Github url: https://github.com/wingftsui/COMP3010HK-CW2

(A) Introduction

This report using the view of “Frothly” company’s Security Operations Centre (SOC) lead to analyze the Cyber Kill Chain(CKC) of incident data (BOTSv3).
Part (B) reflects the SOC tiers on BOTSv3 incident. It also discuss the incident handling phrases.
Part (C) is to justify the tools used to analyze the data. As well as ensuring a proper analytical environment.
Part (D) analysis the BOTSv3 guided questions. They are provided by Frothly.
Part (E) is the conclusion.

(B) Soc Roles & Incident Handling

SOC has three tiers. Tier 1 is the Triage specialist, which mainly reviews the alerts or adjust SIEM rules. Tier 2 acts as the incident responder. That is what I am doing in this analysis report. Tier 3 is the threat hunter. It is mainly hunting threats, implement the penetration tests, designing security strategies. Also, it is the evaluation of tier 1 and tier 2. In this report, part (D) will use the view of SOC tier2. The suggestions in Part (E) will use the view of SOC tier3.

SOC TIER 1

Frothly 's deficiency is that they are depend on "People" to initiate the alert. The better measure is SIEM's auto alert system. Frothly lacks proactive monitoring.

SOC TIER 2

In Tier 2, analyze the incidents deeply (as part(D)). Using the evidence found, find out the solution to tackle the problems at the moments (e.g. restore the database, reinstall the computer, block the attacker’s IP address)

SOC TIER 3

After reviewing this report, the Frothly’s management will decide the improving strategies to prevent the similar incidents in the future.

Prevention

"Frothly" has no effective IPS(like Amazon S3 Block Public Access dicuss in the Part(E)). Therefore, the bud and other colleaques in Frothly does not know the incident had been happened. Frothly failed the prevention phrase.

Detection

The MTTD (Mean Time To Detect) is very long. It is too long to protect their assets. They even not aware the incidents until the attacker complete the attack. The reasons is that the SOC tier1 is heavily rely on people not system automation. BOTSv3 shows that Frothly is using reactive detection not proactive.

Response

Frothly's colleaques did not know the events until the whole attacked had completed. Then, they ask me to prepare this analysis report. This is also a kind of response although it is a little bit late. The better response should be automated playbooks (dicuss in part(E))

Recovery

Restore the backup file if there are any.

(C) Installation and Data Preparation

Splunk are used for the detection of this analysis report. Splunk is installed in Ubuntu in VM vitualBox.(Fig INS_1, INS_2) Running Splunk in ubuntu can save 2GB RAM compare with running in Windows. It is because ubuntu has fewer GUI and background running services.

