.1.1.2	25	104	zara	913
Session		TCP	13:42	10.1.1.1	1	<<---	10.1.1.2	25	54	zara	913
Session		TCP	13:43	10.1.1.1	1	--->>	10.1.1.2	25	60	zara	913
Session		TCP	13:44	10.1.1.1	1	<<---	10.1.1.2	25	54	zara	913

Alert	Threat tag	From	To	Current Level	Maximum Level	Pending Maps	Total Maps	Group	Monitored by	Status
ICMP Source Qu	All.OS	18/09/2001-02:35:39	Thursday-10:01:10			48	48	group2	default	V
ICMP Source Qu	All.OS	18/09/2001-02:35:39	Thursday-10:01:10			48	48	group2	default	V
DNS named versi	UNIX.DNS	19/09/2001-01:28:52	Thursday-10:00:06			7	7	group2	default	V
SCAN nmap TCP	All.OS	17/09/2001-17:29:50	Thursday-09:59:08			7	7	group2	default	V
StatsICMP_all	All.All	Thursday-09:57:41	Thursday-09:57:41			1	1	group2	default	V

Whois Window

The Analyst Console allows you to run *whois* queries from the source or destination IP addresses of events with a click of the mouse.

Packet Session Viewer

K2 can be used to capture entire TCP sessions. The Packet Session Viewer shows additional information about the data recorded by a TCP session capture, including the rule that triggered the session capture, the source and destination of the packet that raised the alert, the packet flow, and information about the sensor that collected the packet. Using this tool, the Analyst can drill-down into every packet captured in both directions.

Real-Time Alerts Window

The Real-Time Alerts window gathers together all the current security events happening on your network into one place. Each alert comprises one or more Alarms, or signature triggers. The Analyst can see at a glance the severity of an alert, when it was raised and when the last alarm was raised against it. Sophisticated sorting and filtering capabilities enable analysts to focus in and out of events, allowing them to switch between single incidents and the “big picture” with ease.