

The screenshot displays the LogRhythm Console interface. At the top, there are three charts showing event counts over the past 24 hours for 'Operations', 'Security', and 'Audit Events'. Below these is an 'Alarm List' table with columns for Alarm Date, Alarm Status, Alarm Rule Name, Events, Avg RB, Max RB, Entity, Last Updated By, Last Updated On, First Event Date, Last Event Date, and AlarmID. A 'Quick Search Tool Bar' is highlighted over the table. Below the table, an 'Expanded View' of the search bar is shown, displaying the search criteria: 'User', 'Value', 'trent.heisler', 'In the past', '7', 'Day(s)', 'Include', 'All Audit', 'Options', and 'Go'.

Alarm Date	Alarm Status	Alarm Rule Name	Events	Avg RB	Max RB	Entity	Last Updated By	Last Updated On	First Event Date	Last Event Date	AlarmID
12/22/2008 2:19:56.84	New	Critical Error	1	42.00	42.00	LogRhythm Labs	LogRhythm Labs	12/22/2008 2:19:57.21	12/22/2008 2:19:57.21	12/22/2008 2:19:57.21	105075
12/22/2008 2:10:12.17	New	Brute Force Attack	18	24.00	24.00	LogRhythm Labs	LogRhythm Labs	12/22/2008 2:10:12.17	12/22/2008 2:10:12.17	12/22/2008 2:10:12.17	105074
12/22/2008 2:07:34.42	New	Brute Force Slow	2	6.00	6.00	LogRhythm Labs	LogRhythm Labs	12/22/2008 2:07:34.42	12/22/2008 2:07:34.42	12/22/2008 2:07:34.42	105073
12/22/2008 2:04:58.05	New	Failed Remote Authentication	6	6.00	6.00	LogRhythm Labs	LogRhythm Labs	12/22/2008 2:04:58.05	12/22/2008 2:04:58.05	12/22/2008 2:04:58.05	105072
12/22/2008 2:02:55.30	New	Account Management Activity	14	2.00	2.00	LogRhythm Labs	LogRhythm Labs	12/22/2008 2:02:55.30	12/22/2008 2:02:55.30	12/22/2008 2:02:55.30	105071
12/22/2008 2:01:11.05	New	Brute Force Slow	14	25.00	25.00	LogRhythm Labs	LogRhythm Labs	12/22/2008 2:01:11.05	12/22/2008 2:01:11.05	12/22/2008 2:01:11.05	105070
12/22/2008 2:01:09.55	New	Brute Force Slow	14	25.00	25.00	LogRhythm Labs	LogRhythm Labs	12/22/2008 2:01:09.55	12/22/2008 2:01:09.55	12/22/2008 2:01:09.55	105069
12/22/2008 1:58:54.30	New	Suspicious Host [quick]	4	18.00	31.00	LogRhythm Labs	LogRhythm Labs	12/22/2008 1:58:54.30	12/22/2008 1:58:54.30	12/22/2008 1:58:54.30	105068
12/22/2008 1:57:04.05	New	Brute Force Slow	28	28.00	28.00	LogRhythm Labs	LogRhythm Labs	12/22/2008 1:57:04.05	12/22/2008 1:57:04.05	12/22/2008 1:57:04.05	105067
12/22/2008 1:50:49.80	New	Brute Force Slow	28	25.00	25.00	LogRhythm Labs	LogRhythm Labs	12/22/2008 1:50:49.80	12/22/2008 1:50:49.80	12/22/2008 1:50:49.80	105066
12/22/2008 1:50:49.80	New	Brute Force Slow	28	28.00	28.00	LogRhythm Labs	LogRhythm Labs	12/22/2008 1:50:49.80	12/22/2008 1:50:49.80	12/22/2008 1:50:49.80	105065

The LogRhythm Quick Search Toolbar enables users to launch a search quickly from any screen in the LogRhythm console based upon a variety of attributes such as email address, port, user, host, event type, time frame, etc. In this sample use case we're searching for all audit-related activity that a terminated administrator (Trent Heisler) performed during the 7 days prior to his termination