SEAS-8414

Analytical Tools for Cyber Analytics

Survey of analytical tools for analyzing cyber security data with particular attention to the use of data analytics procedures in supporting appropriate cyber security policy decisions.

Dr. M

Welcome to SEAS Online at George Washington University

SEAS-8414 class will begin shortly

- **Audio:** To eliminate background noise, please be sure your audio is muted. To speak, please click the hand icon at the bottom of your screen (**Raise Hand**). When instructor calls on you, click microphone icon to unmute. When you've finished speaking, ***be sure to mute yourself again***.
- **Chat:** Please type your questions in Chat.
- **Recordings:** As part of the educational support for students, we provide downloadable recordings of each class session to be used exclusively by registered students in that particular class for their own private use. Releasing these recordings is strictly prohibited.

Agenda

Week-7: Log-centric detection analytics tools

Now that we have covered all the prevention controls for securing gwuscc.com, we will focus on detection engineering using log-centric tools.

- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)
- Root Cause Analysis (RCA)

Class-7

Structure

- We will talk about building an application
- Discuss various techniques for analysis
- Hands-on implementation

Prerequisites

Software Install

- Docker - https://docs.docker.com/get-docker/
- Splunk - https://hub.docker.com/r/splunk/splunk/
- AWS - https://console.aws.amazon.com/
- Python - https://www.python.org/downloads/

Develop Analytics Application

Practical - 1

1. Install required libraries
2. Write a simple web program
3. Run the application

Hands-on: App Development

Hands-on: Splunk Deployment

Splunk Deployment

- `systemctl start docker`
- `git clone https://github.com/gwuml/seas-8414.git`
- `cd seas-8414/week-7/application`
- `docker run -d -v $(pwd):/data/ -p 80:8000 -e "SPLUNK_START_ARGS=--accept-license" -e "SPLUNK_PASSWORD=Admin321" --name splunk splunk/splunk:latest`
  - OR
- `make splunk`

Command History

- [root@ip-10-0-13-6 application]# history
- 1 yum install git docker
- 2 git clone https://github.com/gwuml/seas-8414.git
- 3 ls -l
- 4 cd seas-8414/
- 5 ls
- 6 ls -l
- 7 cd week-7/
- 8 ls
- 9 cd application/
- 10 ls
- 11 ls -l
- 12 cat app.py
- 13 vim app.py
- 14 ls -l
- 15 vim week7.py

What is data analytics?

- Data analytics is analyzing raw data to make conclusions.

What are the types of data analytics?

- **Descriptive analytics:** Find out **what** has happened over a given period.
- **Diagnostic analytics:** Find out **why** it has happened.
- **Predictive analytics:** Find out **what will happen** in the near term.
- **Prescriptive analytics:** Find out **what to do**

Install Streamlit

- `git clone https://github.com/gwuml/seas-8414.git`
- `cd seas-8414/week-7/application`
- `pip3 install -r requirements.txt`

Descriptive Analytics

Column Chart

- A column chart is primarily used to compare and track the development of quantitative values over a period. Compared to area and line charts, column charts are suitable for discrete data points. Column charts can also compare non-time series data. However, a bar chart or another comparison chart might be better suited for that purpose.

- Purpose: Trend

(Source: Splunk)

Bar Chart

- Bar charts are used to compare data of one period or point in time across multiple categories

- Purpose: Comparison

(Source: Splunk)

Line Chart

- A line chart is used to show the development of quantitative values over a period. Line charts tend to be visually simpler than area charts and are useful for quickly identifying trends in your data for both single and multiple data series.

- Purpose: Trend

(Source: Splunk)

Area Chart

- An area chart is used to show the development of quantitative values over a period of time. It can also be used to show the development of multiple data series summed

- Purpose: Trend

(Source: Splunk)

Bubble Chart

- Pie charts are effective at showing the value of different fields in terms of relative importance or volume out of a whole. Pie charts are better at showing visual differences, without the need to know specific values for that field, which can only be done on hover in Dashboard Studio.

- Purpose: Comparison

(Source: Splunk)

Types of Graphs

- Line & Area chart: Continous data
- Pie chart: Categorical data
- Column & bar chart: Discrete data

Hands-on: Python Way

https://github.com/anarabiyev/EDA_Streamlit_App.git

Hands-on: Splunk Way

Diagnostic Analytics

Hands-on: Import Linux Logs

- Create and schedule an alert
- Splunk Universal Forwarder
- HTTP Event Forwarder

Prescriptive Analytics

Hands-on: Regression

- Predict Bitcoin price using Quadratic Linear Regression

What is due?

Homework & Discussions

Homework

- Setup a Linux system to forward logs to the Splunk docker instance
- Create an alert & widget for three consecutive login failures
- Create an alert & widget for the user logging in after work hours
- Create a dashboard with widgets *
- Add a demo Pie, Column, Bar, Area, and Line chart to the dashboard *
- Submit a PDF of the dashboard for homework *

Whiteboard content from the class