# Lab 3: Establishing and Applying the ELK Stack for Cyber Analytics

**References:**

[1] <https://dzone.com/articles/how-to-install-the-elk-stack-on-aws-a-step-by-step>

[2] <https://logz.io/blog/install-elk-stack-amazon-aws/>

[3] <http://www.unb.ca/cic/datasets/index.html>

[4] <https://www.sciencedirect.com/science/article/pii/S0167404811001672>

[5] <http://scikit-learn.org/stable/>

[6] <https://www.tensorflow.org>

[7] <https://scipy.org>

[8] <https://ipython.org/notebook.html>

[9] <https://web.stanford.edu/class/cs259d/>

[10] <https://github.com/elastic/examples/tree/master/Security%20Analytics>

**Note:** Provide all source files separately. Include screenshots for each step.

# Introduction

In this lab you will learn how to deploy and apply the ELK stack for cyber analytics.

**Part I**

1. Establish the ELK stack in AWS:

<https://dzone.com/articles/how-to-install-the-elk-stack-on-aws-a-step-by-step>

1. Configure logstash to read AWS logs:

<https://logz.io/blog/install-elk-stack-amazon-aws/>

1. Demonstrate
   1. Logstach Capture of EC2 instance security logs
   2. Kibana Graphics View

**Part II**

1. Build a Log Analytic Solution in AWS
   1. Use this file: <https://d0.awsstatic.com/Projects/P4113850/aws-projects_build-log-analytics-solution-on-aws.pdf>
2. Demonstrate all completion of all tutorial steps. Be sure to specifically highlight success in
   1. AWS Elasticsearch
   2. AWS Kinesis Analytics

**Part III**

1. Choose an existing cyber data set; reference: <http://www.unb.ca/cic/datasets/index.html>. Follow links and contact information to acquire.
2. Choose atleast one analytic
   1. From these examples: <https://github.com/elastic/examples/tree/master/Security%20Analytics>
   2. From one of the following frameworks:
      1. <http://scikit-learn.org/stable/>
      2. <https://www.tensorflow.org>
      3. <https://scipy.org>
      4. <https://ipython.org/notebook.html>

Consider the following research and guidance for analytic selection: <https://web.stanford.edu/class/cs259d/>

1. Select an approach to perform the analytic. You may use:
   1. The ELK Stack you set up in Part I using any Apache framework
   2. The AWS Elasticsearch and Kinesis system you setup in Part II
   3. The EMR instance you set up in Lab #2.
2. Describe your solution in a single design diagram, describe the cyber example log ingested and describe the analytic you are using.
3. Demonstrate:
   1. Cyber Log Ingest
   2. Analytic Execution

Grading Evaluation:

1. Part 1 (33%)
2. Part II (33%)
3. Part III (34%)