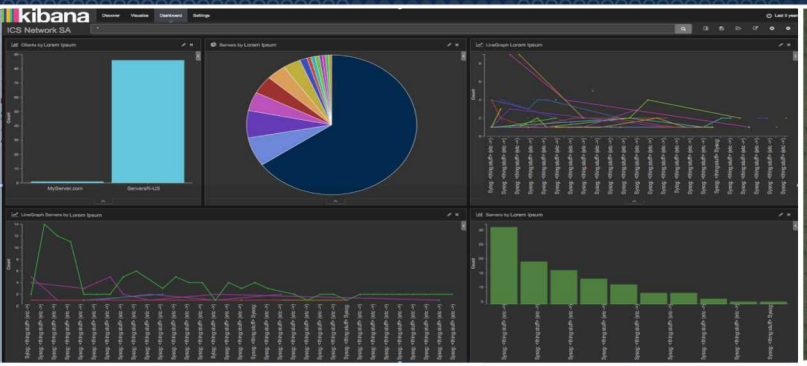
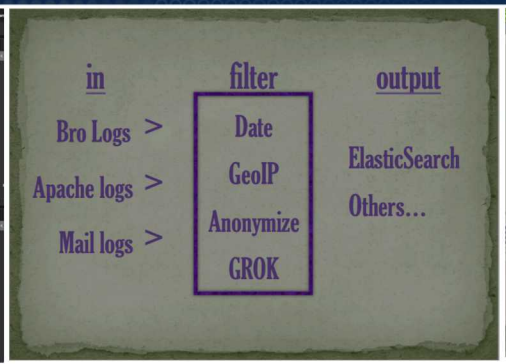
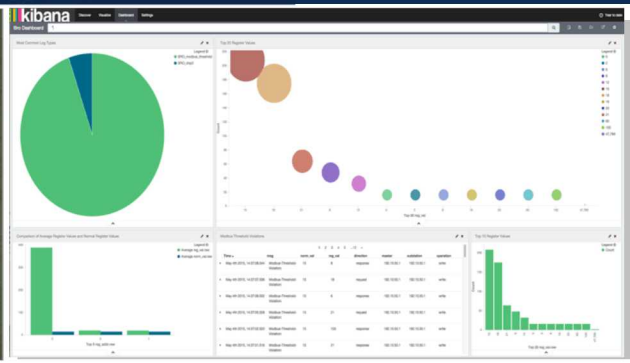
SAND2016-4246PE





