Filtering syslog data to dev null

There may be events or hosts you do not want to receive in Splunk Connect for Syslog (SC4S) so they are not forwarded on to Splunk. SC4S can discard matching events as they are processed. This is achieved by editing the configuration files that work in unison to identify and enrich the events:

- **vendor_product_by_source.csv**, located in `/opt/sc4s/local/context`, and contains a “key” that is referenced in the log path for each data source
- **vendor_product_by_source.conf**, located in `/opt/sc4s/local/context`, and contains the filter to match events

The example edits below create a filter called "f_null_queue" that matches to the terms "discarded" OR "deny" and sends every event that matches to dev_null (Blackhole).

```ini
vendor_product_by_source.csv
  f_null_queue,sc4s_vendor_product,"null_queue"

vendor_product_by_source.conf
  filter f_null_queue {
    message('discarded')
    or message('deny')
  };
```

Next steps

These additional Splunk resources might help you understand and implement this use case:

- Blog: [Splunk Connect for Syslog: Configuration in depth](#)
- .Conf Talk: [Splunk Connect for Syslog: Extending the platform](#)
- Github: [Splunk Connect for Syslog](#)

Finally, you might be interested in other processes associated with the [Understanding best practices for Splunk Connect for Syslog](#) use case.