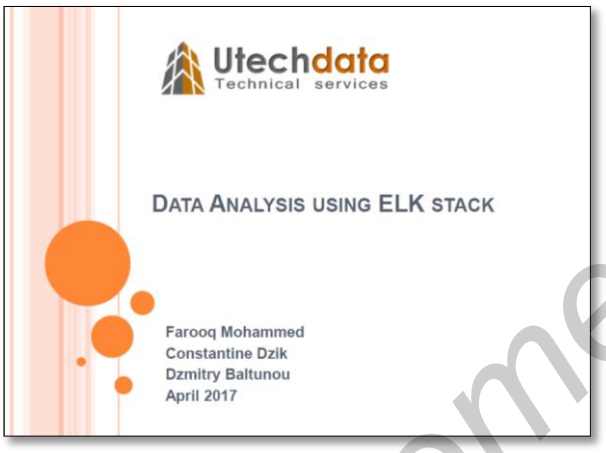
DATA ANALYSIS USING ELK STACK

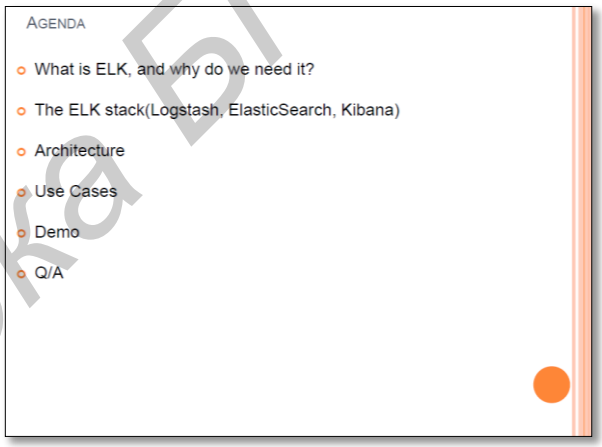
F. MOHAMMED
Utech LLC location – Madison

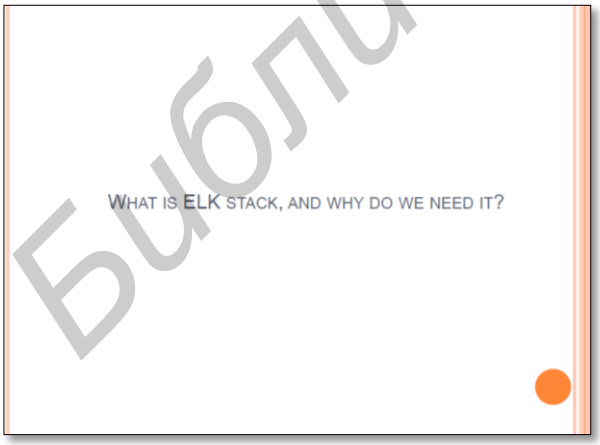
D. BALTUNOU
Utech LLC location – Madison

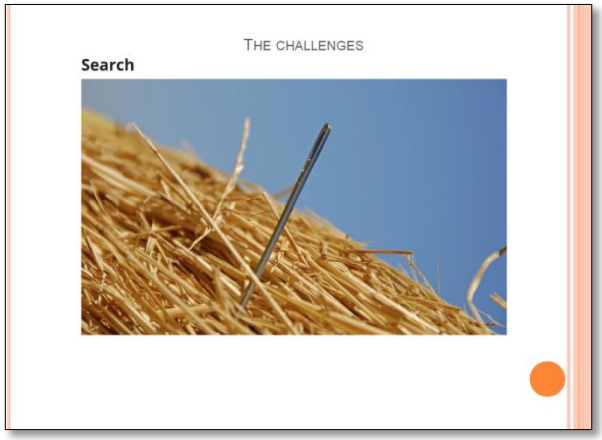
C.S. DZIK
Utech LLC location – Madison

Utech Solution Inc, Madison, USA
E-mail: constantine.dzik@utechdata.com









ONE SOLUTION: ELK

What is the ELK stack

- Elasticsearch
  - Search server
  - Based on Apache Lucene
- Logstash
  - Data pipeline
  - Processes logs and other data
  - Plugins
- Kibana
  - Web frontend for Elasticsearch

ELK Overview

Stack Components by Type
- Shippers
- Brokers
- Storage / Processing
- Visualization

Elasticsearch: NoSQL DB Storage
Logstash: Data Collection & Digestion
Kibana: Visualization standard.

THE ELK STACK(LOGSTASH, ELASTICSEARCH, KIBANA)

LOGSTASH

LOGSTASH CONFIG STRUCTURE