CYB102 Project 7

(🔗 Instructions Page)

👤 Student Name: Weicong Xie
✉️ Student Email: Weicongx.wx@gmail.com

Reflection (Required)

> 🤔 **Reflection Question #1:** If I had to **explain "what is an IOC" in 3 emojis,** they would be… (Feel free to put other comments about your experience in this unit here, too!)
>
> 🕵️💻🚨

> 🧠**Reflection Question #2:** If you found out that an IP address was reported malicious a year ago, would you still consider it dangerous? Why or why not?
>
> I would still consider it dangerous and approach with caution because any sign of abuse should not be overlooked.

> 📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!

Required Challenges (Required)

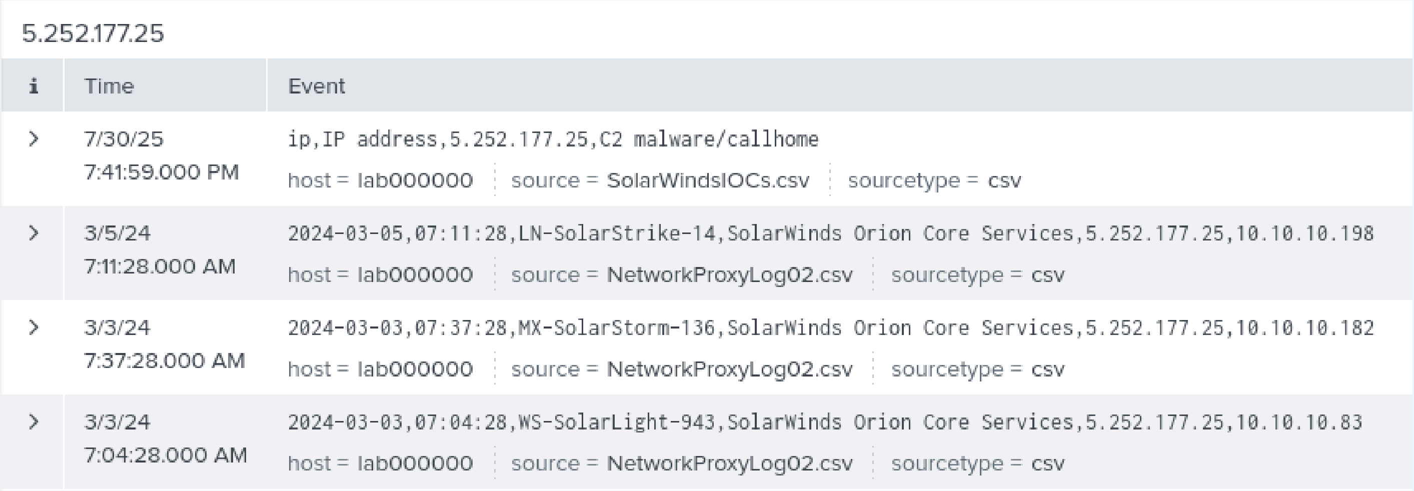
Match #1

Steps 1-2.5: General match data from Splunk (see Step 2.5)

Matched IP address:	**5.252.177.25**
The event date(s) and time(s):	- **3/3/24 7:04:28.000 AM** - **3/3/24 7:37:28.000 AM** - **3/5/24 7:11:28.000 AM**
Affected computer(s):	- **WS-SolarLight-943**

