

COMP3010 CW2

Contents

Introduction:.....	2
SOC Roles and Incident Handling Reflection:.....	2
SOC:.....	2
Prevention:.....	2
Detection:.....	2
Response:.....	3
Recovery:.....	3
Installation and Data Preparation:	3
Splunk Installation:.....	3
BOTSV3 Dataset Preparation:.....	8
Guided Questions:	13
Question 1:	14
Question 2:	14
Question 3:	15
Question 4:	16
Question 5:	17
Question 6:	17
Question 7:	18
Question 8:	19
Conclusion:.....	20
References:.....	21

Introduction:

In this report, I will be analysing the BOTSV3 dataset within Splunk. The BOTSV3 dataset is a public dataset made up of 2,083,056 events which simulates an incident to allow cyber security professionals to practice event analysis in a simulated environment. By utilising the 3 tiers of SOC – triage, investigation and hunting – I will answer a series of questions to determine how the incident occurred, including information about the user(s) and device(s) involved. This report will focus on 8 of those questions, explaining their relevance to SOC, as well as how to install Splunk and how to prepare the BOTSV3 dataset for analysis.

Screenshots can be found here: <https://github.com/Mark7567/COMP3010>

Video walkthrough: <https://www.youtube.com/watch?v=ijebfZ6ZJcl>

SOC Roles and Incident Handling Reflection:

SOC:

The Security Operations Centre (SOC) consists of 3 tiers, each having unique roles and responsibilities surrounding cyber security prevention and analysis. Tier 1 - triage - involves monitoring dashboards and events to determine if an incident has occurred. Since attacks cannot be 100% prevented, tier 1 acts as a way to catch incidents early, as well as filter out false positives which prevention methods may have caught.

Once an event has been flagged as an incident, tier 2 - investigation - takes place. This involves checking logs and confirming that an incident has occurred and containing them to prevent any more damage from occurring. Tier 2 also involves determining how the incidents occurred by performing an in-depth analysis.

Lastly, tier 3 - hunting - involves performing an advanced analysis on the incident and improving overall security following it. The BOTSV3 dataset focusses predominantly on tier 2 of SOC, since the dataset contains incidents which have already occurred, with the purpose of the dataset being to confirm this and investigate how they happened.

Prevention:

Prevention is an incident handling methodology which involves mitigating the risk of an incident occurring rather than directly stopping it, since it is not possible to 100% prevent an attack. Rules and proper system configurations are implemented to make a system as secure as it can be in an attempt to reduce the risk of successful attacks. Prevention relates to the BOTSV3 exercise since the events in the dataset can help to determine normal user behaviour which may make any outliers more obvious as potentially malicious. Furthermore, it links with tier 1 of SOC as there are links with monitoring dashboards and analysing behaviour.

Detection:

Detection is an incident handling methodology that involves identifying incidents which could be considered suspicious and may indicate an incoming incident. Typical detection methods include analysing network traffic and timestamping user actions or system events to find concerning behaviour. The BOTSV3 dataset involves using filters and searching within Splunk to

analyse millions of events and identify information about them, such as which users were involved and which operating system their device was running. This links to tiers 1 and 2 of SOC since detection involves flagging potentially malicious events and analysing them to determine their causes.

Response:

Response is an incident handling methodology which involves containing an incident to prevent it from causing any more damage to a system, as well as investigating how the incident occurred. The BOTSV3 dataset contains a variety of incidents which need to be confirmed as valid, as well as investigating into how they occurred by gathering information about the events using Splunk filters. Since it is a premade dataset, Splunk cannot contain the incidents in any way, but it can be used to investigate them. Response has strong links with tier 2 of SOC as the purpose of this methodology is to investigate how the incident occurred, which is also the main idea behind SOC tier 2.

Recovery:

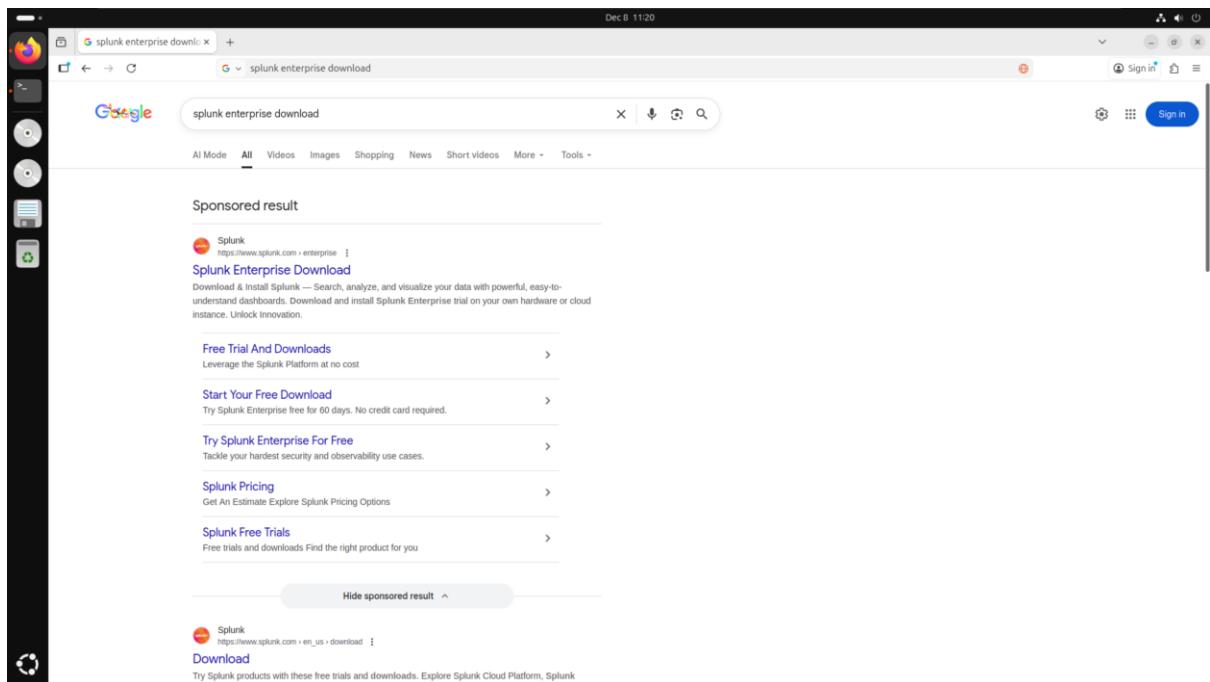
Recovery is an incident handling methodology which involves restoring damaged systems after an incident has been resolved. It also includes improving security to reduce the risk of a similar incident happening in future. While there is no active recovery within the BOTSV3 dataset, it helps with this methodology as the dataset is premade to contain events for analysis which can then be reviewed to prevent further incidents.

Installation and Data Preparation:

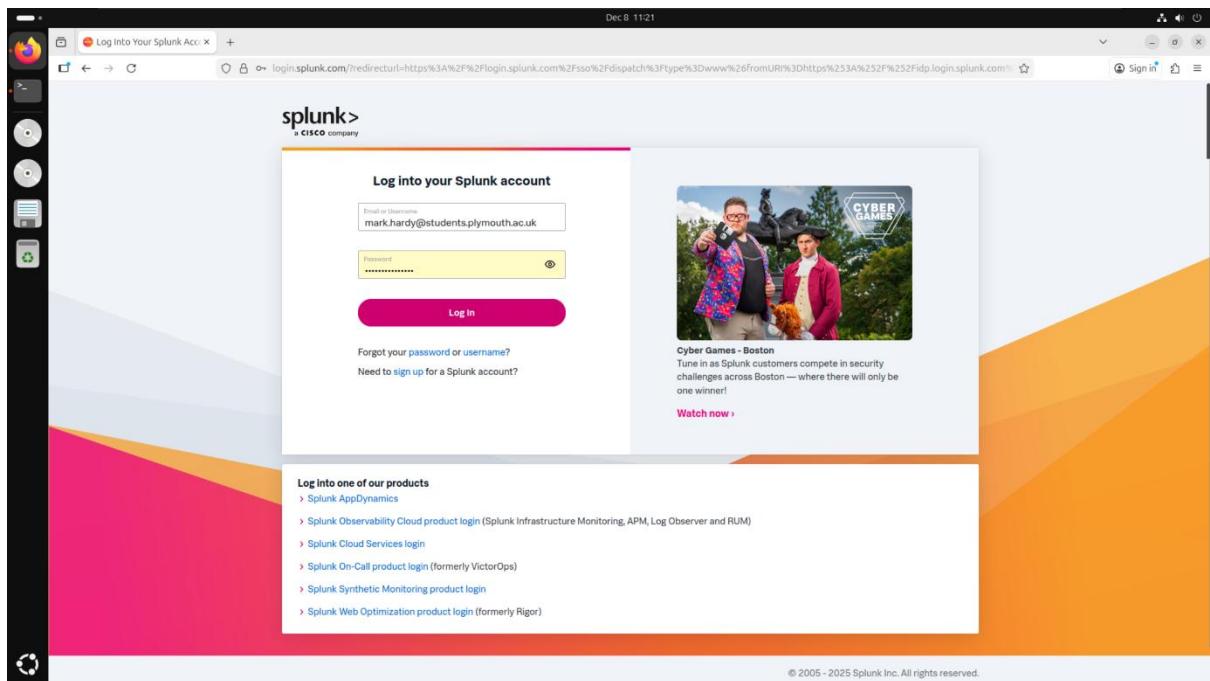
This section will explain how Splunk was installed within an Ubuntu Linux virtual machine hosted by VMWare, and how the BOTSV3 dataset was loaded. As I performed the installation before taking screenshots for this section, the screenshots display later timestamps compared to those for the guided questions. To effectively demonstrate the installation of Splunk, I reinstalled it on the same virtual machine ensuring the configuration of the machine remained the same throughout this report. The reason for using a Linux virtual machine is to mimic real world SOC environments which would typically use Linux-based systems. By installing Splunk locally on my device, this allowed me to have full control over the configuration, and which data was ingested, keeping the integrity and accuracy of the analysis.

Splunk Installation:

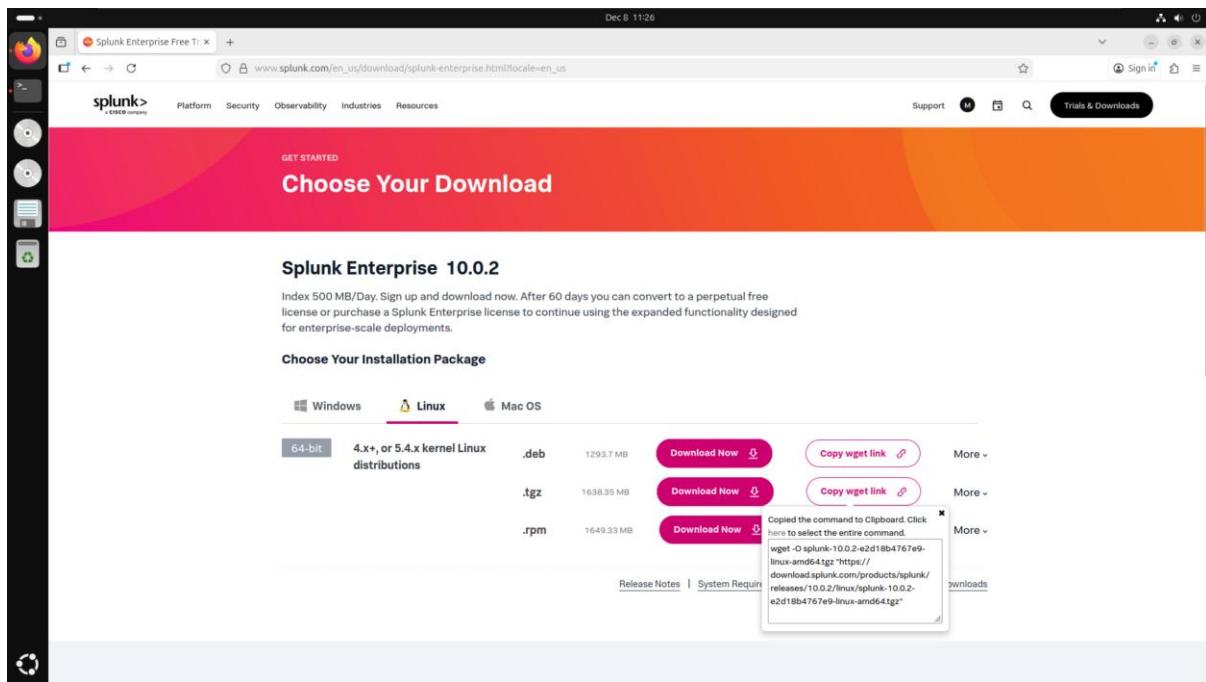
I opened Firefox inside an Ubuntu Linux virtual machine and searched for “splunk enterprise download”, clicking on the first link in the search results.



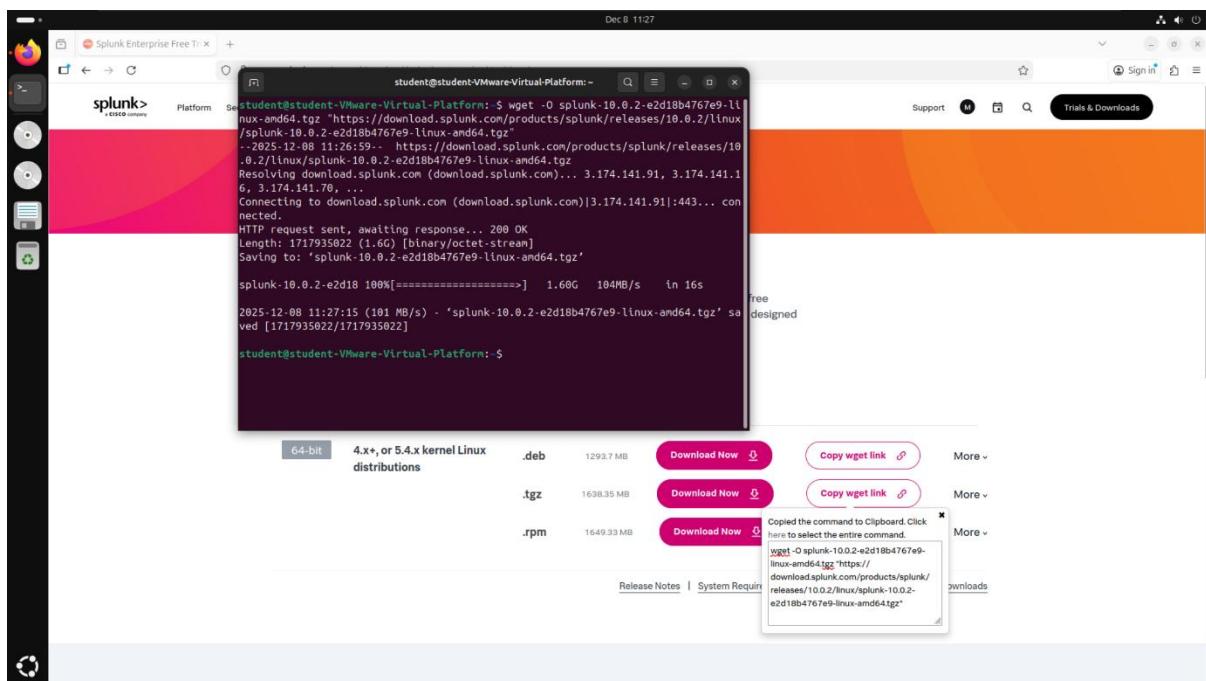
This link took me to the official Splunk website, where I logged into an account which I had already created.



I selected “Copy wget link” for the .tgz version of Splunk, to ensure that all packages were downloaded alongside the main Splunk software. This meant I did not have to individually download all relevant packages to complete this coursework.



I downloaded Splunk directly from the Linux terminal by pasting the wget link directly into the terminal and running it. I received a confirmation message in the terminal to state that Splunk had been successfully downloaded.