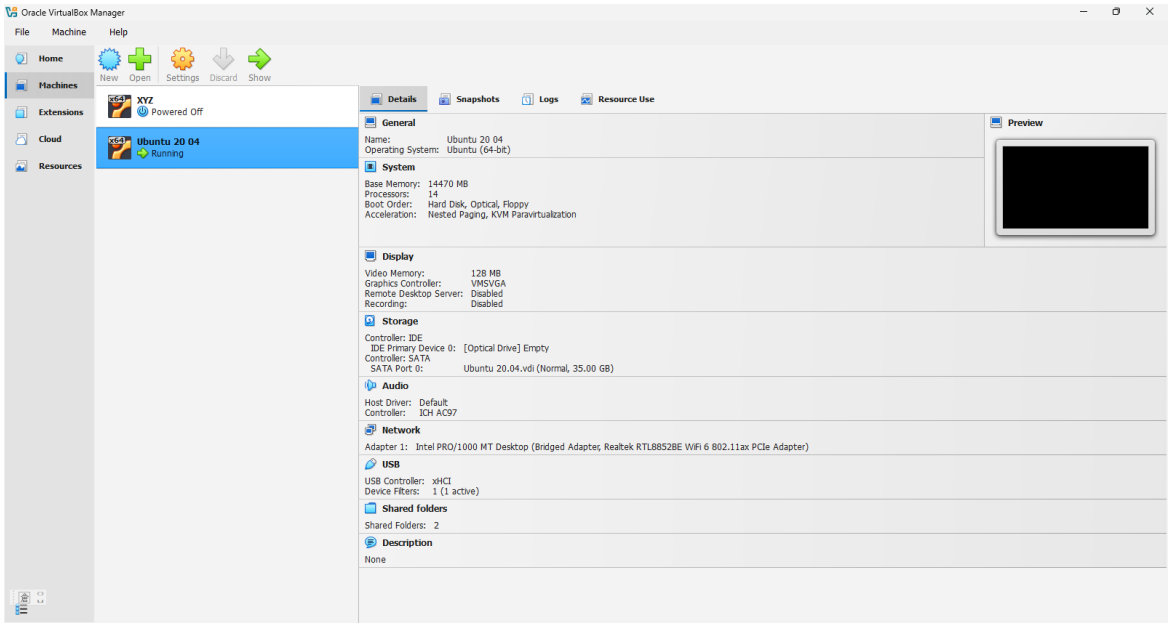

Fig INS_1

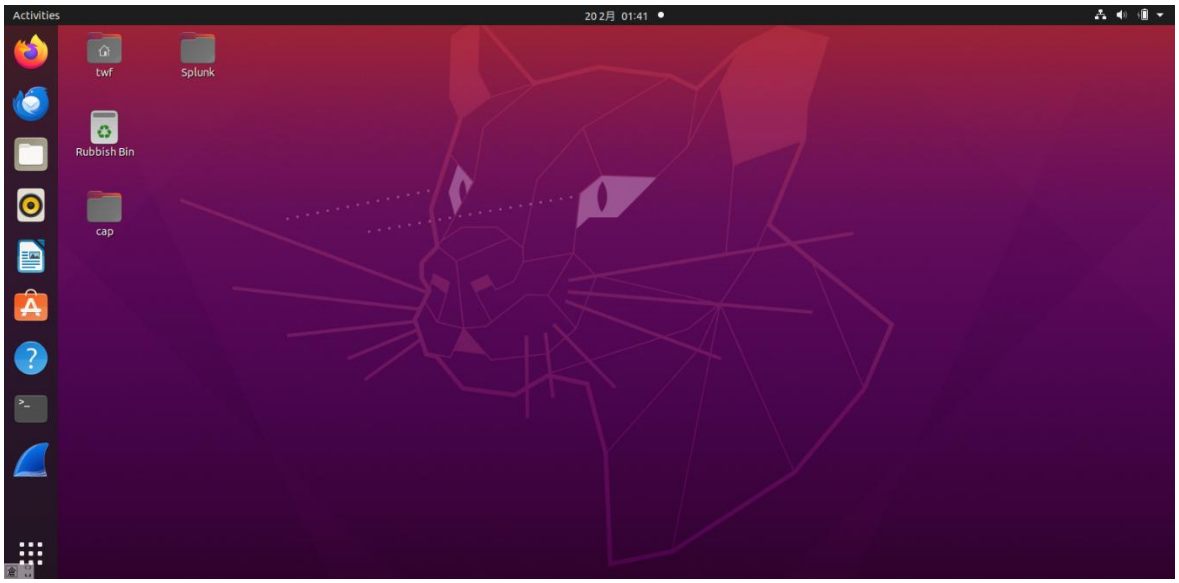

Fig INS_2

Running the script in terminal to ensure the Ubuntu’s safety quit(Fig.INS_3). It is to avoid crash in Ubuntu.

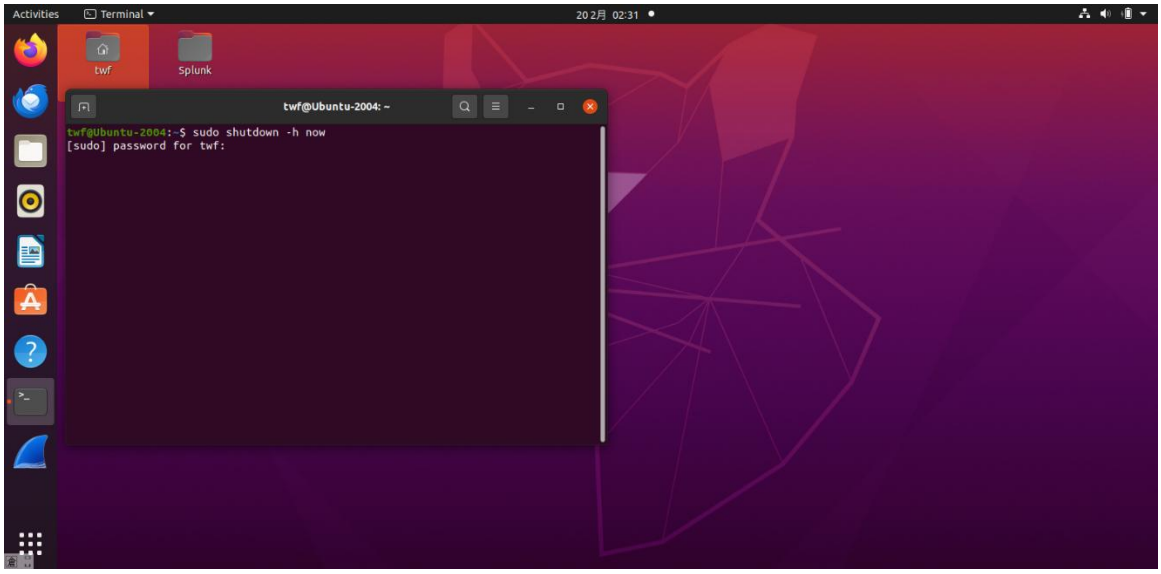

Fig.INS_3

After installing splunk and importing the BOTSv3 into it, I run “index=botsv3 earliest=0” to check the data integrity. There are 2,083,056 events (Fig INS_4) which is larger than 2,030,269 events [2]. Therefore, it is okay.

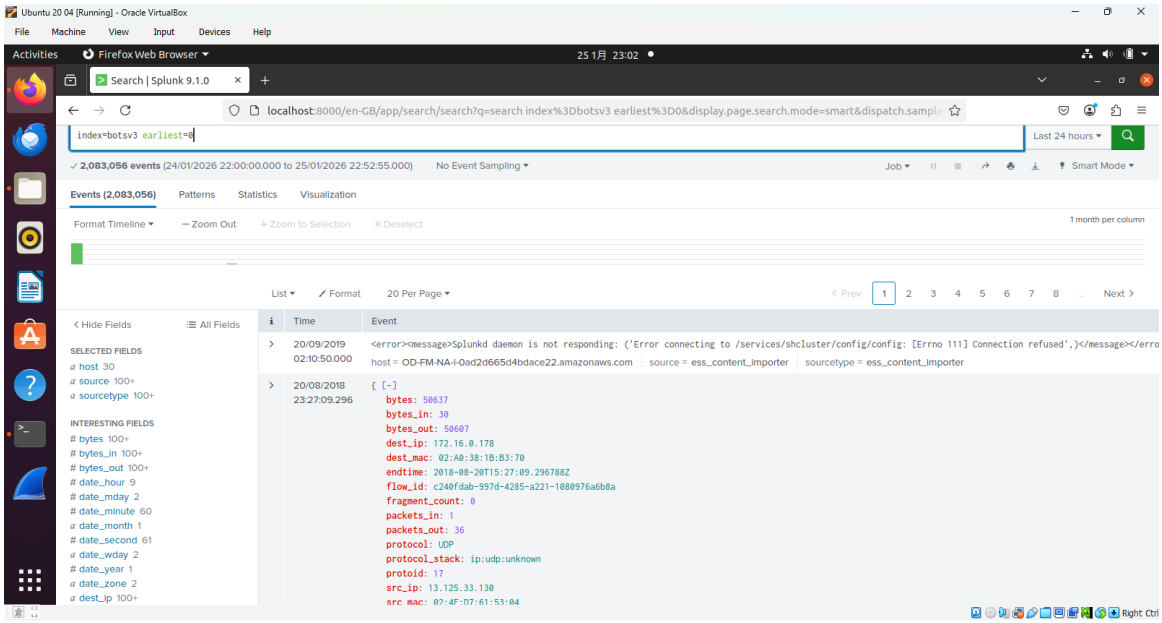

Fig.INS_4

(D) Guided Questions

Overview:

This set of 8 guided questions includes 3 phrases. Phrase 1(Q1 to Q6) is cloud oversight leads to vulnerable environment. The turning point(Q4-Q6) occurs when Bud accidentally makes an S3 bucket public. It is human negligence that leads to insider threats. Phrase 2 (Q7) describes exploitation, where the attacker discovers this publicly accessible S3 bucket. Phrase 3 (Q8) find out the outliers. This may act as the attacker’s base.

Q1

Query:

index=botsv3 earliest=0 sourcetype="aws:cloudtrail" userIdentity.type=IAMUser
| stats count by userIdentity.userName

Result (Fig.SO_CW2_Q1A):

Bstoll, btun, splunk_access, web_admin

Explanation and SOC relevance:

Using the query to search for the IAMUser that access the AWS service, bud is the main character of the whole incident. In addition, Bstoll has the activities "GetBucketAcl" (query: index=botsv3 earliest=0 sourcetype="aws:cloudtrail" | stats count by userIdentity.userName, eventName | sort – count)(results:fig.SO_CW2_1B) together with the “PutBucketAcl” in Q4 create a vulnerability for the attacker to take advantage of.

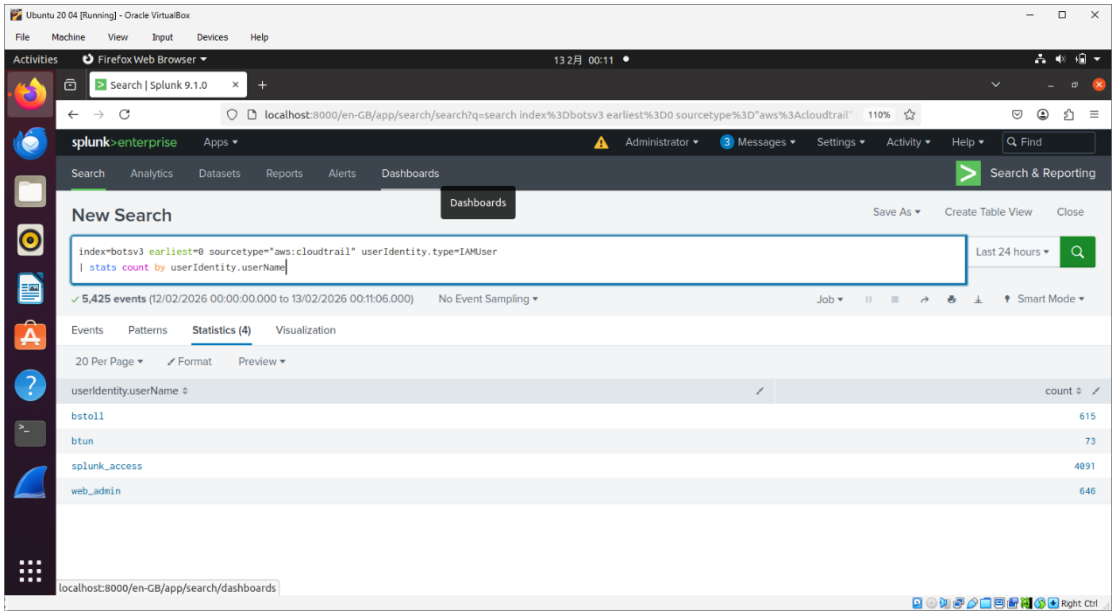

Fig.SO_CW2_Q1A

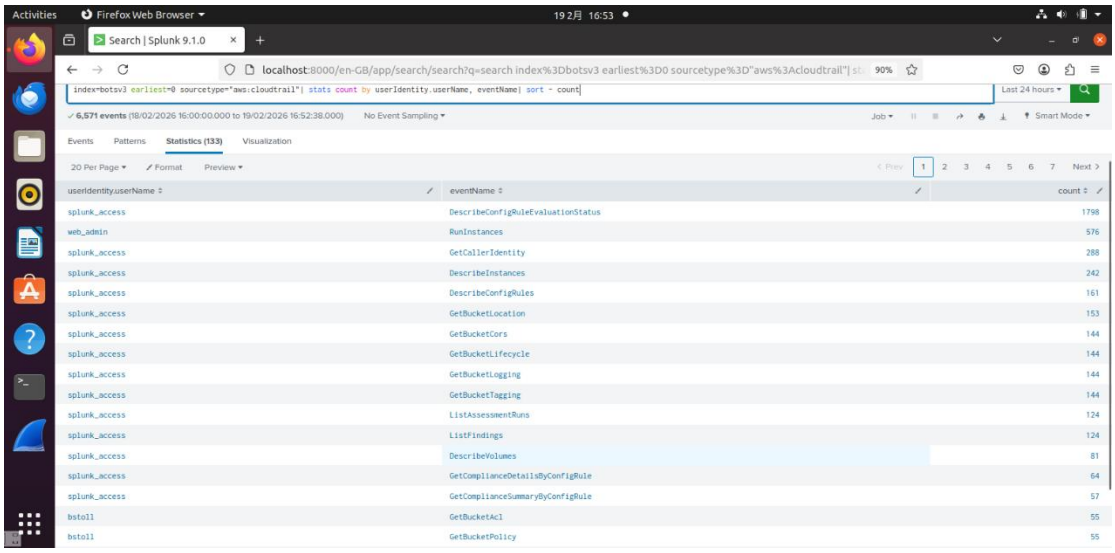

Fig.SO_CW2_Q1B

Q2

Query:

index=botsv3 earliest=0 sourcetype="aws:cloudtrail"