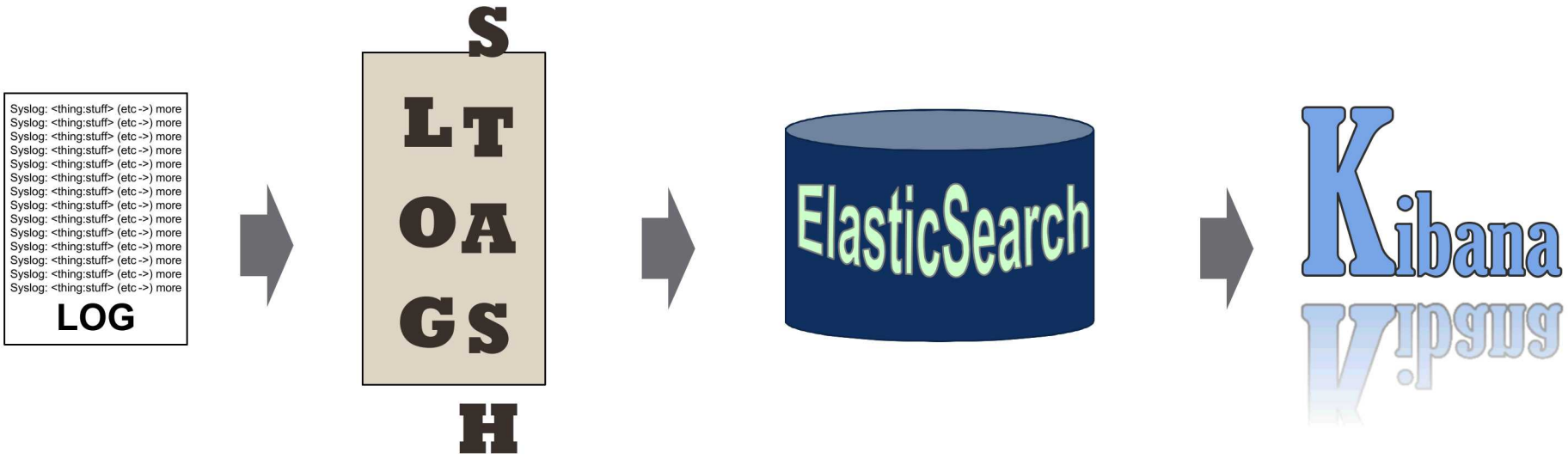


Visualization for ICS-CERT

Susan Wade

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

ICS Network Data Visualization



Data Visualization in Four Steps

Sandia National Laboratories

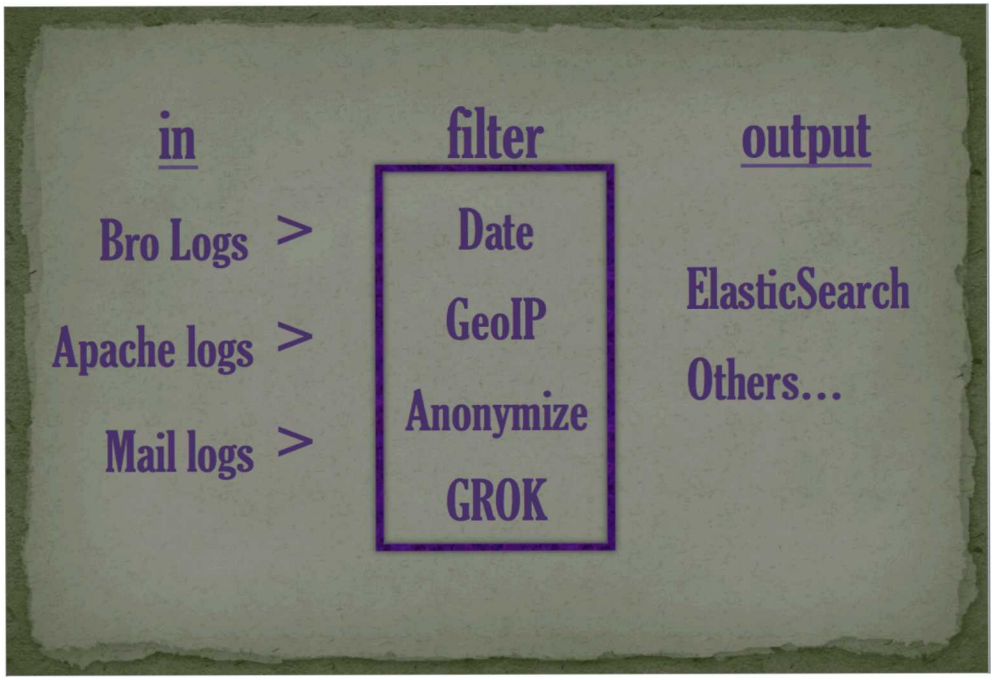
- Generate/gather log file(s)
- Create a Logstash configuration file
- Start servers
  - Elasticsearch server
  - Logstash
  - Kibana
- Open Kibana in a browser

Step 1: Generate Log File(s)

Sandia National Laboratories

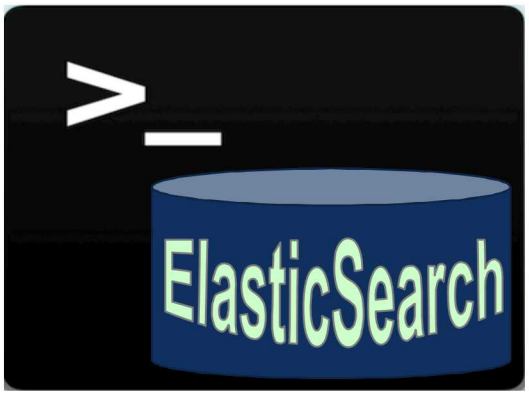
- Firewall logs
- Packet captures
- DNS logs
- IDS/IPS logs
- Flow data from routers and switches
- Host and application logs