I ran the command “sudo tar xvzf splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz -C /opt” which installed Splunk and all its dependencies into the /opt folder.

```

student@student-Virtual-Platform:~$ sudo tar xvzf splunk-10.0.2-e2d18b476e9-llinux-amd64.tgz -C /opt/

```

64-bit 4.x+, or 5.4.x kernel Linux distributions
 .deb 1293.7 MB Download Now Copy wget link More
 .tgz 1638.35 MB Download Now Copy wget link More
 .rpm 1649.33 MB Download Now Copy wget link More

Copied the command to Clipboard. Click here to select the entire command.
 wget -O splunk-10.0.2-e2d18b476e9-llinux-amd64.tgz "https://download.splunk.com/products/splunk/releases/10.0.2/linux/splunk-10.0.2-e2d18b476e9-linux-amd64.tgz"

To start Splunk, I ran the command “`sudo ./splunk start`” from within the “`/opt/splunk/bin`” folder. Since this was my first time running Splunk on this installation, I had to include the command “`--accept-license`” which accepted the user license agreement for Splunk. I had to set a username and password for the administrator account which I could then use to sign in once on `localhost:8000`.

```

student@student-Virtual-Platform:~$ cd /opt/splunk/bin
student@student-Virtual-Platform:/opt/splunk/bin$ sudo ./splunk start --accept-license

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise,
you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: admin
Password must contain at least:
 * 8 total printable ASCII character(s).

Please enter a new password:

```

64-bit 4.x+, or 5.4.x kernel Linux distributions
 .deb 1293.7 MB Download Now Copy wget link More
 .tgz 1638.35 MB Download Now Copy wget link More
 .rpm 1649.33 MB Download Now Copy wget link More

Copied the command to Clipboard. Click here to select the entire command.
 wget -O splunk-10.0.2-e2d18b476e9-llinux-amd64.tgz "https://download.splunk.com/products/splunk/releases/10.0.2/linux/splunk-10.0.2-e2d18b476e9-linux-amd64.tgz"

After setting up the initial login details, Splunk generated the web server on `localhost:8000`, providing a clickable link to the website to allow access into Splunk.

The screenshot shows a terminal window and a web browser side-by-side.

Terminal Window:

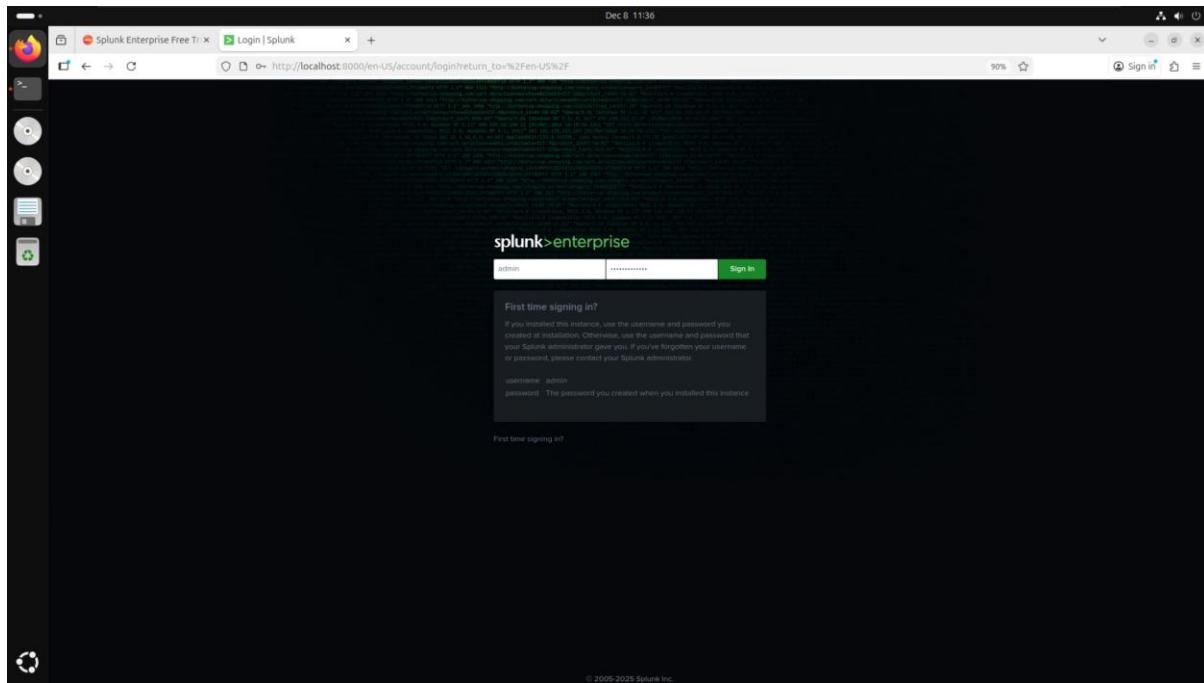
```
student@student-VMware-Virtual-Platform: /opt/splunk/bin
=====
Warning: ignoring --extensions option without --extfile
Certificate request self-signature ok
subject=CN = student-VMware-Virtual-Platform, O = SplunkUser
Done

Waiting for web server at http://127.0.0.1:8000 to be available..... Done
```

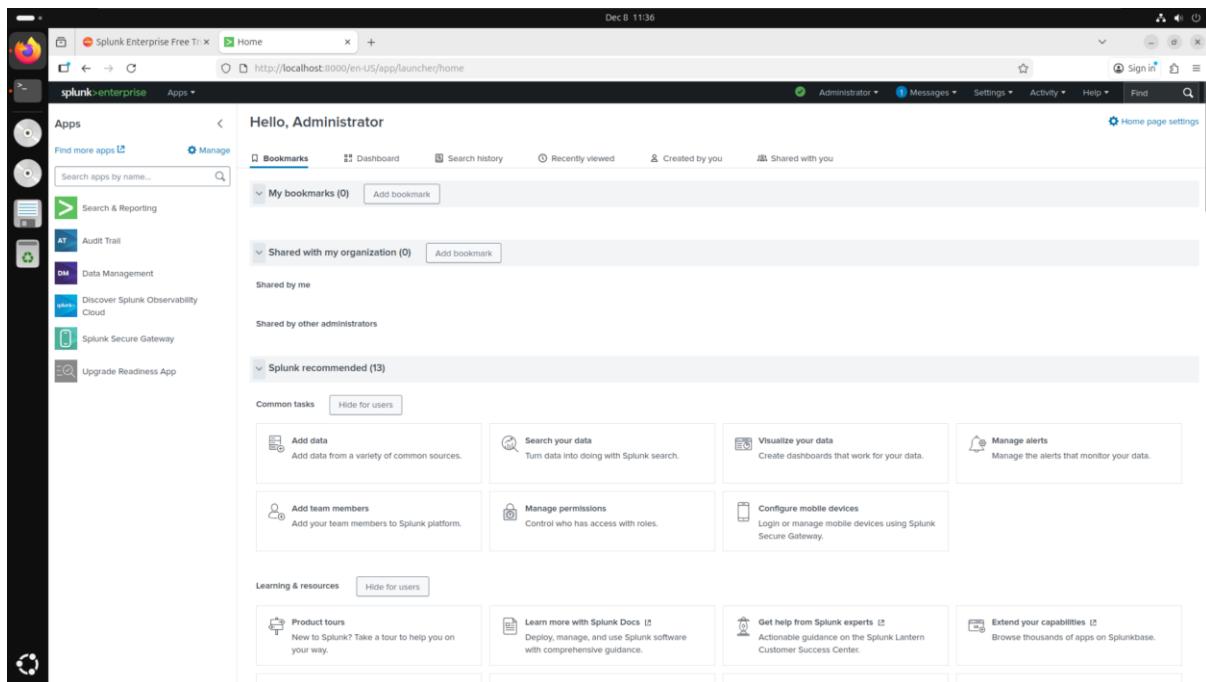
Browser:

The browser displays the Splunk Enterprise Free Trial download page. It shows download links for 64-bit, 4.x+, or 5.4.x kernel Linux distributions (.deb, .tgz, .rpm) and provides a "Copy wget link" button for each. A tooltip for the .tgz link contains the command: `wget -O splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz https://download.splunk.com/products/splunk/releases/10.0.2/linux/splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz"`.

