Elastic Stack: Getting Started

DETAILING ELASTICSEARCH FOUNDATIONAL FUNCTIONS

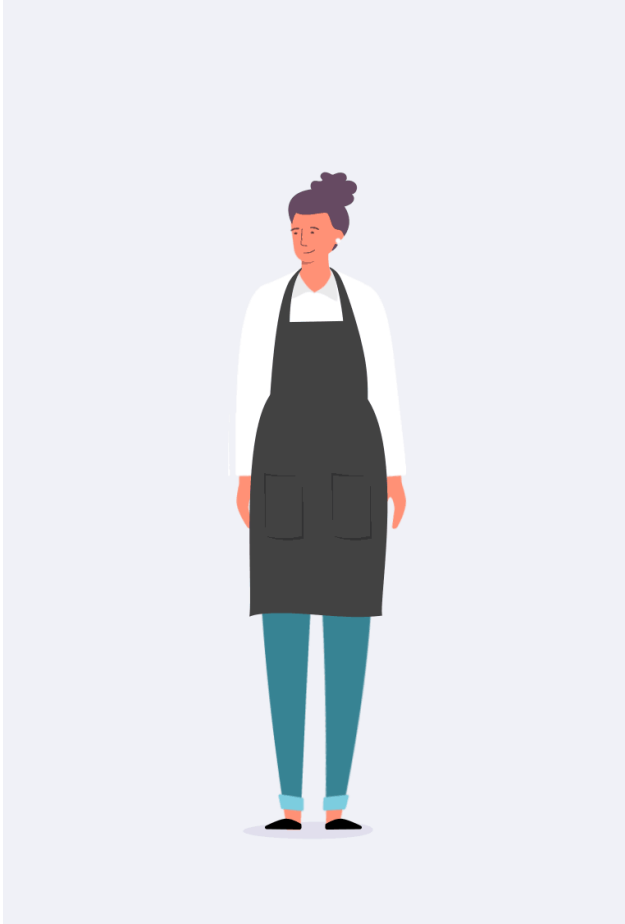
Aaron Rosenmund
AUTHOR EVANGELIST – SECURITY OPERATIONS

@arosenmund www.AaronRosenmund.com

The capabilities and applications of the elastic stack technology are limited only by your imagination.

Who is the Elastic Stack for?

Is this just for Security Analysts?



No, it is for everyone!

Community Driven

Open Source First

Security Data is also just known as data, it is NOT exclusive to security operations

Custom non relational database for use in development and custom data search

Predefined support for hundreds of services with pre-built data processing and dashboards

Heavily used in community security monitoring projects as well as a significant investment into a native security solution

and the beat goes on and on…

Overview

What is the Elastic Stack?

Lucene and full-text search

Look at security logs in Elastic

The power of JSON

YAML or YML?

Elasticsearch configuration

What Is the Elastic Stack?