Results(Fig.SO_CW2_Q2A):

userIdentity.sessionContext.attributes.mfaAuthenticated

Explanation and SOC relevance:

“userIdentity.sessionContext.attributes.mfaAuthenticated” is used to determine whether the AWS service has MFA. And it is found that they are without MFA. (Fig.SO_CW2_Q2B) It is a weak link that can be exploited by an attacker

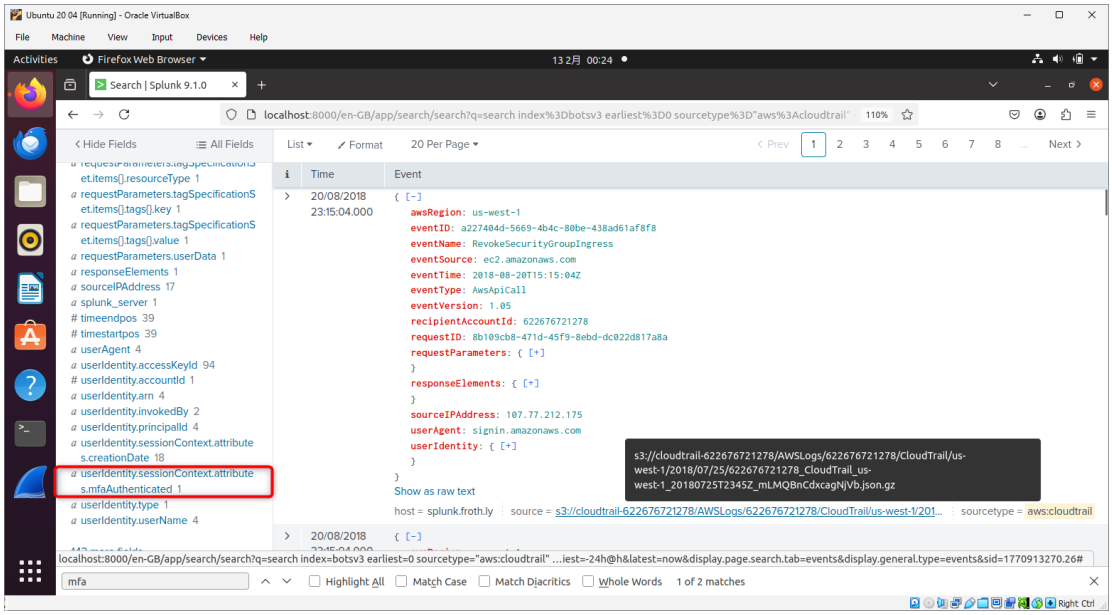

Fig.SO_CW2_Q2A

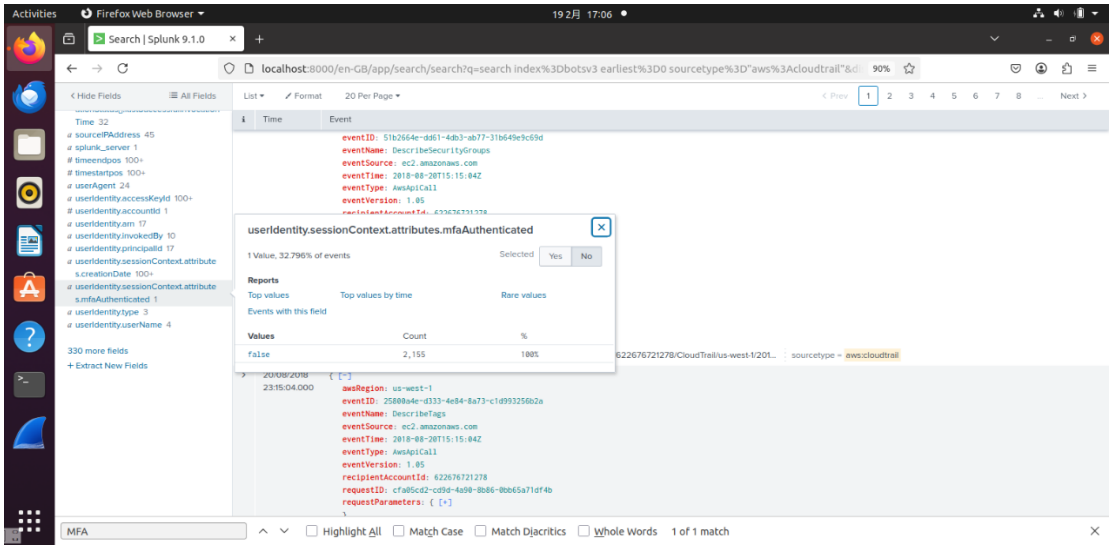

Fig.SO_CW2_Q2B

Q3

Query:

index=botsv3 earliest=0 sourcetype="hardware"

Results(Fig.SO_CW2_Q3):

E5-2676

Explanation and SOC relevance:

The processor number in the web server is important. It is because is the web server may serves as the attacker's base (where attacker can“Implanting viruses” or “executing malicious scripts”), but not this time (the bud incident).