Searching for localhost:8000 on Firefox took me to the Splunk enterprise login page. I entered the username and password I created previously.

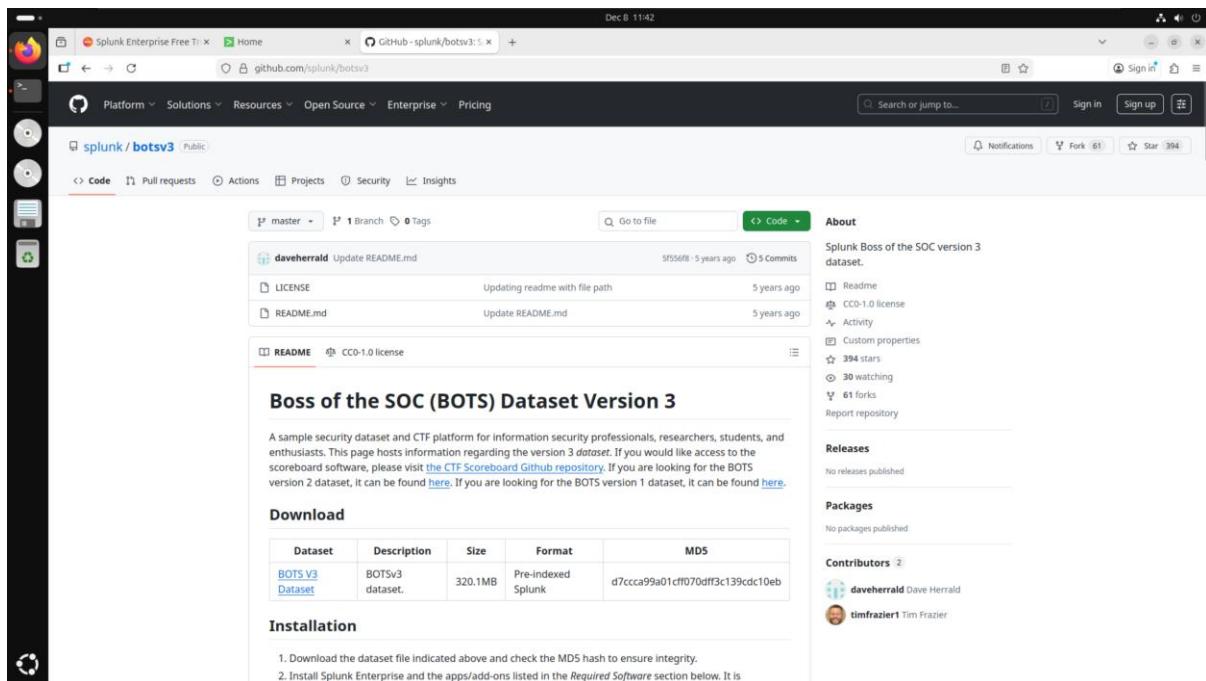


I was able to see the dashboard which houses all of the features I used to answer the guided questions, most notably the “Search & Reporting” tab, which will be explained below.



BOTSv3 Dataset Preparation:

I visited the link <https://github.com/splunk/botsv3> and clicked on the link under dataset in the table to download BOTSv3 to my virtual machine.



Clicking on the link downloaded the file `botsv3_data_set.tgz` onto my virtual machine as shown in the downloads tab on Firefox.

The screenshot shows a Firefox browser window with the GitHub URL `github.com/splunk/botsv3`. The repository page for 'splunk/botsv3' is displayed. The 'Downloads' tab is active, showing a single file entry:

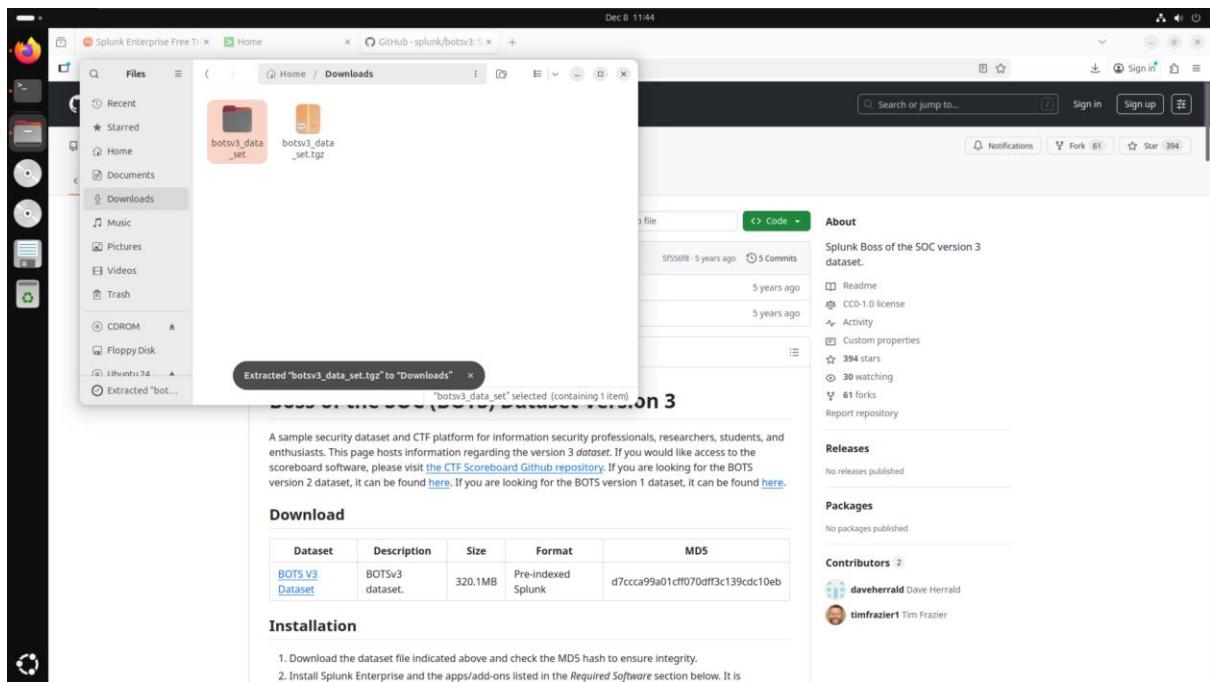
	<code>botsv3_data_set.tgz</code>	Completed — 320 MB
--	----------------------------------	--------------------

Below the download list, the repository's main content is visible, including the README, LICENSE, and other files. The 'About' section describes it as the 'Splunk Boss of the SOC version 3 dataset'. The 'Contributors' section lists `daveherrald` and `timfrazier1`.