- **MX-SolarStorm-136**
- **LN-SolarStrike-14**

Step 2.5: Screenshot of the match in Splunk



5.252.177.25

i	Time	Event

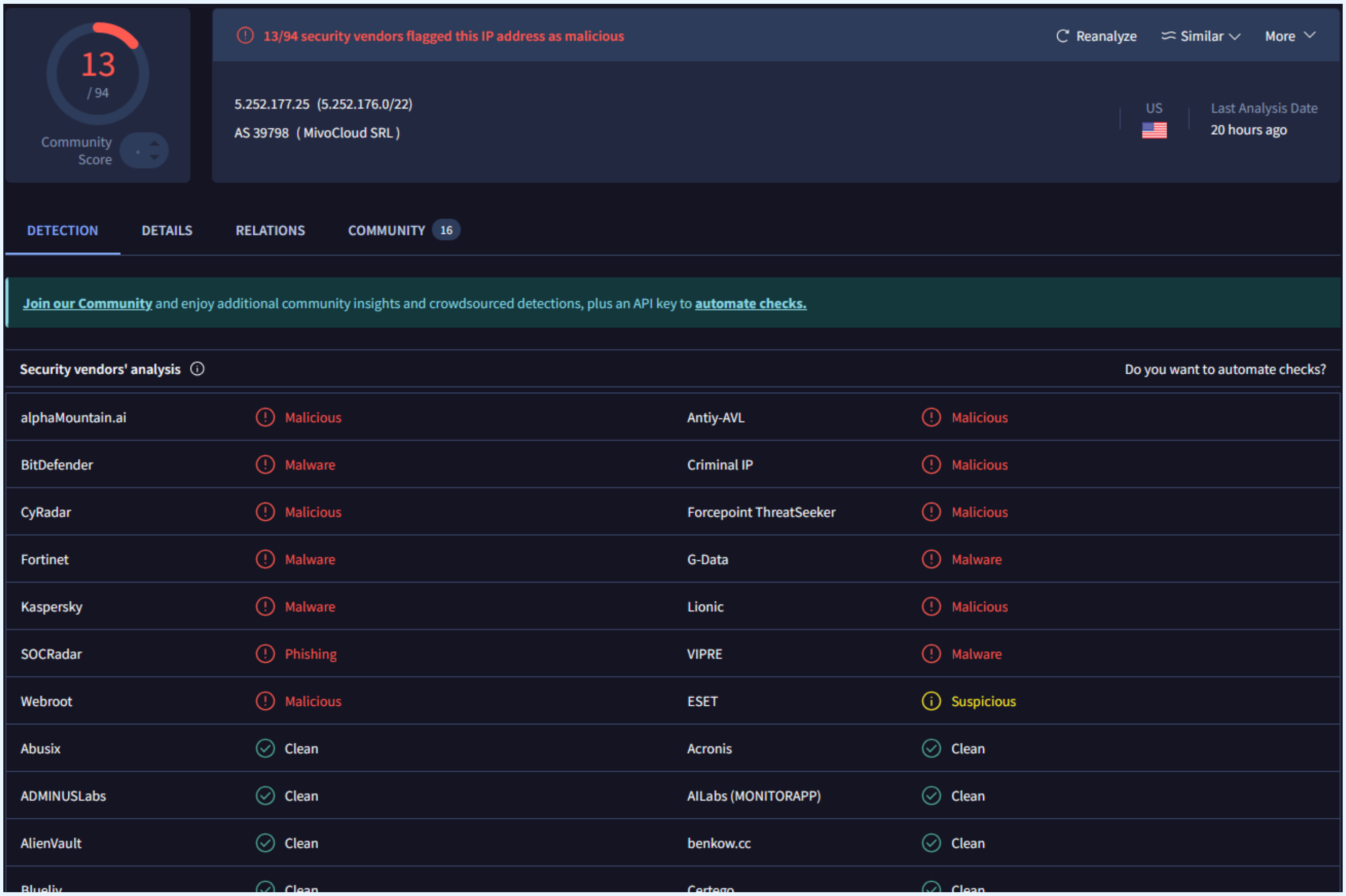
>	7/30/25
	7:41:59.000 PM
		`ip,IP address,5.252.177.25,C2 malware/callhome`
		host = lab000000 source = SolarWindsIOCs.csv sourcetype = csv

>	3/5/24
	7:11:28.000 AM
		`2024-03-05,07:11:28,LN-SolarStrike-14,SolarWinds Orion Core Services,5.252.177.25,10.10.10.198`
		host = lab000000 source = NetworkProxyLog02.csv sourcetype = csv

>	3/3/24
	7:37:28.000 AM
		`2024-03-03,07:37:28,MX-SolarStorm-136,SolarWinds Orion Core Services,5.252.177.25,10.10.10.182`
		host = lab000000 source = NetworkProxyLog02.csv sourcetype = csv

>	3/3/24
	7:04:28.000 AM
		`2024-03-03,07:04:28,WS-SolarLight-943,SolarWinds Orion Core Services,5.252.177.25,10.10.10.83`
		host = lab000000 source = NetworkProxyLog02.csv sourcetype = csv

Step 3: Screenshot of VirusTotal search for the IP listed above



13/94 security vendors flagged this IP address as malicious

5.252.177.25 (5.252.176.0/22)
AS 39798 (MivoCloud SRL)

US

Last Analysis Date
20 hours ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis — Do you want to automate checks?

