**Performing a Query w/ Splunk**

A black and green logo

Description automatically generated

Material & instructions developed by: Google Cybersecurity Professional Certificate Course

Completed by: Alexander Herman on 01/31/24

**Table of Contents:**

Scenario (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2**

Step-By-Step Instructions (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2**

Instruction Output (My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2-5**

**Scenario**

You are a security analyst working at the e-commerce store Buttercup Games. You've been tasked with identifying whether there are any possible security issues with the mail server. To do so, you must explore any failed SSH logins for the root account.

**Step-By-Step Instructions**

1. Create a Splunk cloud account
2. Sign up for a free trial
3. Upload data into Splunk
4. Perform a basic search
5. Evaluate the fields
6. Narrow your search
7. Search for a failed login for root
8. Evaluate the search results
9. Answer provided questions about the search results

**Instruction Output**

1. **Create a Splunk cloud account**

✅

1. **Sign up for a free trial**

✅

1. **Upload data into Splunk**

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated

1. **Perform a basic search**

A screenshot of a computer

Description automatically generated

1. **Evaluate the fields**

* Fields are host, source, and sourcetype
* the host field specifies the name of the network host from which the event originated
* the source field indicates the file name from which the event originates
* the sourcetype determines how data is formatted

1. **Narrow your search**

A screenshot of a computer

Description automatically generated

1. **Search for a failed login for root**

A screenshot of a computer

Description automatically generated

1. **Evaluate the search results**

* 346 events were returned (before 2/1/24 7:01:57.000 PM)
* using the wildcard ‘\*’ is key to returning accurate results
* you can drill down into each specific event further my pressing the ‘>’ in the ‘i’ column

1. **Answer provided questions about the search results**

* How many events are contained in the main index across all time? 109,846 events
* Which field identifies the name of a network device or system from which an event originates? host
* Which of the following hosts used by Buttercup Games contains log information relevant to financial transactions? vendor\_sales
* How many failed SSH logins are there for the root account on the mail server? 346