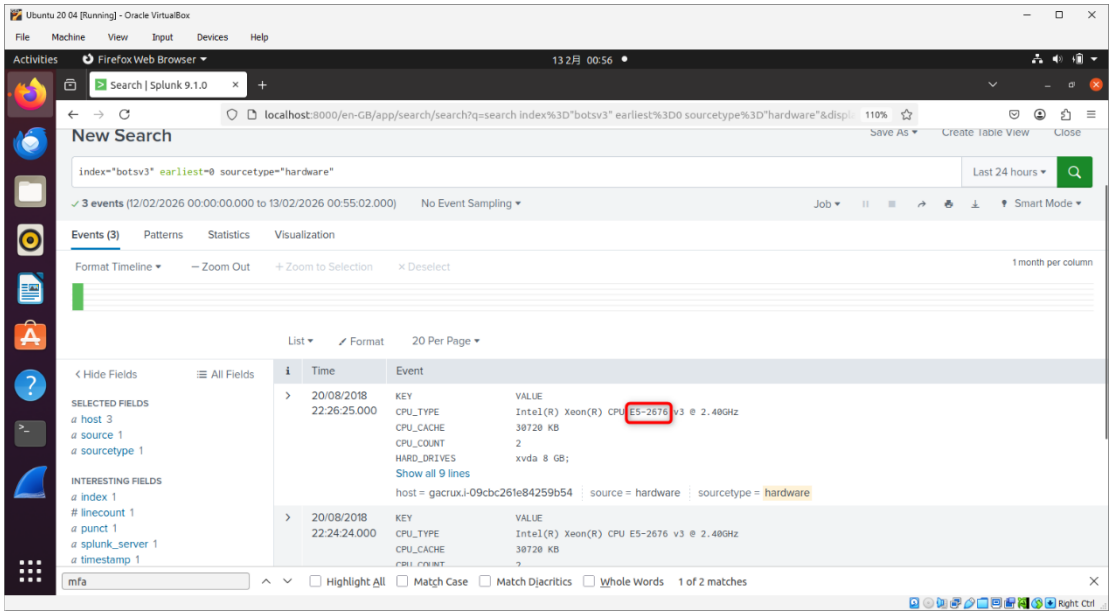

Fig.SO_CW2_Q3

Q4

Query:

index=botsv3 earliest=0 sourcetype="aws:cloudtrail" "PutBucketAcl"

Results (Fig.SO_CW2_Q4A):

ab45689d-69cd-41e7-8705-5350402cf7ac

Explanation and SOC relevance:

"PutBucketAcl" is the API call to update the access right in the S3 bucket. This event involves Bud accidentally making S3 bucket public. The attackers can use this open door to attack S3 bucket. After running the above query, there are 2 events. There are 2 reasons that the lower event is the bud incident: (i) it occurs earlier. (ii) In the payload, it has the wording "AllUsers"(Fig.SO_CW2_Q4B) which in turn meaning the bucket is publicly accessible.

