

# Intro to Elasticsearch

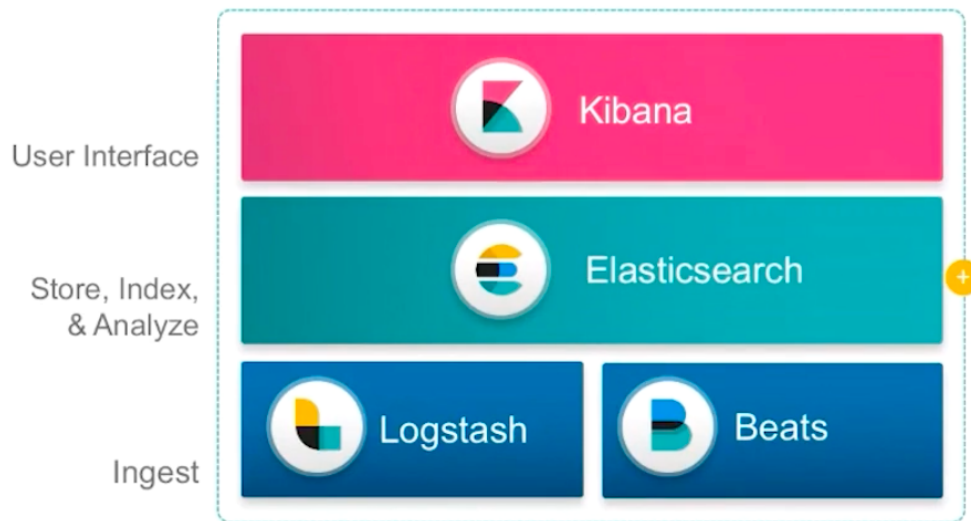
**Evan Yand**

**Vehicle Systems Engineer – TriMet**

[yande@trimet.org](mailto:yande@trimet.org)