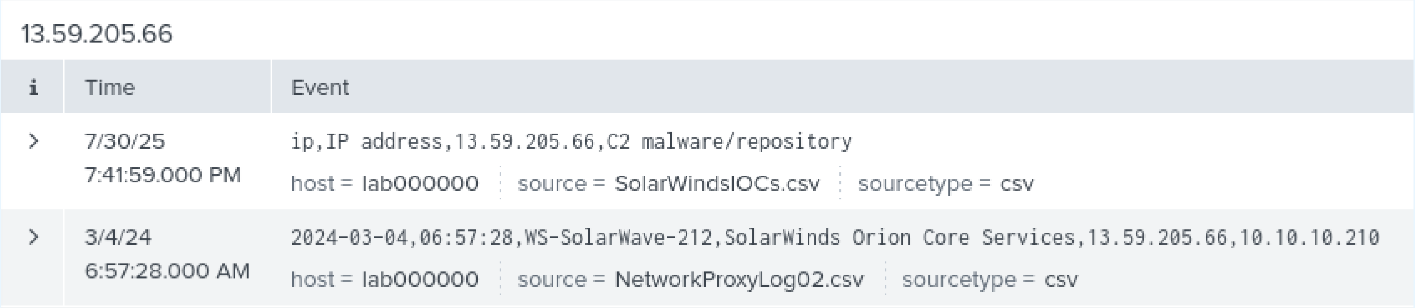
alphaMountain.ai	Malicious	Antiy-AVL	Malicious
BitDefender	Malware	Criminal IP	Malicious
CyRadar	Malicious	Forcepoint ThreatSeeker	Malicious
Fortinet	Malware	G-Data	Malware
Kaspersky	Malware	Lionic	Malicious
SOCRadar	Phishing	VIPRE	Malware
Webroot	Malicious	ESET	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	benkow.cc	Clean
Blueliv	Clean	Certego	Clean

Match #2

Steps 1-2.5: General match data from Splunk (see Step 2.5)

Matched IP address:	**13.59.205.66**
The event date(s) and time(s):	**3/4/24 6:57:28.000 AM**
Affected computer(s):	**WS-SolarWave-212**

