Adding compliance data to syslog data in stream

When routing data from Splunk Connect for Syslog (SC4S), you may need to add fields for compliance. For example, you may need tag data that come from the PCI zone. SC4S can attach indexed fields to matching events as they are processed. This is achieved by editing the configuration files that work in unison to identify and enrich the events:

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

The example edits below creates a filter called “f_pcidata” that matches to the 192.168.2.0/24 subnet and adds the fields “compliance”, “datacentre”, and “country” to every event that matches.

**compliance_meta_by_source.csv**

```
f_pcidata,fields.compliance,"pci"
f_pcidata,fields.datacenter,"DC1"
f_pcidata,fields.country,"New Zealand"
```

**compliance_meta_by_source.conf**

```
filter f_pcidata {
  netmask(192.168.12.0/24)
}
```

Next steps

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

- Blog: [Splunk Connect for Syslog: Configuration in depth](#)
- White Paper: [How Splunk Enterprise maps to 12 PCI compliance requirements](#)
- .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.