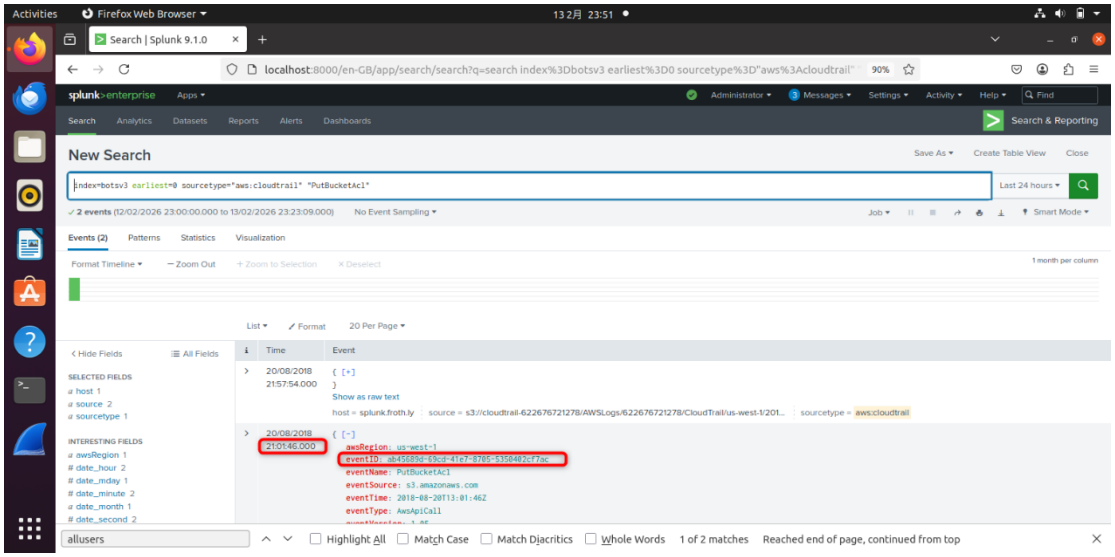

Fig.SO_CW2_Q4A

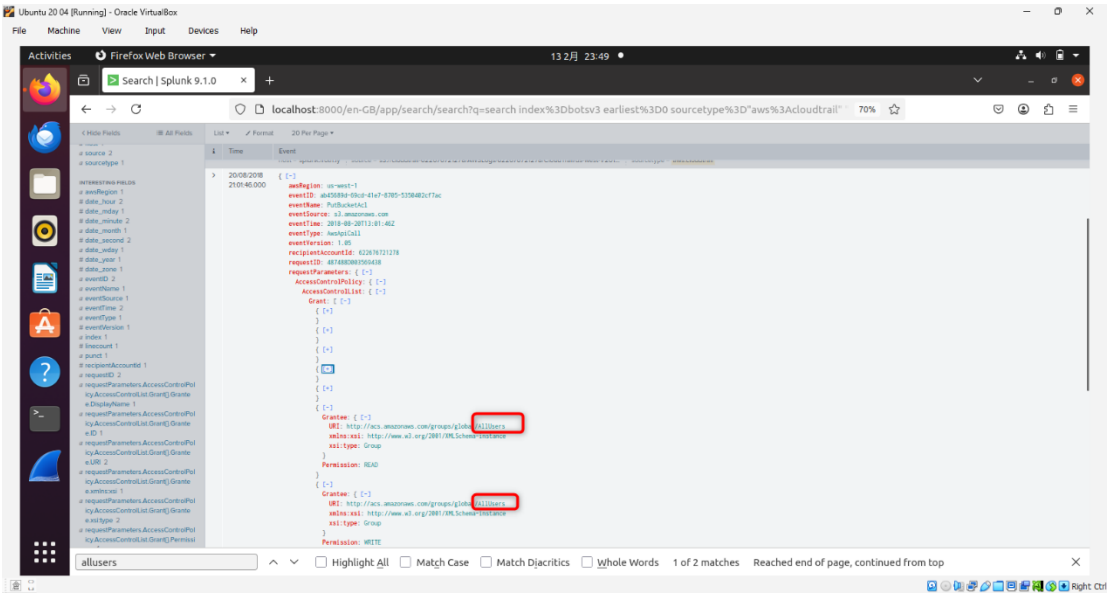

Fig.SO_CW2_Q4B

Q5

Query:

index=botsv3 earliest=0 sourcetype="aws:cloudtrail" "PutBucketAcl"

Results(Fig.SO_CW2_Q5):

Bstoll

Explanation and SOC relevance:

This user is the main character of the whole bud incident. His fault leads to S3 bucket being attacked.

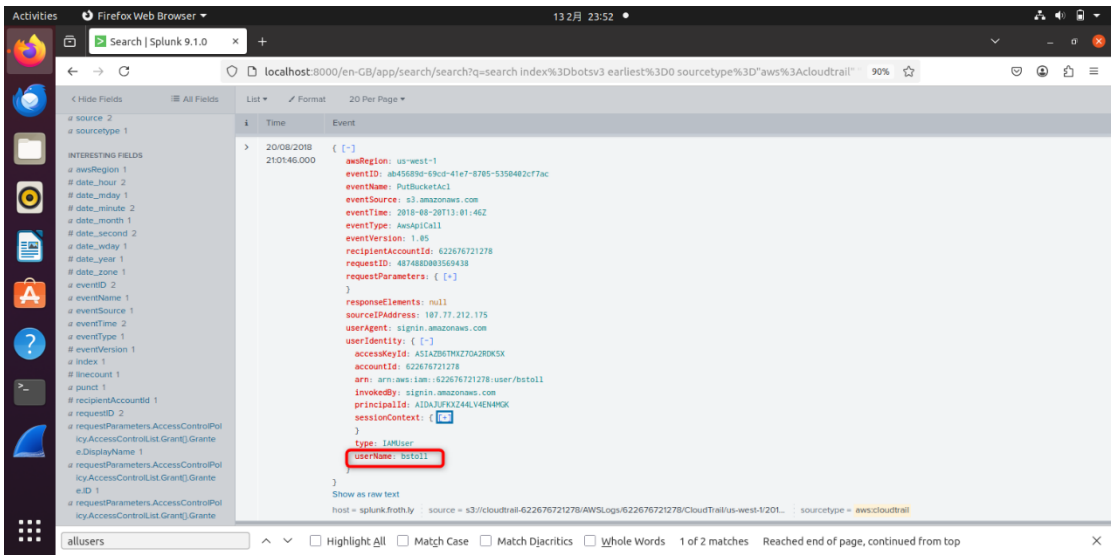

Fig.SO_CW2_Q5

Q6

Query:

index=botsv3 earliest=0 sourcetype="aws:cloudtrail" "PutBucketAcl"

Results(Fig.SO_CW2_Q6):

frothlywebcode

Explanation and SOC relevance:

Using the same query as Q4 and Q5, can found the incident's S3 bucket name. "frothlywebcode" may become the attack target of the attacker or may be used as lateral movement in the cyber kill chain.

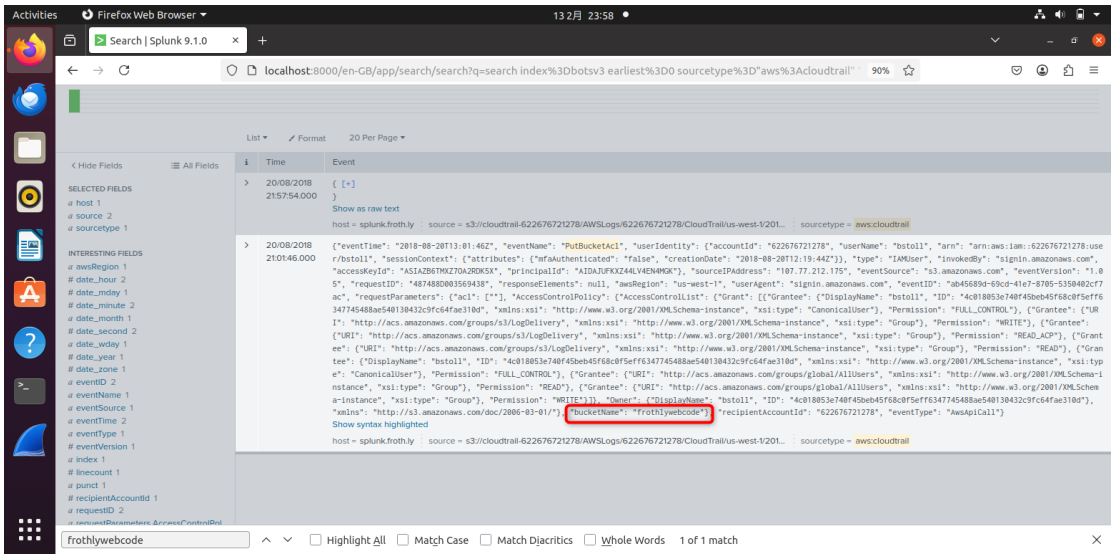

Fig.SO_CW2_Q6

Q7

Query:

index="botsv3" earliest=0 sourcetype="aws:s3:accesslogs" "*.txt"

Results(Fig.SO_CW2_Q7B):

OPEN_BUCKET_PLEASE_FIX.txt

Explanation and SOC relevance:

First of all, (using query: index="botsv3" earliest=0 sourcetype="*aws")I found that "aws:s3:accesslogs" is the access logs of aws(Fig.SO_CW2_Q7A). Then, I found that the attacker upload the file to the S3 bucket. This is the exploitation occurs. The attacker used the vulnerability (in Q4 to Q6, that is the publicly access S3 bucket) to launch an offensive.

