AutoRun Logger (User Interface)

The User Interface (UI) is split into four sections; Alerts, Single Host, Search and Data. The

Alerts

Alerts are generated by the analysis server. Alerts indicate that either a new autorun item has been added, an autorun has been modified (launch string, file path, SHA256) or an autorun has been deleted.

Single Host

The Single Host view shows the current AutoRun data for a single host. Individual AutoRun data can be downloaded as a CSV delimited file.

Search

The Search view permits simple searching of the Alert/Autorun data. The **Data** dropdown allows either the Alerts or Autorun data to be searched. The **Type** dropdown is used to search specific fields of the data type.

Export

The Export view allows the downloading of single sets of data. The exports available are:

- SHA256: All SHA256 hashes from the current autoruns data
- MD5: All MD5 hashes from the current autoruns data
- Domains: All domains from the current autoruns data
- Hosts: All hosts from the current autoruns data
- User: All users from the current autoruns data
- Host: All autoruns from a single host