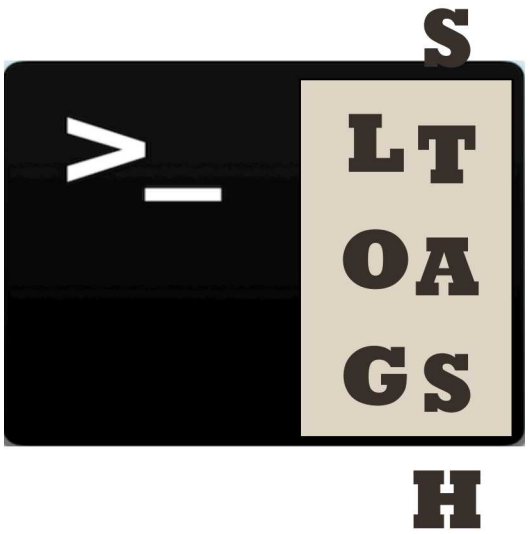
Step 2:Create a Logstash Config File



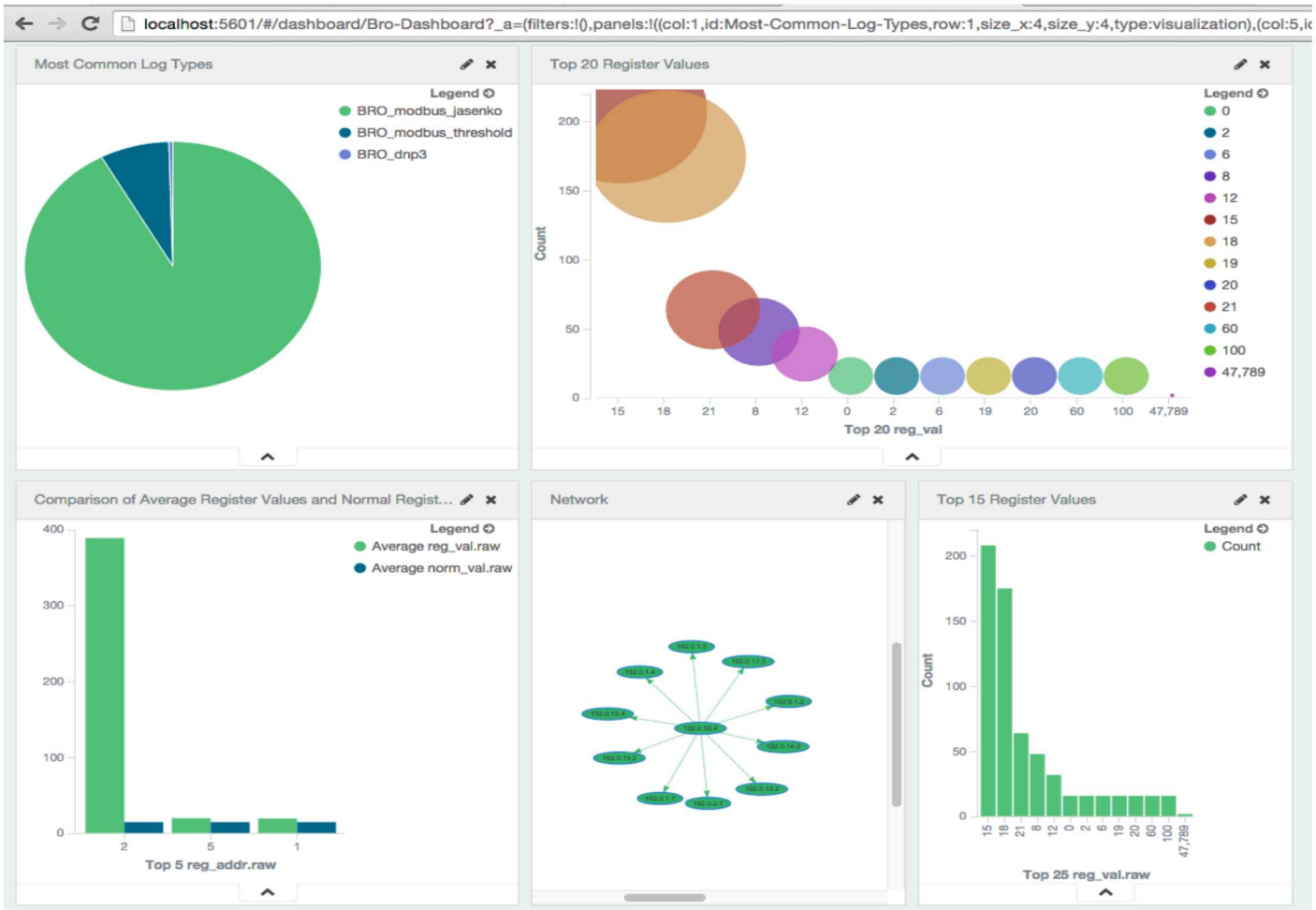

```
input {

#Production Logs####################
 file {
   type => "BRO_modbus"
   path => ”/logs/bro/modbus.log"
   start_position => "beginning"
 }
 filter {

 if [message] =~ /^#/ {
   drop { }
 } else {
 # BRO_modbus ###################
   if [type] == "BRO_modbus" {
       grok {
            match => [ "message", "(?<ts>(.*?))\t(?<fuid>(.*?))\t(?<tx_hosts>(.*?))\t(?<rx_hosts>(.*?))\t(?<conn_uids>(.*?))\t(?<source>(.*?))\t(?<depth>(.*?))\t(?
            <missing_bytes>(.*?))\t(?<timedout>(.*?))\t(?<parent_fuid>(.*?))\t(?<md5>(.*?))\t(?<sha1>(.*?))\t(?<sha256>(.*?))\t(?<extracted>(.*))" ]
       }
   }
 output {
     elasticsearch {
      embedded => true
      protocol => "http"
      host => "localhost"
   }
 }
```