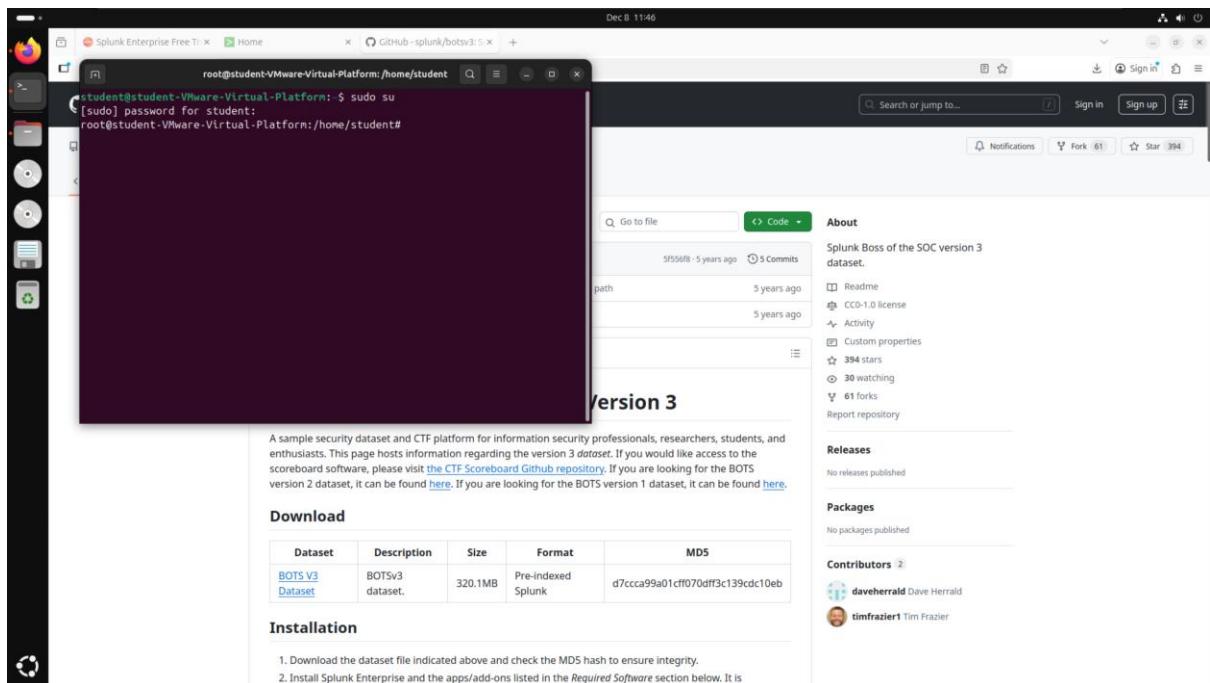
I opened up my file explorer and found the file in the downloads folder where I then extracted it.

The screenshot shows a file explorer window on a Linux desktop environment. The current directory is `/Downloads`, and a context menu is open over the file `botsv3_data_set.tgz`. The menu includes options like 'Extract', 'Return', 'Extract to...', 'OpenWith...', 'Cut', 'Copy', 'Move to...', 'Copy to...', 'Rename...', 'Compress...', 'Email...', 'Move to Trash', and 'Delete'. The 'Extract' option is highlighted.

In the background, the GitHub repository page for `splunk/botsv3` is still visible in the browser, showing the same dataset information and contributors.



To copy the folder to the correct path for Splunk, I entered root mode in the Linux terminal by running the command “sudo su” and entering the password for my virtual machine.



Once in root mode, I ran the command “cp -r botsv3_data_set /opt/splunk/etc/apps/” to copy the file (botsv3_data_set) into the correct path (/opt/splunk/etc/apps/) to allow it to load into Splunk correctly.

```
root@student-VMware-Virtual-Platform:~$ sudo su
[sudo] password for student:
root@student-VMware-Virtual-Platform:~$ cd Downloads
root@student-VMware-Virtual-Platform:~/Downloads$ ls
botsv3_data_set  botsv3_data_set.tgz
root@student-VMware-Virtual-Platform:~/Downloads$ cp -r botsv3_data_
set /opt/splunk/etc/apps/
root@student-VMware-Virtual-Platform:~/Downloads$
```

The terminal shows the user navigating to the Downloads directory, listing files, and then copying the 'botsv3_data_set' directory to the '/opt/splunk/etc/apps/' directory.

Version 3

A sample security dataset and CTF platform for information security professionals, researchers, students, and enthusiasts. This page hosts information regarding the version 3 dataset. If you would like access to the scoreboard software, please visit [the CTF Scoreboard Github repository](#). If you are looking for the BOTS version 2 dataset, it can be found [here](#). If you are looking for the BOTS version 1 dataset, it can be found [here](#).

Download

Dataset	Description	Size	Format	MDS
BOTS V3 Dataset	BOTSv3 dataset.	320.1MB	Pre-indexed Splunk	d7ccca99a01cff070dff3c139cdc10eb

Installation

1. Download the dataset file indicated above and check the MDS hash to ensure integrity.
2. Install Splunk Enterprise and the apps/add-ons listed in the *Required Software* section below. It is

About

Splunk Boss of the SOC version 3 dataset.

- Readme
- CC0-1.0 license
- Activity
- Custom properties
- 394 stars
- 30 watching
- 61 forks
- Report repository

Releases

No releases published

Packages

No packages published

Contributors

daveherrald Dave Herald

timfrazier1 Tim Frazier

I navigated to the correct path to confirm that the file had been correctly copied.

```
root@student-VMware-Virtual-Platform:~$ cd /opt/splunk/etc/apps/
root@student-VMware-Virtual-Platform:/opt/splunk/etc/apps$ ls
botsv3_data_set  botsv3_data_set.tgz
root@student-VMware-Virtual-Platform:/opt/splunk/etc/apps$ cp -r botsv3_data_
set /opt/splunk/etc/apps/
root@student-VMware-Virtual-Platform:/opt/splunk/etc/apps$ cd /opt/splunk/etc
/apps/
<root>
```

The terminal shows the user navigating to the '/opt/splunk/etc/apps/' directory, listing files, and then copying the 'botsv3_data_set' directory back into the '/opt/splunk/etc/apps/' directory.

Version 3

A sample security dataset and CTF platform for information security professionals, researchers, students, and enthusiasts. This page hosts information regarding the version 3 dataset. If you would like access to the scoreboard software, please visit [the CTF Scoreboard Github repository](#). If you are looking for the BOTS version 2 dataset, it can be found [here](#). If you are looking for the BOTS version 1 dataset, it can be found [here](#).

Download

Dataset	Description	Size	Format	MDS
BOTS V3 Dataset	BOTSv3 dataset.	320.1MB	Pre-indexed Splunk	d7ccca99a01cff070dff3c139cdc10eb

Installation

1. Download the dataset file indicated above and check the MDS hash to ensure integrity.
2. Install Splunk Enterprise and the apps/add-ons listed in the *Required Software* section below. It is

About

Splunk Boss of the SOC version 3 dataset.

- Readme
- CC0-1.0 license
- Activity
- Custom properties
- 394 stars
- 30 watching
- 61 forks
- Report repository