Step 2.5: Screenshot of the match in Splunk



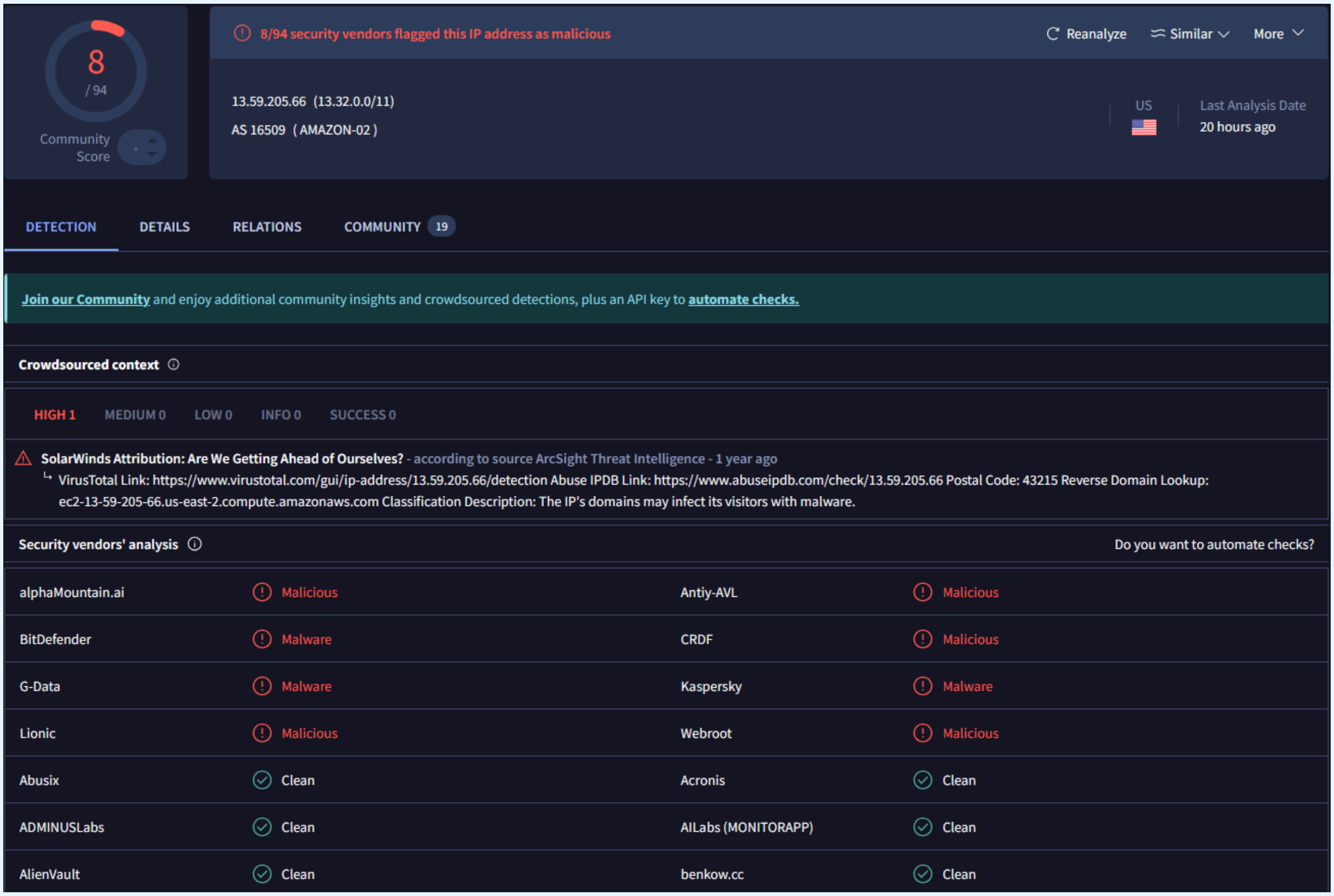
13.59.205.66

i	Time	Event

>	7/30/25
	7:41:59.000 PM
		`ip,IP address,13.59.205.66,C2 malware/repository`
		host = lab000000 ⋮ source = SolarWindsIOCs.csv ⋮ sourcetype = csv

>	3/4/24
	6:57:28.000 AM
		`2024-03-04,06:57:28,WS-SolarWave-212,SolarWinds Orion Core Services,13.59.205.66,10.10.10.210`
		host = lab000000 ⋮ source = NetworkProxyLog02.csv ⋮ sourcetype = csv

Step 3: Screenshot of VirusTotal search for the IP listed above



8/94 security vendors flagged this IP address as malicious

13.59.205.66 (13.32.0.0/11)
AS 16509 (AMAZON-02)

US

Last Analysis Date
20 hours ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Crowdsourced context

HIGH 1 MEDIUM 0 LOW 0 INFO 0 SUCCESS 0

SolarWinds Attribution: Are We Getting Ahead of Ourselves? - according to source ArcSight Threat Intelligence - 1 year ago
↳ VirusTotal Link: https://www.virustotal.com/gui/ip-address/13.59.205.66/detection Abuse IPDB Link: https://www.abuseipdb.com/check/13.59.205.66 Postal Code: 43215 Reverse Domain Lookup: ec2-13-59-205-66.us-east-2.compute.amazonaws.com Classification Description: The IP's domains may infect its visitors with malware.

