**IBM QRadar**

This is *a Cloud-based service*, so it can be accessed from anywhere. The system covers all aspects of intrusion detection including the log-centered activities of a *HIDS* as well as the examination of live traffic data, which also makes this a NIDS. The network infrastructure that QRadar can monitor extends to Cloud services. IBM QRadar **employs deep learning to ease anomaly-based intrusion detection** and has a very comprehensive dashboard that integrates data and event visualizations.

**SPLUNK**

Splunk is a popular network traffic analyzer that also has NIDS capabilities. Security features of Splunk can be enhanced with an extensive tool, called **Splunk Enterprise Security**. This tool enhances the accuracy of anomaly detection and reduces the occurrences of false positives through the use of **AI and deep learning**. The extent of alerting can be adjusted by warning severity level to prevent your system administration team getting swamped up by an obsessive reporting module.