Releases

No releases published

Packages

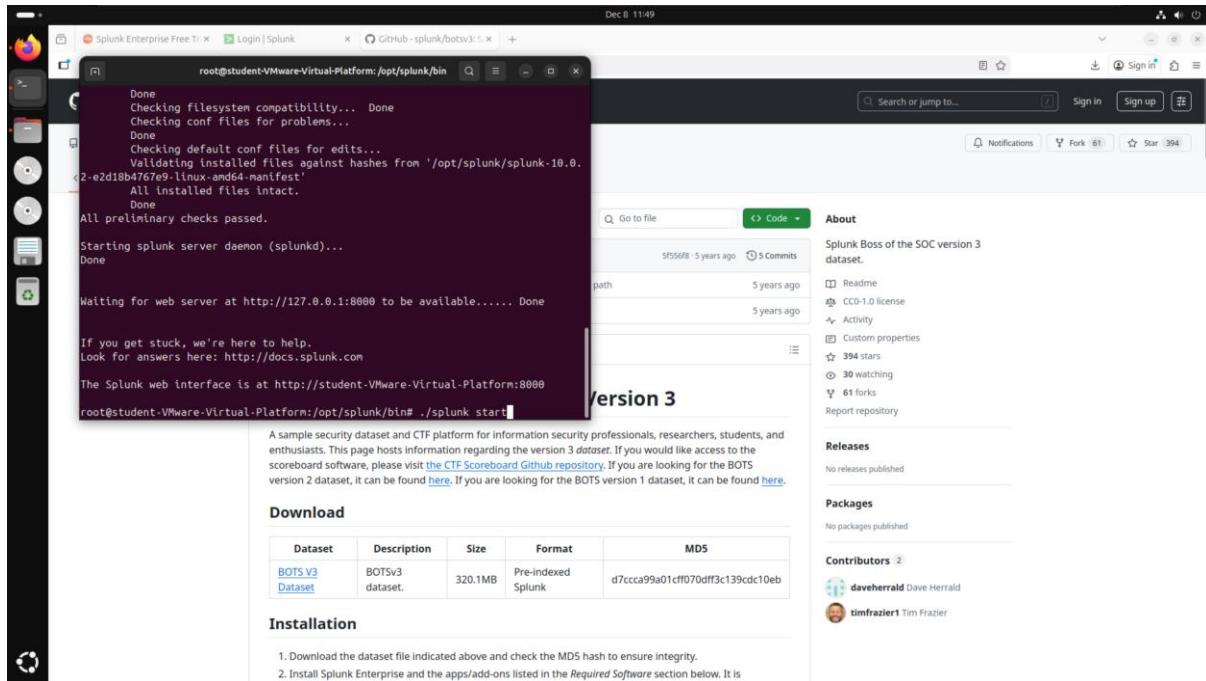
No packages published

Contributors

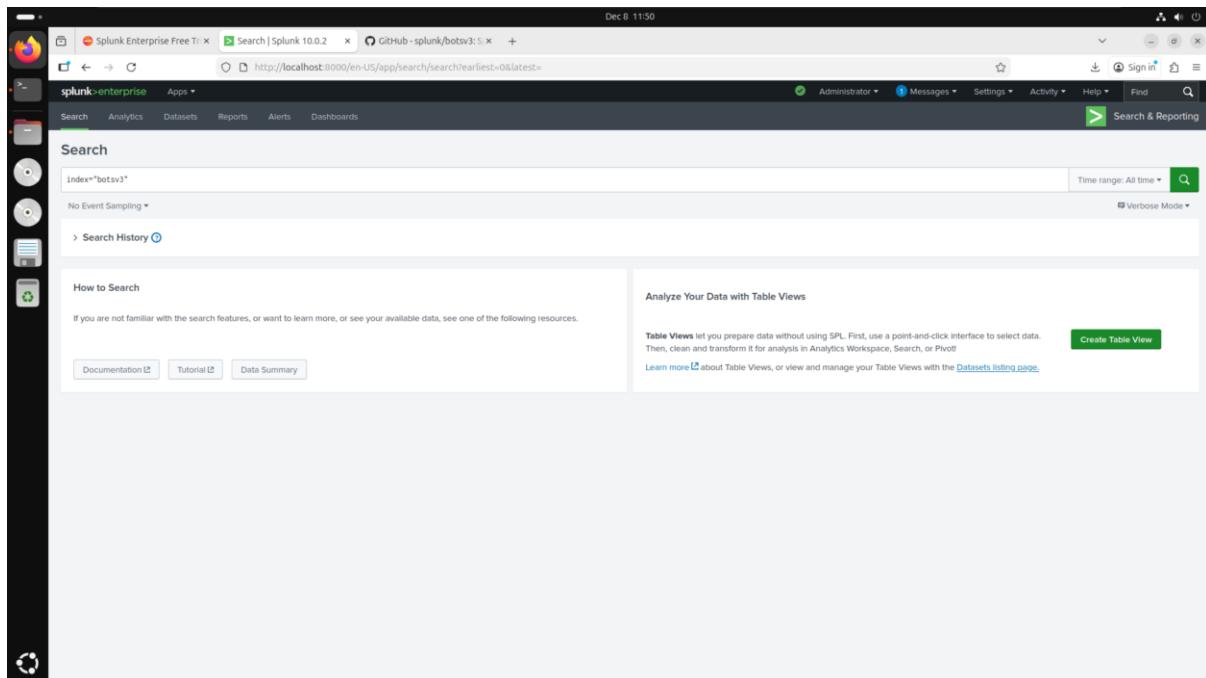
daveherrald Dave Herald

timfrazier1 Tim Frazier

I started Splunk using the command “./splunk start”. I did not have to include the “sudo” command at the beginning of the line as I was still in root mode.



I opened Splunk by searching for localhost:8000 on Firefox. I navigated to the Search & Reporting page then applied the filter index="botsv3".



Running the search with the filter index="botsv3" and setting the time range to filter for all time, I confirmed that the dataset had correctly installed as I had the correct number of 2,083,056 search results. This meant my data was correctly prepared and ready for me to answer the questions. Validating the correct number of events was important to keep data integrity, which is critical in SOC environments since incorrect data could lead to incorrect results.

The screenshot shows the Splunk Enterprise Free Edition interface. The search bar at the top contains the query "index='botsv3'". Below the search bar, it says "2,083,056 events (before 12/8/25 11:50:45.000 AM) No Event Sampling". The main area displays a table of search results with columns for Time and Event. The first event in the table is a log entry:

```

9/19/19 7:10:50.000 PM <error><message>Splunk daemon is not responding: ('Error connecting to /services/shcluster/config/config: [Errno 1111] Connection refused.',)</message></error>
host = OD-FM-NA-1-Osd2d65d4bdace22.amazonaws.com

```

Below the table, there are sections for "SELECTED FIELDS" and "INTERESTING FIELDS", each listing numerous fields such as @decorations.username, @eventTime, @host, @bytes_in, @bytes_out, @date_hour, @date_minute, @date_second, @date_year, @date_zone, @dest_ip, @dest_mac, @endtime, @flow_id, @punct, and @source.

Guided Questions:

This section answers some of the 200-level questions relating to BOTSv3, showing a typical real-world SOC workflow, determining an attacker and identifying information surrounding an incident. There are 8 questions total that I will answer, outlining which Splunk filters I used and what my results were.

Question 1:

The screenshot shows the Splunk interface with a search bar containing the query "index=botsv3 sourcetype='aws:cloudtrail'". The results show 6,571 events. A modal window is open for the field "useridentity.userName", which displays top values: splunk_access (4,891 events, 75.41%), web_admin (646 events, 11.998%), bstoll (615 events, 11.336%), and btun (73 events, 1.346%). Below the modal, a specific event is expanded, showing details like awsRegion: us-west-1, eventID: f6f6013b-5b87-432c-bd87-d2219345e920, eventName: Decrypt, and eventSource: kms.amazonaws.com.

I used the provided hint to filter Splunk by sourcetype="aws:cloudtrail". I then searched through the available filters to find anything which could be related to usernames. Here I found the filter for "useridentity.username", which I then applied to show me the 4 usernames; bstoll, btun, splunk_access and web_admin. This links to tier 1 of SOC as I am monitoring the dashboards to find if an incident has occurred by checking which users have access.

Question 2:

The screenshot shows the Splunk interface with a search bar containing the query "index=botsv3 sourcetype='aws:cloudtrail' rnf='". The results show 2,355 events. A modal window is open for the field "Event", displaying a single event from 8/20/18 at 4:15:20.000 PM. The event details include awsRegion: us-west-1, eventID: 976bfccb-3cf-437c-8b85-4043635ce306, eventName: DescribeInstanceStatus, eventSource: ec2.amazonaws.com, eventTime: 2018-08-20T15:15:20Z, eventVersion: 1.05, recipientAccountId: 622676721278, requestId: f4bd49e9-e27c-4a52-93fa-fab7a76d3639, and requestParameters: {}.

I kept the same filter as question 1 and searched additionally for *MFA* using the provided hint to find anything relating to multi-factor authentication. I then searched for “mfa” in the additional filters which led me to find the filter `userIdentity.sessionContext.attributes.mfaAuthenticated`.

Question 3:

	Time	Event
1	8/20/18 3:26:25.000 PM	KEY VALUE CPU_TYPE Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.4GHz CPU_CACHE 38720 KB CPU_COUNT 2 HARD_DRIVES xvda 8 GB; host = gacrux-i-09cbc261e04299654
2	8/20/18 3:24:24.000 PM	KEY VALUE CPU_TYPE Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.4GHz CPU_CACHE 38720 KB CPU_COUNT 2 HARD_DRIVES xvda 8 GB; host = gacrux-i-06fea5b6f3d3c1ce8
3	8/20/18 2:34:50.000 PM	KEY VALUE CPU_TYPE Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.4GHz CPU_CACHE 38720 KB CPU_COUNT 2 HARD_DRIVES xvda 8 GB; host = gacrux-i-occ93bafe2b3cba63

I changed the filter to be `sourcetype="hardware"` using the provided hint, which then showed me the list of hardware being used to connect to the server. Looking into these values, I found the value `CPU_TYPE` which was listed as the model number `E5-2676`.