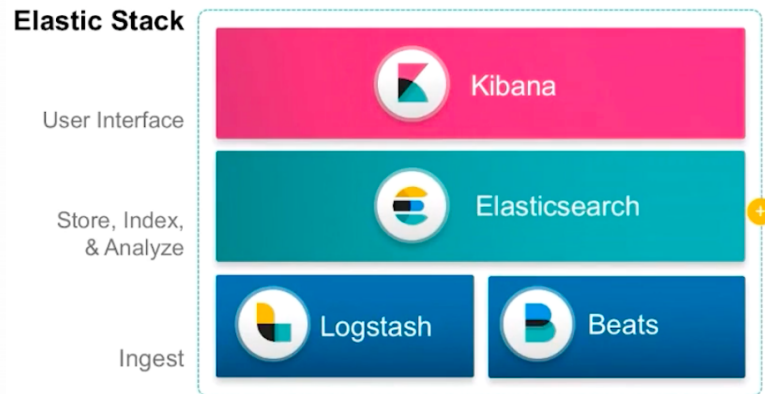
Portal User Group Meeting 2019-04-17

# Elastic Stack

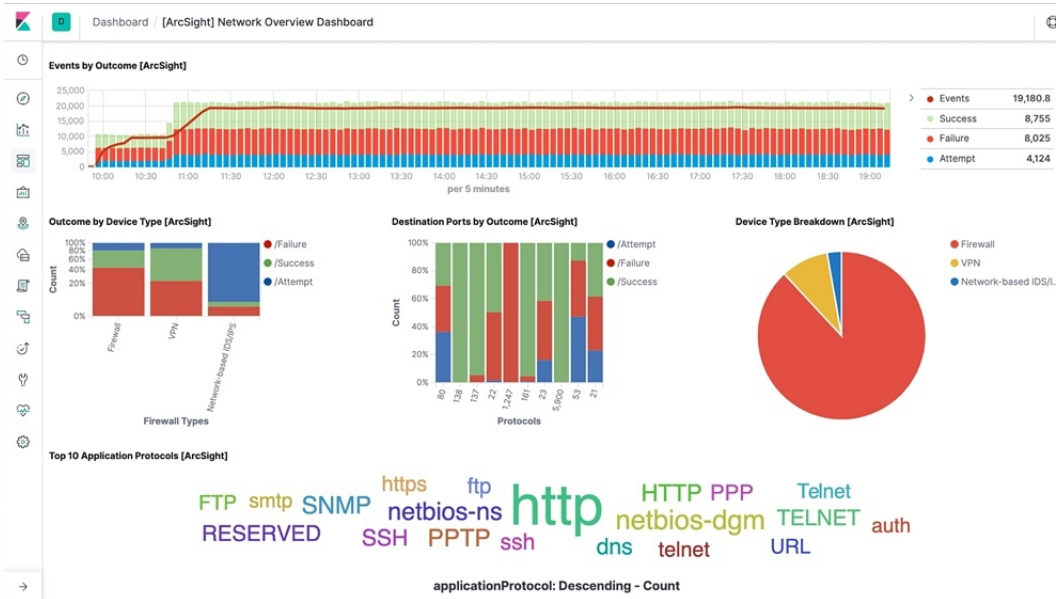


# Typical Use Cases

- **Network Monitoring**
- **Enterprise Search**
- **Site Search**
- **APM**



# Example Dashboard



# ITS Use Case

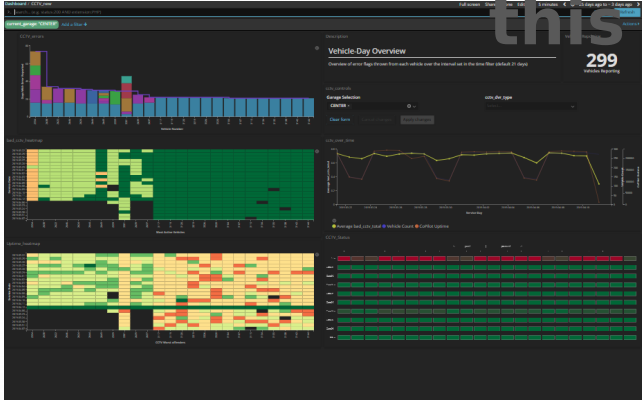
- **System health monitoring**
  - CCTV
  - Radio
  - CAD/AVL
- **Most monitoring currently handled in an Oracle DB**

# Improved Presentation

VEH	SVC_D	SRY	EC	F13	GAR_CU	GAR_DR	AA_CU	AA_DR	ON_RCH	HAS_STA	HAS_SCH	BAD_CEL	BAD_RAD	BAD_HF	BAD_PN	BAD_CC	DPLY_TY	BAD_IPR_FL	BAD_CU_FL	CDP_FL	IPR_FL	BAD_C	
2524	03/09/19 S	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/10/19 U	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/11/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/12/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/13/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/14/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/15/19 S	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/16/19 S	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/17/19 U	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/18/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/19/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/20/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/21/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/22/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/23/19 S	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/24/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/25/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/26/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2524	03/27/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	03/28/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	03/29/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	03/30/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	03/31/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/01/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/02/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/03/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/04/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/05/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/06/19 S	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/07/19 U	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/08/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/09/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/10/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/11/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/12/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/13/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/14/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/15/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/16/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/17/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/18/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/19/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/20/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/21/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/22/19 W	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2525	04/23/19 S	B	052	POWELL	POWELL	AA	AA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1



... to this



From this...

# Logstash

- **Based on Input, Output, and filtering plugins**
- **Supports parallel pipelines on a single instance**

# Logstash - Plugins

- **Input**
  - Elastic Beats, jdbc, http, twitter....
- **Filter**
  - Data extraction and formatting into typed fields
- **Output**
  - Elasticsearch, http, email, csv...