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Malicious	Antiy-AVL	Malicious
BitDefender	Malware	CRDF	Malicious
G-Data	Malware	Kaspersky	Malware
Lionic	Malicious	Webroot	Malicious
Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	benkow.cc	✓ Clean

> **Steps 1-2.5:** General match data from Splunk (see Step 2.5)

If you find a Match #3, enter it in the Stretch Challenge below!

Splunk Dashboard Query

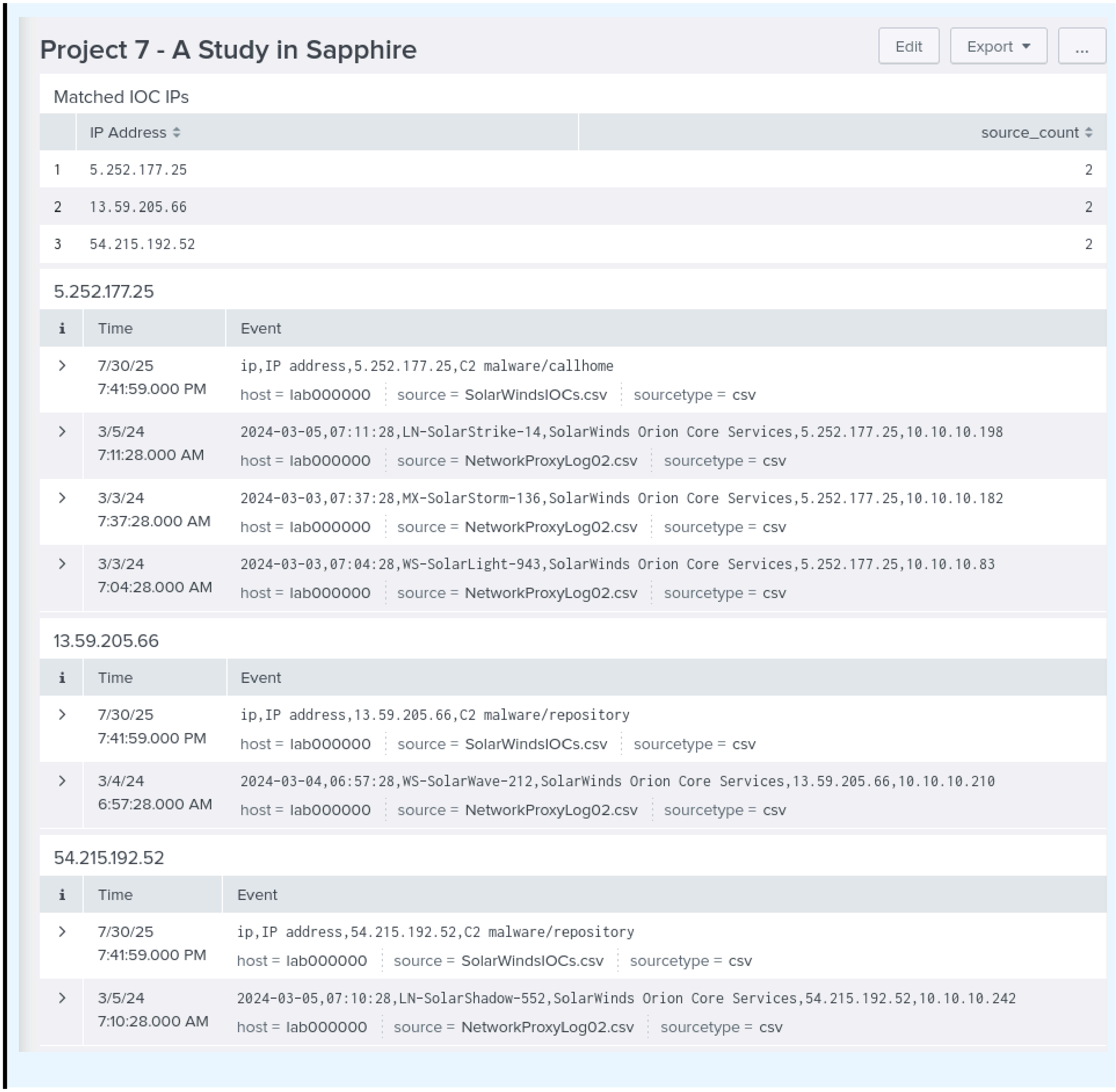
> **Step 4:** Enter the search query used to generate your Splunk Dashboard below

```
(index=main source="SolarWindsIOCs.csv" OR source="NetworkProxyLog02.csv")

| stats dc(source) as source_count by "IP Address"

| where source_count=2

| sort "IP Address"
```