Elastic Stack

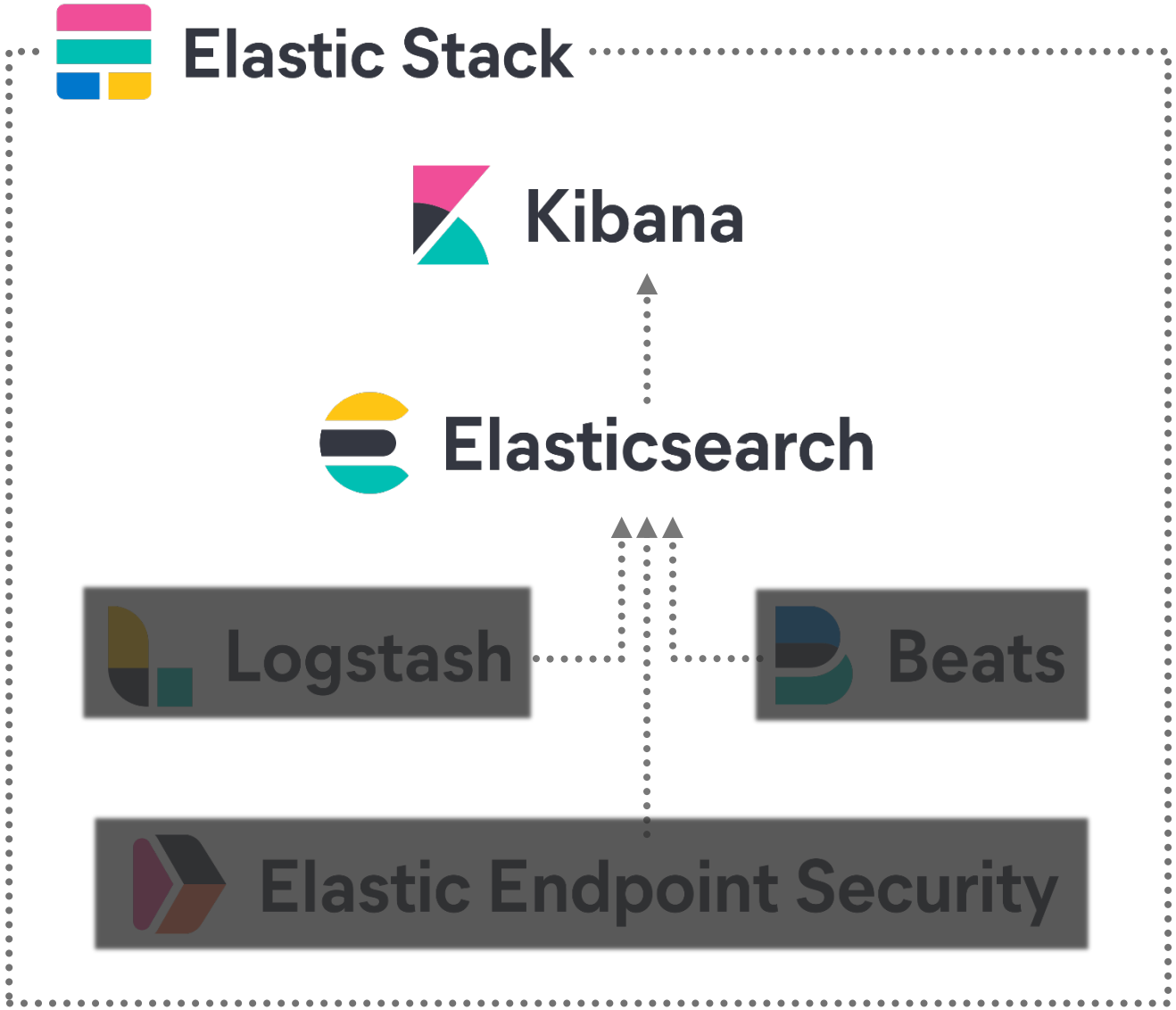
Elasticsearch

Kibana

Logstash

Beats

Endpoint Security



Apache Lucene

Full-text Search

Scaleable

Elasticsearch

Apache Lucene

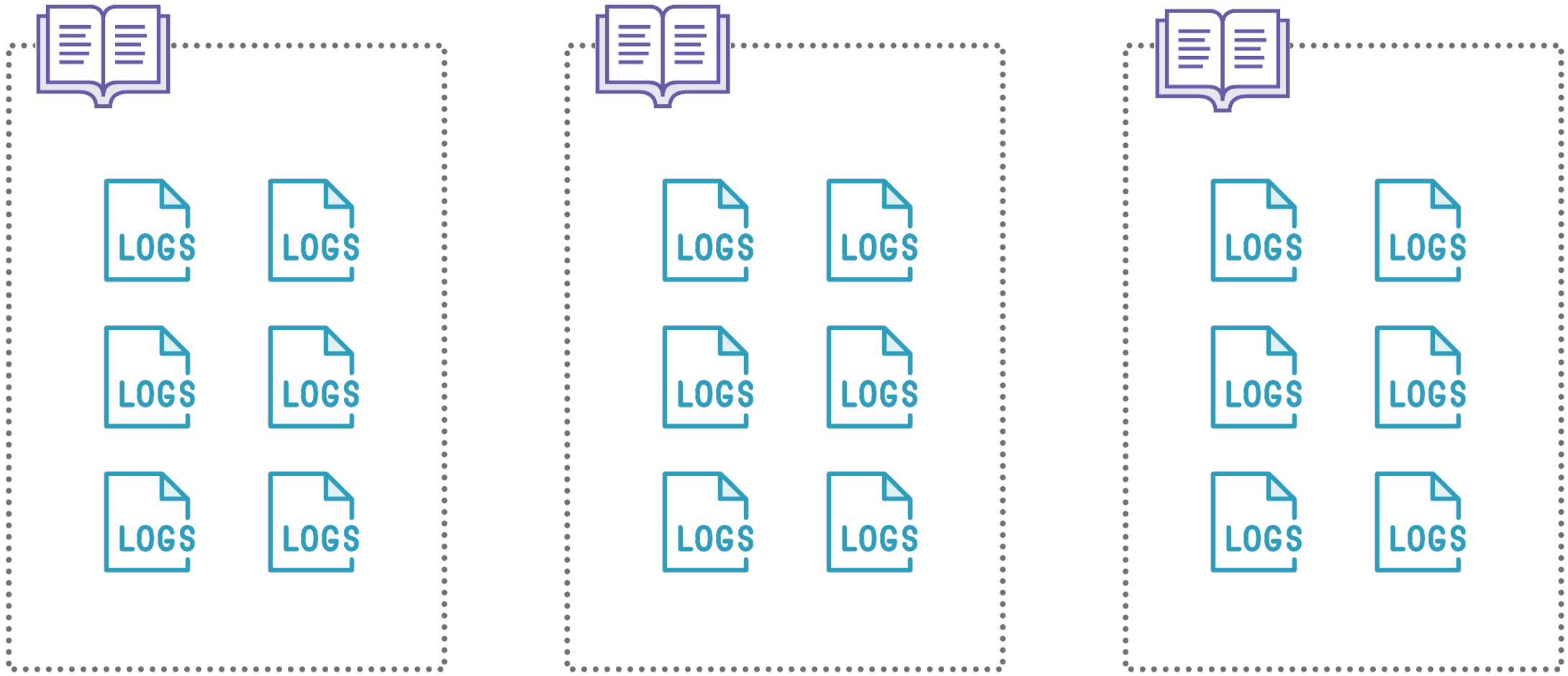
Inverted Index

Like a book index; fast searches!

Document

Event, network, metric, or security logs

Apache Lucene



Documents and Fields

Windows log 1

- @timestamp: [time]
- source.ip: 192.168.2.10
- log.level: ...

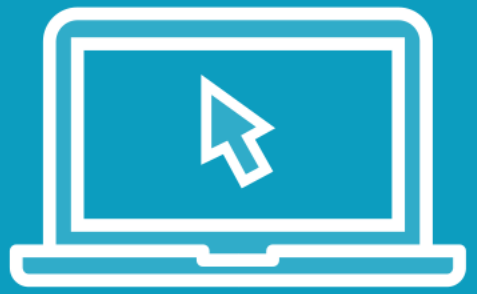
Suricata log 1

- @timestamp: [time]
- source.ip: 192.168.2.10
- event.id: ...

Zeek log 1

- @timestamp: [time]
- source.ip: 192.168.2.10
- conn.duration: ...

Demo



Kibana Overview

Look at Sample Logs

Index Configuration

JavaScript Object Notation (JSON)

```
{
  “_index”: “sample_data_logs”,
  “_type”: “_doc”,
  “_id”: “Zmvdi3MBMKnW8GT1L-Fv”,
  “_source”: {
    “host”: “www.pluralsight.com”,
    “ip”: “104.19.162.127”,
    “request”: “/library”,
    “response”: 200,
    “tags”: [
      “success”,
      “info” ]
  }
}
```


- Name-Value pairs
- Grouped fields from the source log
- Ability to enrich with arrays
- Closing braces