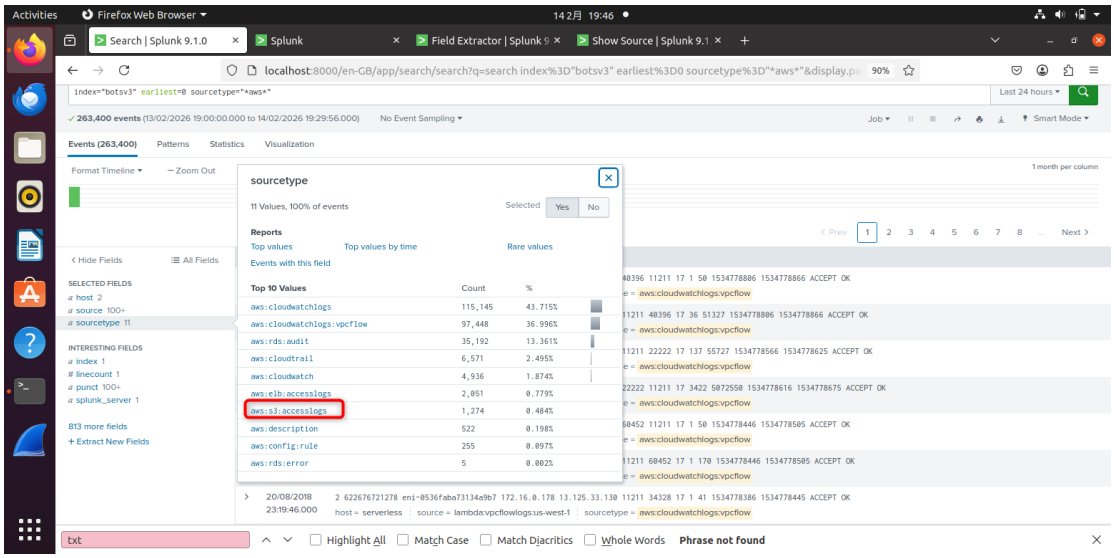

Fig.SO_CW2_Q7A

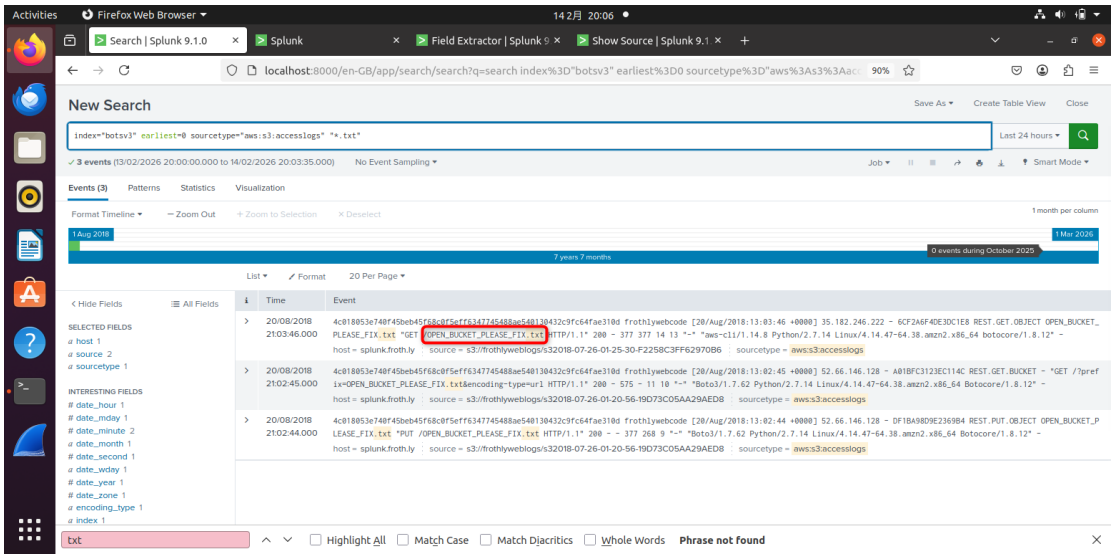

Fig.SO_CW2_Q7B

Q8

Query:

(i)

```
index="botsv3" earliest=0 sourcetype="winhostmon"
| stats count by OS, host
```

(ii)

```
index="botsv3" earliest=0 sourcetype="WinEventLog:Security" host="BSTOLL-L"
|head 1
|table ComputerName
```

Results (SO_CW2_Q8B):

BSTOLL-L.froth.ly

Explanation and SOC relevance:

Using query(i) can find out the different Windows operating systems that are running(Fig.SO_CW2_Q8A). In the SOC point of view, anything that deviate from the normal practice can be the part of cyber kill chain. In this case, only one host is using Windows 10 Enterprise. Therefore, it is the outlier. It needs to be aware of it. Using query(ii) can find out its FQDN.