Project 7 - A Study in Sapphire

Matched IOC IPs

	IP Address	source_count
1	5.252.177.25	2
2	13.59.205.66	2
3	54.215.192.52	2

5.252.177.25

i	Time	Event
>	7/30/25 7:41:59.000 PM	ip,IP address,5.252.177.25,C2 malware/callhome host = lab000000 source = SolarWindsIOCs.csv sourcetype = csv
>	3/5/24 7:11:28.000 AM	2024-03-05,07:11:28,LN-SolarStrike-14,SolarWinds Orion Core Services,5.252.177.25,10.10.10.198 host = lab000000 source = NetworkProxyLog02.csv sourcetype = csv
>	3/3/24 7:37:28.000 AM	2024-03-03,07:37:28,MX-SolarStorm-136,SolarWinds Orion Core Services,5.252.177.25,10.10.10.182 host = lab000000 source = NetworkProxyLog02.csv sourcetype = csv
>	3/3/24 7:04:28.000 AM	2024-03-03,07:04:28,WS-SolarLight-943,SolarWinds Orion Core Services,5.252.177.25,10.10.10.83 host = lab000000 source = NetworkProxyLog02.csv sourcetype = csv

13.59.205.66

i	Time	Event
>	7/30/25 7:41:59.000 PM	ip,IP address,13.59.205.66,C2 malware/repository host = lab000000 source = SolarWindsIOCs.csv sourcetype = csv
>	3/4/24 6:57:28.000 AM	2024-03-04,06:57:28,WS-SolarWave-212,SolarWinds Orion Core Services,13.59.205.66,10.10.10.210 host = lab000000 source = NetworkProxyLog02.csv sourcetype = csv

54.215.192.52

i	Time	Event
>	7/30/25 7:41:59.000 PM	ip,IP address,54.215.192.52,C2 malware/repository host = lab000000 source = SolarWindsIOCs.csv sourcetype = csv
>	3/5/24 7:10:28.000 AM	2024-03-05,07:10:28,LN-SolarShadow-552,SolarWinds Orion Core Services,54.215.192.52,10.10.10.242 host = lab000000 source = NetworkProxyLog02.csv sourcetype = csv

Stretch Challenge (Optional)

Match #3

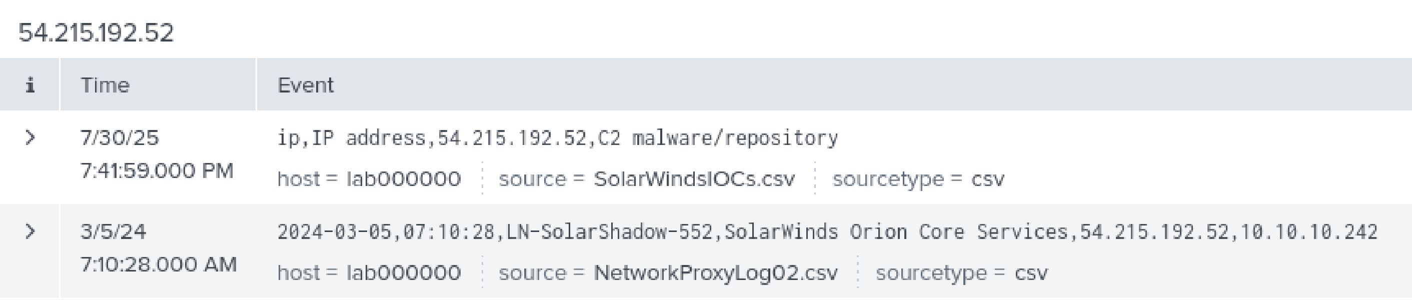
Steps 1-2.5: General match data from Splunk (see Step 2.5)