JSON vs. XML

Comparing formats

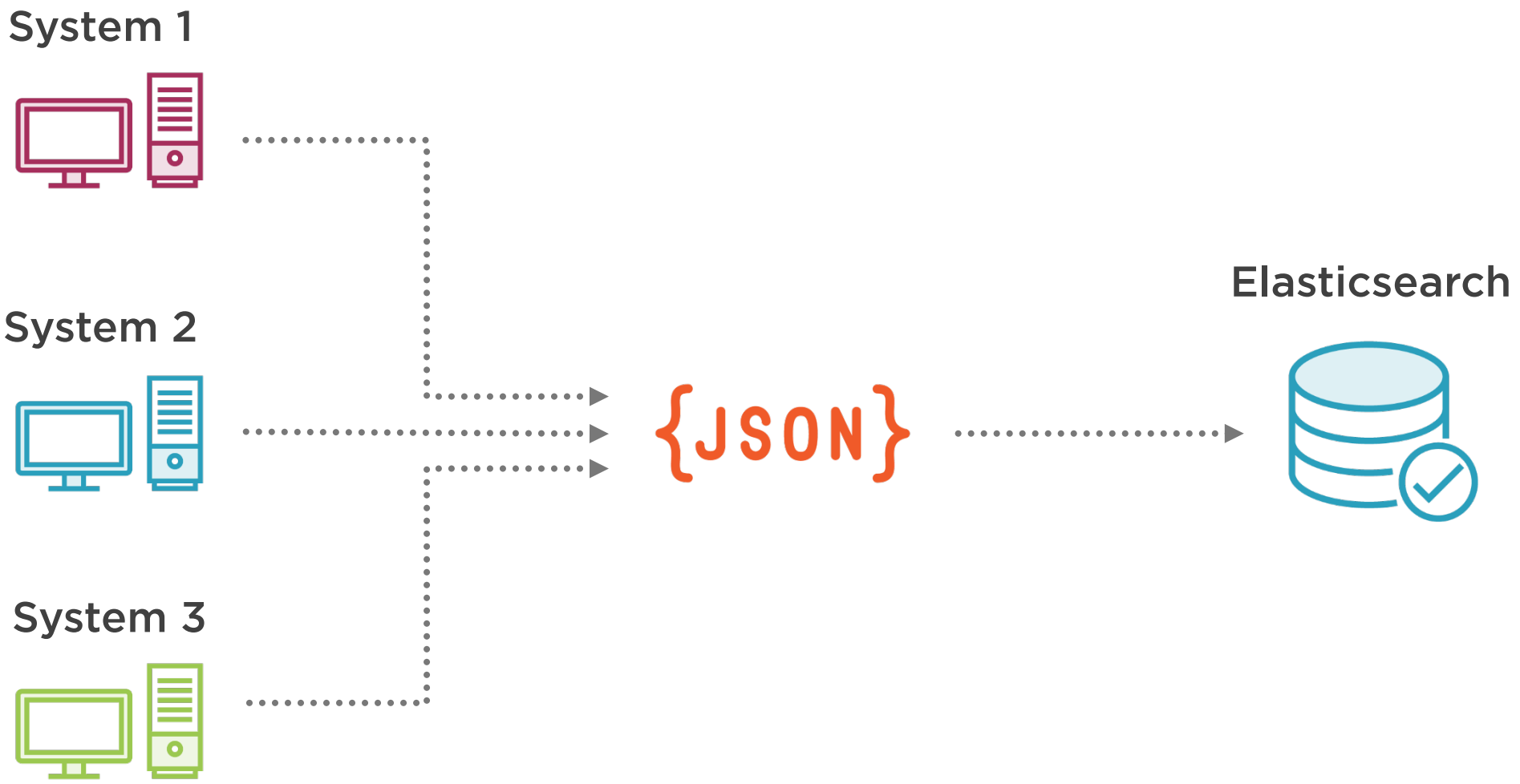
Sample.json

```
{
  “employees”: [
    { “first”: “Brandon”,
    “last”: “DeVault” },
    { “first”: “Aaron”,
    “last”: “Rosenmund” }
]}
```

Sample.xml

```
<employees>
  <employee>
    <first>Brandon</first>
    <last>DeVault</last>
  </employee>
  <employee>
    <first>Aaron</first>
    <last>Rosenmund</last>
  </employee>
</employees>
```

Data Flow and Conversion



Yet Another Markup Language (YAML)

YAML Ain’t Markup Language (YAML)

```
---
#####
# Employee Record
name: Brandon DeVault
job: Education Architect
employed: True
skills:
  - elasticsearch
  - powershell
  - invisibility
...
```

- ‘#’ designates a commented line
- More name-value pairs!
- Supports nested data structures
- Spacing vs. special characters

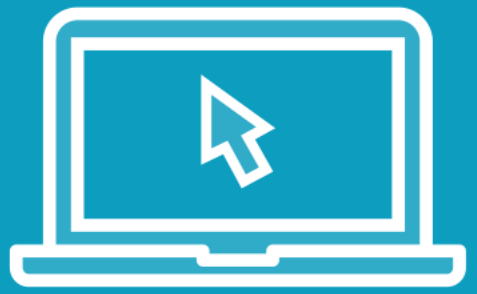
Elasticsearch Configuration

It's built for you!

elasticsearch.yml

```
# ---------------------------------- Cluster -----------------------------------
#
# Use a descriptive name for your cluster:
#
cluster.name: my-cluster
#
# ------------------------------------ Node ------------------------------------
#
# Use a descriptive name for the node:
#
node.name: node1
```

Demo



Elasticsearch configuration file

Kibana configuration file

Rest API

Setting Up the Elastic Stack

Follow Along

https://www.elastic.co/what-is/elk-stack

https://www.elastic.co/guide/en/elastic-stack/current/installing-elastic-stack.html

Install instructions:

- from tar.gz or .zip
- from repo

Ore just have it hosted
https://www.elastic.co/cloud/

- Azure, AWS, GCP

Check Out This Guide for SIEM Data:
Setting up Elasticsearch for the Elastic SIEM | Pluralsight

Summary

Kibana is the window into elasticsearch

Based on Apache Lucene

Data is transmitted in JSON

Configuration is completed with YAML