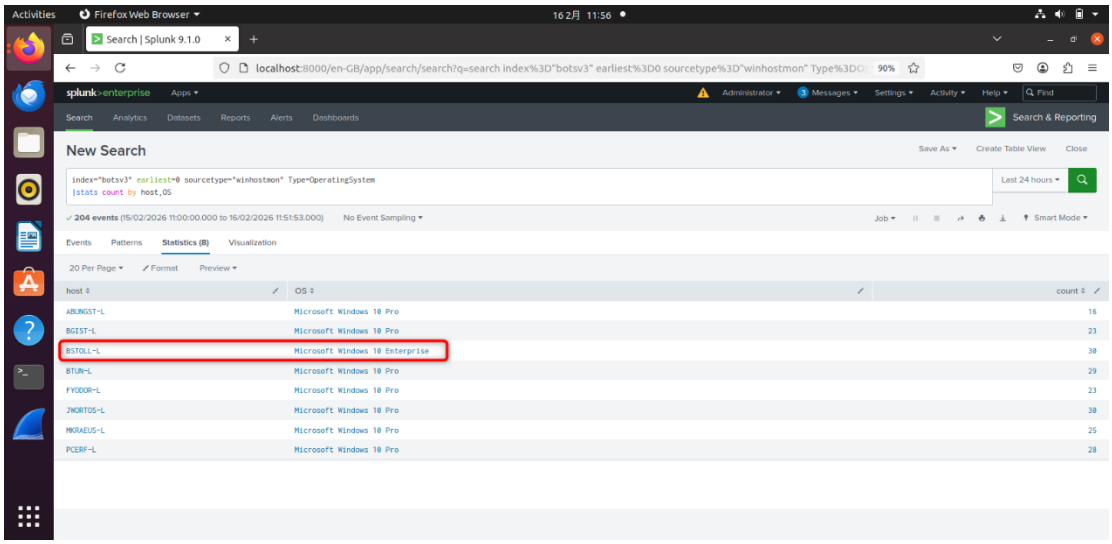

Fig.SO_CW2_Q8A

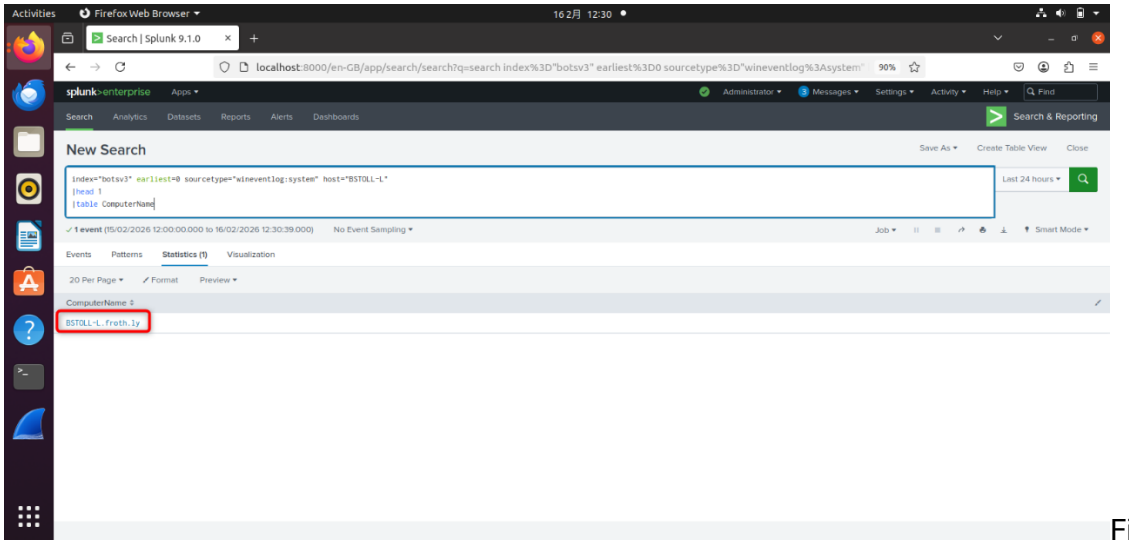

Fig.SO_CW2_Q8B

(E) Conclusion

In this report, I used the SOC tier 2 (incident responder) thinking to investigate the incidents. I successfully go through the detection phases and the response phases.
Further evaluate the incidents, I found out what Frothly lack of. And using the tier 3 (threat hunter) thinking, he suggested strategies are as follows:

Use MFA if needs to process the AWS API activity.
Use "Amazon S3 Block Public Access"[3] to avoid public access by overriding the access policies in Amazon S3 resources.
Use "automated playbooks"[4] to response to the threat.
Process the outliers scanning regularly

(F) References

[1] YouTube, “YouTube,” 2026. [Online]. Available: https://www.youtube.com/watch?v=2cX-Nv0geEY. Accessed: Feb. 19, 2026.

[2] J. Gibbins, “Splunk BOTSv3 Write-Up,” *James’s Peredutions*, Sep. 8, 2020. [Online]. Available: https://www.jamesgibbins.com/botsv3/. Accessed: Feb. 19, 2026.

[3] Amazon Web Services, Inc., “Amazon S3 Block Public Access,” 2026. [Online]. Available: https://aws.amazon.com/tw/s3/features/block-public-access/ . Accessed: Feb. 19, 2026.

[4] Amazon Web Services, “Playbooks - Automated Security Response on AWS,” AWS Solutions Implementation Guide Documentation. [Online]. Available: https://docs.aws.amazon.com/solutions/latest/automated-security-response-on-aws/playbooks-1.html . Accessed: Feb. 19, 2026.

[5] Q-Sec Security Operations Center, “SOC Roles & Responsibilities: Tier 1, Tier 2, Tier 3 Explained,”

Dec. 23, 2025. [Online]. Available: https://q-sec.com/soc-knowledge-base/soc-roles-responsibilities-tier-1-2-3. Accessed: Feb. 19, 2026.