Question 4:

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** index=botsv3 sourcetype="aws:cloudtrail" eventName="PutBucketAcl"
- Results:** 2 events (before 12/7/25 5:07:21.000 PM) No Event Sampling
- Event 1 (Left):** Time: 8/20/18 2:57:54.000 PM. Event ID: ab45689d-69cd-41e7-8705-5350402cf7ac. Event Name: PutBucketAcl. Event Source: s3.amazonaws.com. Event Type: AmazonS3. Version: 1.05. Recipient Account ID: 622676721278. Request ID: 487488003569438. Request Parameters: null. Response Elements: null. Source IP Address: 107.77.212.179. User Agent: signin.amazonaws.com. User Identity: ab45689d-69cd-41e7-8705-5350402cf7ac.
- Event 2 (Right):** Time: 8/20/18 2:01:46.000 PM. Event ID: ab45689d-69cd-41e7-8705-5350402cf7ac. Event Name: PutBucketAcl. Event Source: s3.amazonaws.com. Event Type: AmazonS3. Version: 1.05. Recipient Account ID: 622676721278. Request ID: 487488003569438. Request Parameters: null. Response Elements: null. Source IP Address: 107.77.212.179. User Agent: signin.amazonaws.com. User Identity: ab45689d-69cd-41e7-8705-5350402cf7ac.

I changed the filter back to sourcetype="aws:cloudtrail", and added a filter for eventName="PutBucketAcl" based on the provided hints. From here, I noticed 2 separate events with different event IDs. I assumed that one event would be the user making the S3 bucket public, and the other event would be the user making the S3 bucket private again. Taking the ID of the newest event, this gave me the answer of ab45689d-69cd-41e7-8705-5350402cf7ac.

Question 5:

The screenshot shows a Splunk search interface with the following details:

- Search Query:** `index=botsv3 sourcetype="aws:cloudtrail" eventName="PutBucketAcl"`. This query filters for CloudTrail events where the source type is AWS CloudTrail and the event name is PutBucketAcl.
- Time Range:** Dec 7 17:16 to Dec 7 17:16. The search has found 2 events before 12/7/25 5:07:21 PM.
- Event Details:** One event is displayed in the main pane. It occurred at 8:20:18 on 2018-08-25T14:00:00Z. The event ID is ab45489e-6fc0-41e7-8705-5358482cf7ac. The event source is s3.amazonaws.com, and the event type is AnonApicall. The event version is 1.0S. The recipient account ID is 622676721278, and the request ID is 4f74840000364948. The user identity is bstoll. The event details also include accessKeyId, accountID, arn, invokeIdentity, principalId, sessionContext, type, and userArn.

I applied the same filters as question 4. From there, I opened the userIdentity field within the relevant event and found that the username was bstoll.

Question 6:

The screenshot shows a Splunk search interface with the following details:

- Search Query:** `index=botsv3 sourcetype="aws:cloudtrail" eventName="PutBucketAcl"`. This query filters for CloudTrail events where the source type is AWS CloudTrail and the event name is PutBucketAcl.
- Time Range:** Dec 7 17:22 to Dec 7 17:22. The search has found 2 events before 12/7/25 5:07:21 PM.
- Event Details:** One event is displayed in the main pane. It occurred at 8:20:18 on 2018-08-25T14:00:00Z. The event ID is ab45489e-6fc0-41e7-8705-5358482cf7ac. The event source is s3.amazonaws.com, and the event type is AnonApicall. The event version is 1.0S. The recipient account ID is 622676721278, and the request ID is 4f74840000364948. The user identity is bstoll. The event details now include additional fields such as AccessControlPolicy, AccessControlList, Owner, and website.

I applied the same filters as question 4. From there, I opened the requestParameters field within the relevant event and found that the bucketName was frothlywebcode.

Question 7:

The screenshot shows the Splunk 10.0.2 interface with a search titled "New Search". The search bar contains the query: `index=botsv3 sourcetype="aws:s3:accesslogs" date_hour=14 PUT *txt*`. The results table has one event listed:

	Time	Event
>	8/20/18 2:02:44:000 PM	4c818853e740f45beb45f68c8ff5eff6347745488ae540130432c9fc64fae318d frothlywebcode [20/Aug/2018:13:02:44 +0000] 52.66.146.128 ~ -DF1BA9BD9E236984 REST.PUT_OBJECT OPEN_BUCKET PLEASE_FIX.txt "PUT /OPEN_BU CKET PLEASE_FIX.txt HTTP/1.1" 200 - 377 268 5 "-" "Botos/1.7.62 Python/2.7.14 Linux/4.14.47-64.38.amzn2.x86_64 Botcore/1.8.12" host = splunk.froth.ly source = s3://frothlyweblogs/s32018-07-26-01-20-56-19D73C05AA29AEDB sourcetype = aws:s3:accesslogs

The sidebar on the left lists "SELECTED FIELDS" and "INTERESTING FIELDS".

I changed the filter to `sourcetype="aws:s3:accesslogs"` based on the provided hint. Then, knowing that the events in questions 4 to 6 occurred between 2pm and 3pm, I added a filter for `date_hour=14` to check specifically between these times. Next, I added another filter for HTTP `PUT` requests, since the question involved uploading a file to the S3 bucket. I lastly added a filter for `*txt*` since the question mentioned a text file being uploaded which hinted to me that it would be a .txt file. This led me to find the uploaded text file "OPEN_BUCKET PLEASE_FIX.txt".

Question 8:

Dec 8 02:35

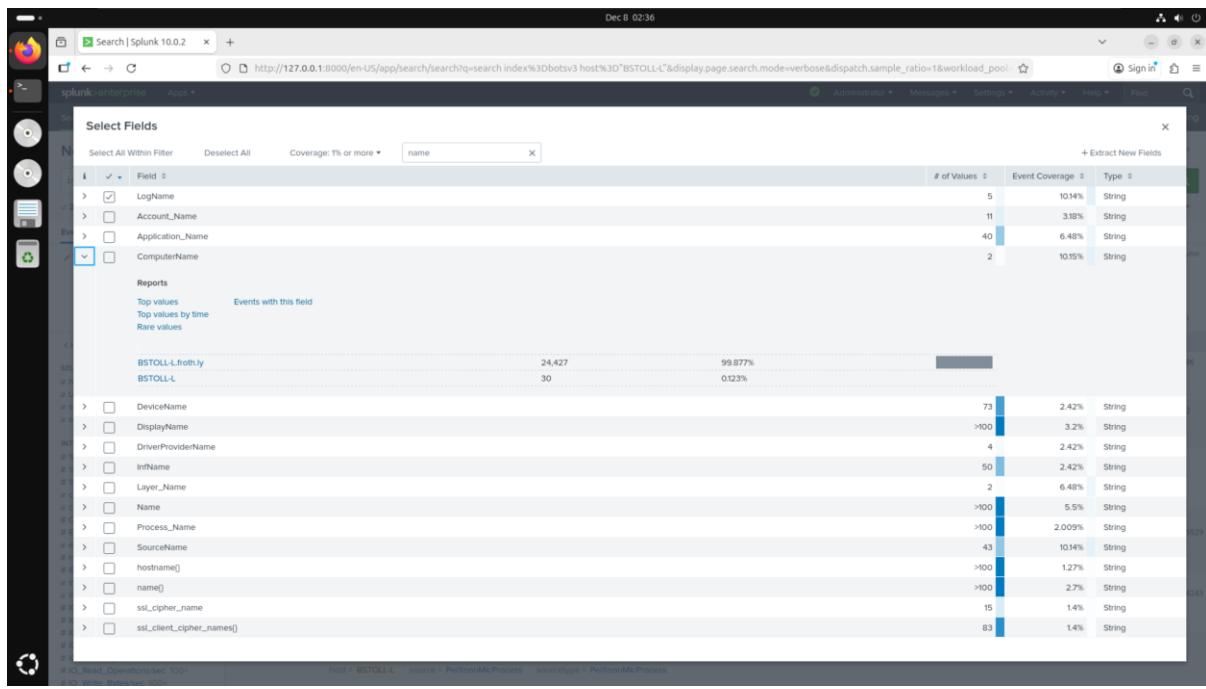
Events (30)

