The combination of Logstash and Elasticsearch were chosen to handle the collection of sFlow records, with Logstash acting as the flow collector and Elasticsearch as the database where flow records are to be stored. In addition, Kibana, which is also created by the same founders of Elasticsearch and Logstash, can assist in record visualizations. Collectively, these three programs are referred to as the ELK stack and are used as the solution to a variety of problems. In our case, we can utilize the stack to handle flow collection. This solution was chosen because the programs are open source, scalable, and provide an API for post-processing of flow records. Resources online can assist in the setup of the server to utilize the ELK stack.

For installation, refer to:
https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-ubuntu-16-04.

To configure the ELK stack to use with flow records, steps can be followed at:
https://whiskeyalpharomeo.com/2015/06/13/logstash-and-sflow/.

Finally, once running, the elasticsearch API can be utilized to manipulate flow records. The API documentation is located at:
https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html.