

Distributed Deployment Data Flow Diagram Key All ports are TCP Forward (Sensor) Node Docker Container Bro/Zeek conn, dns, ftp, http, ssl ) Syslog-NG Curator Elasticsearch OSSEC Services : 55 Master Node 192.168.1.12 Sguil User Interface/Email Alert :7743 sguild SO db Logstash Logstash Kibana Elasticsearch Elastalert Redis Curator Curator

Security Onion

Operator 192.168.1.16