Time	Event
8/20/18 4:14:22.000 PM	Type="operatingSystem OS="Microsoft Windows 10 Enterprise" Architecture="64-bit" Version="10.0.17134" BuildNumber="17134" Show all 22 lines host = BSTOLL-L source = operatingSystem sourcetype = WinHostMon
8/20/18 4:04:21.000 PM	Type="operatingSystem OS="Microsoft Windows 10 Enterprise" Architecture="64-bit" Version="10.0.17134" BuildNumber="17134" Show all 22 lines host = BSTOLL-L source = operatingSystem sourcetype = WinHostMon
8/20/18 3:54:26.000 PM	Type="operatingSystem OS="Microsoft Windows 10 Enterprise" Architecture="64-bit" Version="10.0.17134" BuildNumber="17134" Show all 22 lines host = BSTOLL-L source = operatingSystem sourcetype = WinHostMon
8/20/18 3:29:27.000 PM	Type="operatingSystem OS="Microsoft Windows 10 Enterprise" Architecture="64-bit"

Dec 8 02:36

Events (240,882)

Time	Event
8/20/18 4:17:59.000 PM	ApplicationFrameHost 0 0 0 0 2203614883840 2203607330816 0 51679322 37842944 33497088 20021248 20021248 5 8 21024,4694806 host = BSTOLL-L source = PerfmonMkProcess sourcetype = PerfmonMkProcess
8/20/18 4:17:59.000 PM	Calculator 0 0 0 0 462167248 4618731520 0 54685696 36220928 20492288 16691200 16691200 22 8 19887.78423 5212 host = BSTOLL-L source = PerfmonMkProcess sourcetype = PerfmonMkProcess
8/20/18 4:17:59.000 PM	CrashPlanDesktop 0.339013653131165 0.3139043564397653 0.6260007128794111 339644416 389473288 2.8844757918851634 59437056 48525312 38785024 host = BSTOLL-L source = PerfmonMkProcess sourcetype = PerfmonMkProcess
8/20/18 4:17:59.000 PM	CrashPlanService 24514568 24514568 28 8 21085.668339 10015 4456 516888 42240 710 1.2019159108875273 0 1.2019159108875273 8 278.8454193874391 host = BSTOLL-L source = PerfmonMkProcess sourcetype = PerfmonMkProcess
8/20/18 4:17:59.000 PM	CrashPlanDesktop# 0 0 0 0 3154352 304535394 8.01279940538818 6956120 51744768 64954368 47398912 47398912 16 8 host = BSTOLL-L source = PerfmonMkProcess sourcetype = PerfmonMkProcess
8/20/18 4:17:59.000 PM	CrashPlanService# 0.6260007128794111 0.156592178277 0.4655085346559583 1572859848 15701857536 0 70525120 125366272 659554384 355799480 host = BSTOLL-L source = PerfmonMkProcess sourcetype = PerfmonMkProcess
8/20/18 4:17:59.000 PM	GoogleCrashHandler 0 0 0 0 69746688 64583888 0 6883456 1134592 1953792 1867072 1667872 3 4 20981.8776684 1724 6148 124176 18289 168 host = BSTOLL-L source = PerfmonMkProcess sourcetype = PerfmonMkProcess



I started by filtering for sourcetype="winhostmon" using the provided hint. I then searched through the filters to find a filter for "operatingsystem" and an additional filter for OS="Microsoft Windows 10 Enterprise". This operating system only had 30 uses, which all came from one user – BSTOLL-L. Once I had this user, I then removed my operatingsystem and OS filters, and instead added a filter for host="BSTOLL-L". I searched the filters list again for anything relating to FQDN, however I could not find anything. I instead searched the additional filters for anything relating to "name", where I found the filter ComputerName which when inspected had the value of BSTOLL-L.froth.ly.

Conclusion:

This report has demonstrated the real-world application of SOC tiers when analysing the BOTSV3 dataset within Splunk. I have mainly applied tier 2 of SOC, however, have also applied other incident handling methodologies to investigate and identify security incidents within the dataset. Overall, this report has highlighted the importance of real-world SOC operations in identifying and analysing security incidents.

References:

BOTSv3 GitHub download: <https://github.com/splunk/botsv3>

ChatGPT: <https://chatgpt.com/>

Splunk Enterprise download: https://www.splunk.com/en_us/download/splunk-enterprise.html

SOC roles explanation: <https://www.paloaltonetworks.com/cyberpedia/soc-roles-and-responsibilities#:~:text=A%20security%20operations%20center%2C%20or,security%20solutions%2C%20tools%20and%20products.>

NIST incident handling methodology: <https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions>

AI Declaration:

Solo Work	S1 - Generative AI tools have not been used for this assessment.	<input type="checkbox"/>
Assisted Work	A1 – Idea Generation and Problem Exploration Used to generate project ideas, explore different approaches to solving a problem, or suggest features for software or systems. Students must critically assess AI-generated suggestions and ensure their own intellectual contributions are central.	<input type="checkbox"/>
	A2 - Planning & Structuring Projects AI may help outline the structure of reports, documentation and projects. The final structure and implementation must be the student's own work.	<input type="checkbox"/>
	A3 – Code Architecture AI tools maybe used to help outline code architecture (e.g. suggesting class hierarchies or module breakdowns). The final code structure must be the student's own work.	<input type="checkbox"/>
	A4 – Research Assistance Used to locate and summarise relevant articles, academic papers, technical documentation, or online resources (e.g. Stack Overflow, GitHub discussions). The interpretation and integration of research into the assignment remain the student's responsibility.	<input type="checkbox"/>
	A5 - Language Refinement Used to check grammar, refine language, improve sentence structure in documentation not code. AI should be used only to provide suggestions for improvement. Students must ensure that the documentation accurately reflects the code and is technically correct.	<input type="checkbox"/>
	A6 – Code Review AI tools can be used to check comments within the code and to suggest improvements to code readability, structure or syntax. AI should be used only to provide suggestions for improvement. Students must ensure that the code accurately reflects their knowledge and is technically correct.	<input type="checkbox"/>
	A7 - Code Generation for Learning Purposes Used to generate example code snippets to understand syntax, explore alternative implementations, or learn new programming paradigms. Students must not submit AI-generated code as their own and must be able to explain how it works.	<input type="checkbox"/>
	A8 - Technical Guidance & Debugging Support AI tools can be used to explain algorithms, programming concepts, or debugging strategies. Students may also help interpret error messages or suggest possible fixes. However, students must write, test, and debug their own code independently and understand all solutions submitted.	<input type="checkbox"/>
	A9 - Testing and Validation Support AI may assist in generating test cases, validating outputs, or suggesting edge cases for software testing. Students are responsible for designing comprehensive test plans and interpreting test results.	<input type="checkbox"/>
	A10 - Data Analysis and Visualization Guidance AI tools can help suggest ways to analyse datasets or visualize results (e.g.	<input type="checkbox"/>

	<p>recommending chart types or statistical methods). Students must perform the analysis themselves and understand the implications of the results.</p> <p>A11 - Other uses not listed above</p> <p>Please specify:</p>	
Partnered Work	<p>P1 - Generative AI tool usage has been used integrally for this assessment</p> <p>Students can adopt approaches that are compliant with instructions in the assessment brief.</p> <p>Please Specify:</p> <ul style="list-style-type: none"> - Locating reports - Summarising reports - Fixing grammar - More precise language 	<input checked="" type="checkbox"/>

Please provide details of AI usage and which elements of the coursework this relates to:

Partnered Work – Used to locate and summarise reports for SOC and incident handling, Used to make language more concise and in proper English, including fixing grammar

I understand that the ownership and responsibility for the academic integrity of this submitted assessment falls with me, the student.	<input checked="" type="checkbox"/>
I confirm that all details provided above are an accurate description of how AI was used for this assessment.	<input checked="" type="checkbox"/>