# Logstash filtering

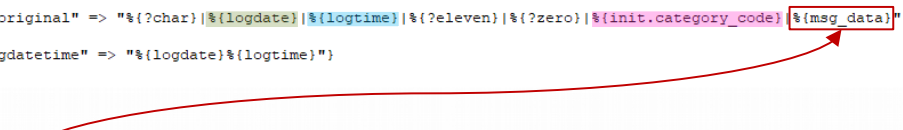
```

M|20170607|215119|11|0|20036|NxSharedInputButtonEmergency_1.1# 43: Emergency: Released
M|20170607|215119|11|0|20036|NxSharedInputPttRadioIn_1.0# 42: PttRadioIn: Deactivated
M|20170607|215119|11|0|20036|NxSharedInputHookDetection_1.2# 63: Hook: On-Hook
M|20170607|215119|11|0|20036|NxSharedInputVoltageK130_1.6# 152: Engine on (27584mV)
M|20170607|215125|11|0|20036|NxRadioTrunkedVoiceCtrl_1.27#1047: TVC: hook speaker pa ptt ch 0 P 118 DDEF CH SEC 0 P 118 Name DDEF
M|20170607|215126|11|0|20036|NxOperationCommands_1.9# 149: INPUT Door 1: CLOSED
M|20170607|215126|11|0|20036|NxOperationCommands_1.9# 149: INPUT Door 2: CLOSED
M|20170607|215126|11|0|20036|NxOperationCommands_1.9# 149: INPUT Yield: OFF
M|20170607|215126|11|0|20036|NxOperationCommands_1.9# 149: INPUT Kneel: OFF
M|20170607|215126|11|0|20036|NxOperationCommands_1.9# 149: INPUT Master Run Park: OFF
M|20170607|215126|11|0|20036|NxOperationCommands_1.9# 149: INPUT Hazard Light: OFF
M|20170607|215126|11|0|20036|NxOperationCommands_1.9# 149: INPUT Master Run Day: ON
M|20170607|215126|11|0|20036|NxOperationCommands_1.9# 149: INPUT Master Run Nite: ON
M|20170607|215127|11|0|20036|NxVolumeSetting_1.37# 699: Handset Speaker GRI volume: new=80 old=79
  
```

```

dissect {
  mapping => { "log.original" => "%{?char}|%{logdate}|%{logtime}|%{?eleven}|%{?zero}|%{init.category_code}|%{msg_data}" }
  add_field => { "logdatetime" => "%{logdate}%{logtime}" }
}

grok {
  match => { "msg_data" => "%{DATA:process}_%{NUMBER}#%{SPACE}%{INT}: %{GREEDYDATA:message}" }
  remove_field => ["msg_data"]
}
  
```



# Elasticsearch

- Data is stored in a Lucene based search engine
- JSON based RESTful APIs (among others)
- Horizontally scalable using data replication and shards across clustered servers

```
GET /_search
{
  "query": {
    "fuzzy": {
      "user": {
        "value": "ki",
        "boost": 1.0,
        "fuzziness": 2,
        "prefix_length": 0,
        "max_expansions": 100
      }
    }
  }
}

POST /_sql?format=json
{
  "query": "SELECT * FROM library ORDER BY page_count DESC",
  "fetch_size": 5
}

POST /_search
{
  "query": {
    "bool": {
      "must": {
        "term": { "user": "kimchy" }
      },
      "filter": {
        "term": { "tag": "tech" }
      },
      "must_not": {
        "range": {
          "age": { "gte": 10, "lte": 20 }
        }
      },
      "should": [
        { "term": { "tag": "wow" } },
        { "term": { "tag": "elasticsearch" } }
      ],
      "minimum_should_match": 1,
      "boost": 1.0
    }
  }
}
```

# Kibana

- **Dashboards**
- **On-the-fly filtering**
- **Stack monitoring and configuration**

# Next Steps

- **Machine Learning**
- **Additional Data Ingestion**
  - Vehicle Radio
  - Central Radio System
  - APC Health
  - Drivetrain Health

# DEMO

<http://yande.tri-met.org:5601>

(Internal Link)

<http://>

<itcs-cs-avl3.itcs.trimet.org:5601/app/kibana#/dashboard/aa787650-8e62-11e7-9ab0-5da0c857c101?>

[https://dae4c496501c4b149de1bdd6e5e8b0ac.elastic.trimet.org:9243/#?\\_g=\(\)](https://dae4c496501c4b149de1bdd6e5e8b0ac.elastic.trimet.org:9243/#?_g=())

# Appendix: Elastic Vocab

- **“Table” -> Index**
- **“Row” -> Event**
- **“Column” -> Field**