Step 3: Start Servers





Step 4: Open Kibana in a Browser



Why Is this Work Important to ICS-CERT?

- Provides visibility into network operations
- Permits visualization of data in real time
- Allows analysts to quickly detect outlier values
- Allows analysts to verify network communications and layout

How Does This Work Fit into the ICS-CERT Workflow?

Sandia National Laboratories

- Enables analysis of ICS-Network historical data
- Provides visualization capabilities during on-site assessments
- Visualizations can be custom-built, specifically designed to meet ICS-CERT assessment needs

Next Steps

- Create additional ICS Network Specific Visualizations not currently available in Kibana
  - Scatter plot for rapid identification of outlier values
  - Additional advanced statistical analysis visualizations using data generated by Archimedes

Sandia National Laboratories

Questions

Supplemental Slides

Elasticsearch Startup Response

- `user$ elasticsearch-1.4.4/bin/elasticsearch`
- Verify that Elasticsearch is running
  - Command Line: '`curl -XGET localhost:9200`'
  - Browser: 'localhost:9200'


```
{
  "status" : 200,
  "name" : "Hobgoblin II",
  "cluster_name" : "FWTK_BroLogs",
  "version" : {
    "number" : "1.4.4",
    "build_hash" : "c88f77ffc81301dfa9dfd81ca2232f09588bd512",
    "build_timestamp" : "2015-02-19T13:05:36Z",
    "build_snapshot" : false,
    "lucene_version" : "4.10.3"
  },
  "tagline" : "You Know, for Search"
}
```

Logstash Startup Response

```
user$ logstash-1.4.2/bin/logstash -f myConfigFile.conf
```

```
{
    "message" => "1447099336.975096\tCsAUWF2YxL3aDTKdvg\t192.0.55.4\t50705\t192.0.1.4\t502\tREAD_COILS\t-”,
    "@version" => "1”,
    @timestamp" => "2015-11-09T20:02:16.975Z",
    "type" => "BRO_modbus”,
    "host" => ”mickey.sandia.gov",
    "path" => "/Users/mickey/Documents/logs/bro/modbus_logs.log”,
    "uid" => "CsAUWF2YxL3aDTKdvg",
    "orig_host" => "192.0.55.4",
    "orig_port" => "50705”,
    "resp_host" => "192.0.1.4”,
    "resp_port" => "502”,
    "function" => "READ_COILS”
}
{
    "message" => "1447099336.987151\tCxkn9y1TPtszBOXvM8\t192.0.55.4\t55827\t192.0.2.5\t502\tREAD_COILS\t-",
    "@version" => "1",
    "@timestamp" => "2015-11-09T20:02:16.987Z",
    "type" => "BRO_modbus",
    "host" => ”mickey.sandia.gov",
     ……
}
```

Kibana Startup Response

```
user$ kibana/grunt dev
```

Running "less:dev" (less) task
File /FWTK/BroBoundsViewer/kibana/src/kibana/components/agg_table/agg_table.css created.
……
File /FWTK/BroBoundsViewer/kibana/src/kibana/plugins/metric_vis/metric_vis.css created.
File /FWTK/BroBoundsViewer/kibana/src/kibana/plugins/markdown_vis/markdown_vis.css created.

Running "jade:clientside" (jade) task
File _FWTK/BroBoundsViewer/kibana/test/utils/istanbul_reporter/report.jade.js created.

Running "kibana_server" task
>> Server started on port 5601

Running "watch" task
Waiting...