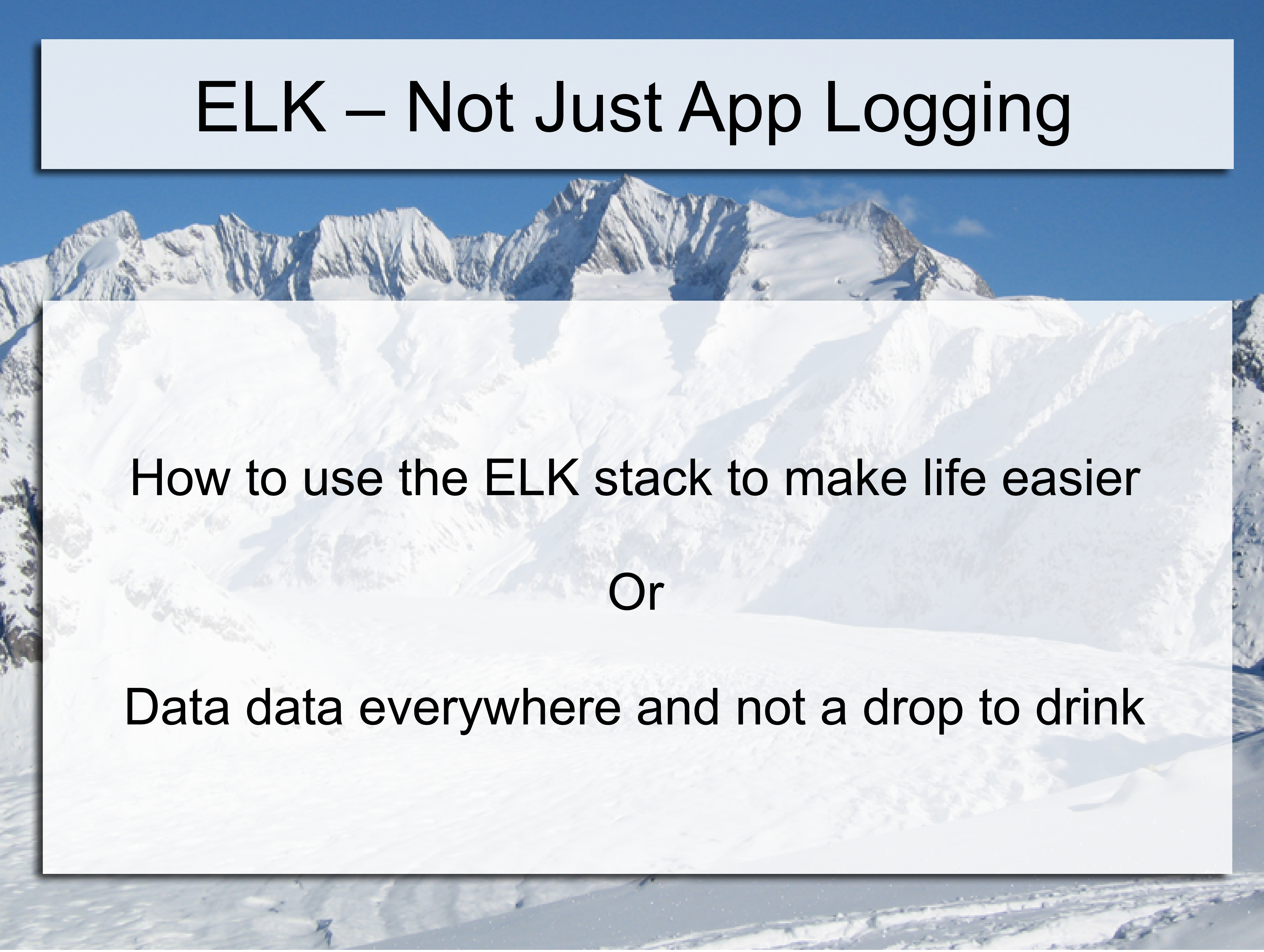
ELK – Not Just App Logging



How to use the ELK stack to make life easier

Or

Data data everywhere and not a drop to drink

Agenda

- Who am I
- What this talk is and is not about
- Why am I giving an ELK talk at BSides?
- What is ELK
- Why ELK?
- ELK Setup
- Tips and Tricks
- Demo
- Q&A

Who Am I

- Systems Engineer at a small automobile manufacturing IT start up
- Kind of a security enthusiast
- Kind of an OWASP enthusiast
- Degrees and security certifications that have nothing to do with this talk
  - MS-IT focusing on InfoSec
  - CEH / ECSA

What will not and will be discussed

- Will not
  - ELK in the enterprise
  - Paid Add-Ons (X-PACK)
  - Logstash Grok (sort of)
  - Kibana Dashboards

- Will
  - Standalone ELK (VM)
  - Data collection methods
  - Why this can do very useful things
  - Use cases that are not normally associated with ELK

Why an ELK talk at BSides?

- Goal – Share some knowledge about how ELK can supplement other tools and applications
- My epiphany
- ELK is very good at application logging but can be used for other scenarios and use cases
- It’s free (open-source stack)
- It’s easy to setup and use
- Did I mention it’s free and easy?

What is ELK

- Elasticsearch
  - RESTful, distributed search and analytics engine built on Apache Lucene
- Logstash
  - “Swiss Army Knife” of log parsers
- Kibana
  - Web UI interface for access data in Elasticsearch
  - Searches/Visualizations/Dashboards

But Wait, if you call now….

…. and the Beat goes on with data shippers

- Metricbeat - metrics from systems and services
- Packetbeat - lightweight network packet analyzer
- Winlogbeat - Windows event log
- Auditbeat – Linux user activity and process
- Heartbeat – monitor services with active probing
- Filebeat - forwards and centralize logs and files

Why ELK?

- Easy to take tool or app output and store it.
- Enrich data
- Run once and have it for reference
- Run many and determine changes
- Small storage footprint
- Can run on a single 4x8 VM
- Searches are easy and can be saved
- Start simple and easy to get to complex
  - If you know what to grep for you know how to search

ELK Setup

- Only requirement is Java
- All major OS’s supported
- Few edits to some configuration files to get up and running
- Supports apt-get and yum to install
- No real version dependencies between the stack components

Tips and Tricks

- Log file location
  - /var/log/elasticsearch
  - /var/log/logstash
  - /var/log/kibana
  - /var/log/filebeat
  - /var/log/messages if really bad
- Syntax checks for configuration files
  - Logstash Conf - /usr/share/logstash/bin/logstash -f ***<file to test>*** -t
  - Filebeat YML - /usr/share/filebeat/bin/filebeat test config ***<file to test>***

Tips and Tricks

- Start Logstash with a specific conf file
  - Useful for testing
  - Send output to standard out and not Elasticsearch
    - /usr/share/logstash/bin/logstash -f ***<file to run>***
- * nix built-in commands/scripts
  - Useful for piping standard out to a file at a regular interval

Demo

- GitHub install
- Data In
  - Add a data source
  - Any requests?
- Data Out
  - Kibana for noobs (it’s not hard but not intuitive)
  - Searches

Links

- Elasticsearch - https://www.elastic.co/products/elasticsearch
- Logstash - https://www.elastic.co/products/logstash
- Kibana - https://www.elastic.co/products/kibana
- Beats - https://www.elastic.co/products/beats
- GitHub - https://github.com/macatak/ELK-Install-scripts
- LinkedIn - https://www.linkedin.com/in/markdmclauchlin/

Q&A