Sensor

- Detection Engine
  - Runs the detection engines against the network traffic
- Storage
  - Optionally saves packet data for later analysis
    - Encrypted with public key
    - Can save single packets, stream related packets, and/or all packets
- Reporting
  - Scripts provided to allow for automated reporting

Analyzer

- Storage
  - Uses data from the sensor
    - Decrypts with private key
- Reporting
  - Uses the reporting tool to generate interactive graphs from the saved logs

Included Tools

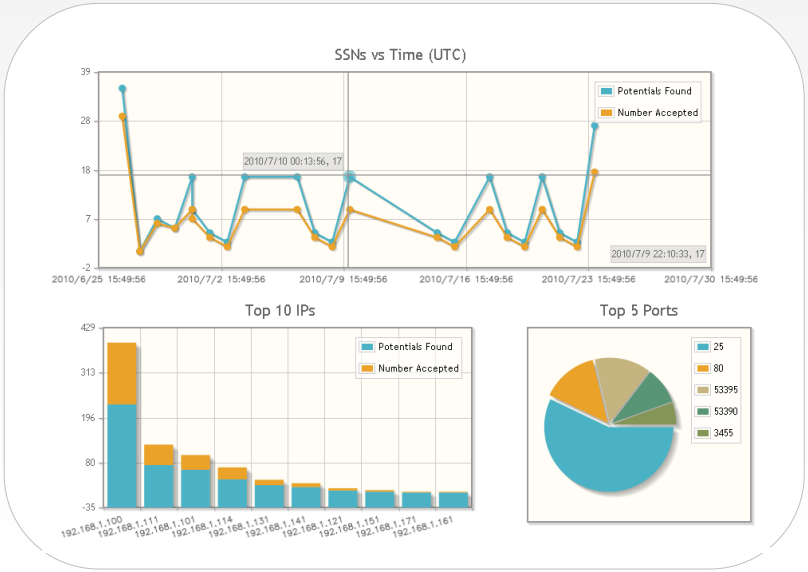
Detection Engine

- Parses the network traffic looking for the offending data
- Outputs the results to any or all of:
  - Standard out
  - Pcap dump files
  - Syslog
- Output can optionally be redacted and/or encrypted to protect the sensitive information

Report Generator

- Can run continuously reading the output of the detection engine
- Output formats include:
  - Comma Separated Values
  - HTML
    - Provides interactive graphs
- Option to periodically run a given command

Sample Report



Recommended Architecture

Sensor

- One sensor provided per subscription

Analyzer

- Multiple analyzers provided per subscription

Benefits of Separation

Minimizes the effects of compromise

- No access to the private key if the sensor is compromised

Less load on the sensor

- Focused on analyzing the traffic instead of report generation