**Suricata:**

* Suricata is a free and open source, mature, fast and robust network threat engine
* This is capable of real time intrusion detection (IDS), Inline intrusion prevention (IPS), and network security monitoring (NSM)
* Suricata inspects the network traffic using a powerful and extensive rules and signature language, and has powerful Lua scripting support for detection of complex threats
* Suricata fast paced community driven development focuses on security, usability and efficiency

**Working:**

* Suricata works by getting one packet at a time from the system
* These are the pre-processed after which they pass to the detection engine
* Suricata can use pcap for this IDS mode, but also connect to the special feature for this IDS-mode, but also connects the special feature for Linux