**COMP3010 CW2**

Things to Note:

* Include screenshots of bars and charts while doing the analysis in the report
* Record video showing how the installation worked – either mention that it was already done therefore just talking through it without running commands, or set up a new VM and re-run through the download of the dataset and analysis etc.
* Change VM background to name or something unique to prove that the recording is mine
* Place search terms on different lines -> Start each line (aside from the first) with |

Introduction:

SOC Roles and Incident Handling Reflection:

Installation and Data Preparation:

Guided Questions:

Conclusions:

References:

Evidence:

Question 1:

A screenshot of a computer

AI-generated content may be incorrect.

* Filtered BOTSv3 by sourcetype=”aws:cloudtrail” as given in the hints on the DLE quiz
* Searched within the filters for “username” and found userIdentity.userName filter
* Selected filter and checked values to find 4 names
* In alphabetical order: bstoll, btun, splunk\_access, web\_admin

Question 2:

A screenshot of a computer

AI-generated content may be incorrect.

* Filtered BOTSv3 by sourcetype=”aws:cloudtrail” as given in the hints on the DLE quiz
* Added additional filter for \*mfa\* since looking for details relating to multi-factor authentication (using asterisks as given in the hints on the DLE quiz)

A screenshot of a computer

AI-generated content may be incorrect.

* Searched additional filters for anything related to “mfa” to find userIdentity.sessionContext.attributes.mfaAuthenticated

Question 3:

A screenshot of a computer

AI-generated content may be incorrect.

* Filtered BOTSv3 by sourcetype=”hardware” as given in the hints on the DLE quiz
* Checked value of CPU\_TYPE and found the model number of E5-2676 in the correct form of \*\*-\*\*\*\* given in the hints on the DLE quiz

Question 4:

A screenshot of a computer

AI-generated content may be incorrect.

* Filtered BOTSv3 by sourcetype=”aws:cloudtrail” and specific eventName=”PutBucketAcl” as given in the hints on the DLE quiz
* Noticed 2 events with this event name but different event IDs
* Assumed these events would be user accidentally making the S3 bucket public (older event) then making it private again (newer event) giving the correct eventID as ab45689d-69cd-41e7-8705-5350402cf7ac

Question 5:

A screenshot of a computer

AI-generated content may be incorrect.

* Applied same filters as question 4
* Opened userIdentity field within the relevant event and found userName: bstoll

Question 6:

A screenshot of a computer

AI-generated content may be incorrect.

* Applied same filters as question 4
* Opened requestParameters field within the relevant event and found bucketName: frothlywebcode

Question 7:

A screenshot of a computer

AI-generated content may be incorrect.

* Filtered BOTSv3 by sourcetype=”aws:s3:accesslogs” as given in the hints on the DLE quiz
* Filtered specifically for events at date\_hour=14 since questions 4-6 show both events occur between 2pm
* Filtered for PUT requests as suggested by the question since this event involved uploading a file to the bucket
* Filtered for \*txt\* since the question asked for the name of the text file uploaded therefore hinting it would be a .txt extension

Question 8:

A screenshot of a computer

AI-generated content may be incorrect.

* Filtered BOTSv3 by sourcetype=”winhostmon” as given in the hints on the DLE quiz
* Searched though the filters list to find source filter and selected source=”operatingsystem” from the list
* Searched through the filters list again to find OS filter and selected OS=”Microsoft Windows 10 Enterprise” from the list as it had the least uses -> Was used 30 times by only one user

A screenshot of a computer

AI-generated content may be incorrect.

* Added host=”BSTOLL-L” from the initial search into a new search to look for any filters with the FQDN

A screenshot of a computer

AI-generated content may be incorrect.

* Initially searched filters list for FQDN but could not find anything so instead searched for “name”
* Found filter called ComputerName which had the value of BSTOLL-L.froth.ly