Matched IP address: **54.215.192.52**

The event date(s) and time(s): **3/5/24 7:10:28.000 AM**

Affected computer(s): **LN-SolarShadow-552**

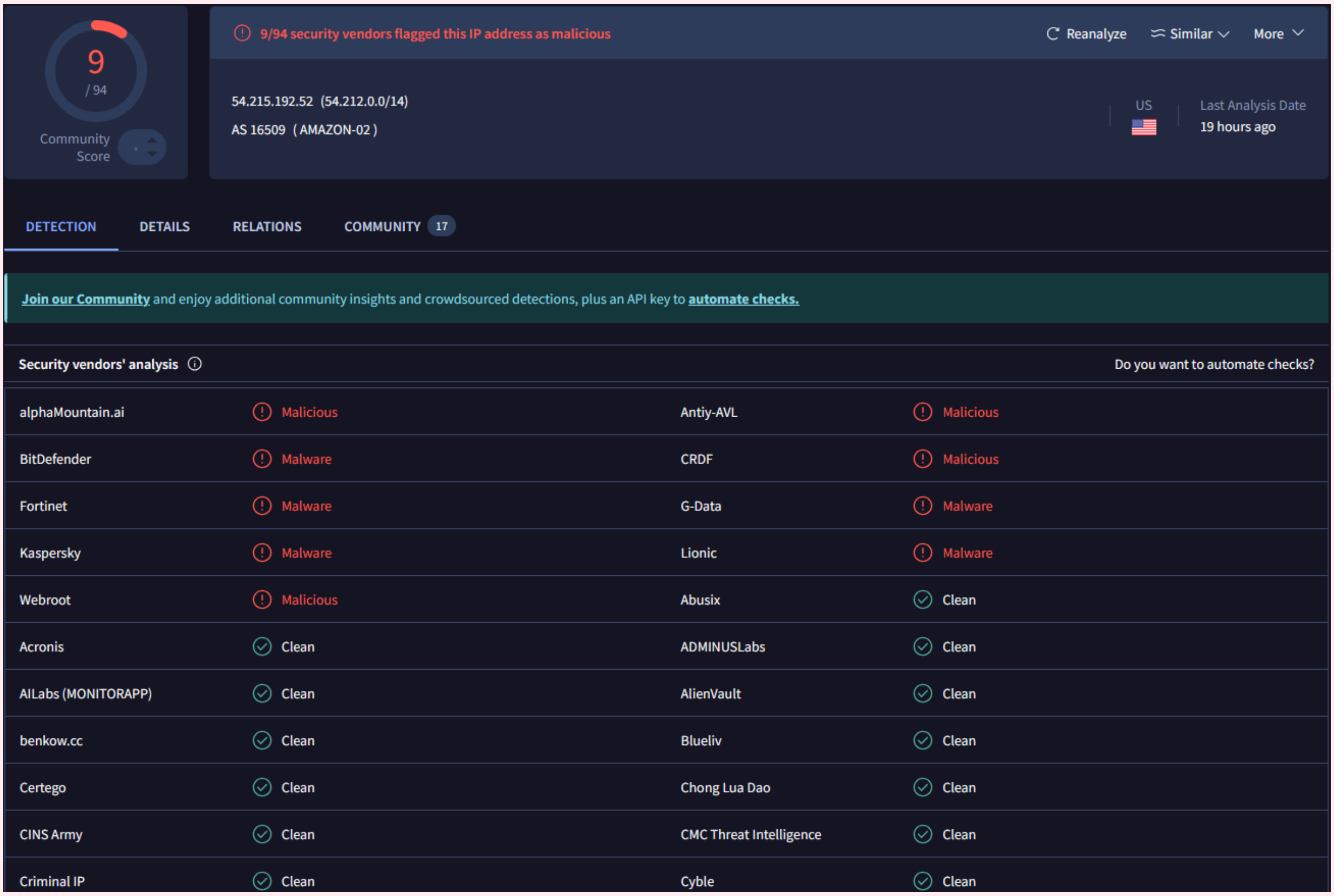
Step 2.5: Screenshot of the match in Splunk



54.215.192.52

i	Time	Event
>	7/30/25 7:41:59.000 PM	ip,IP address,54.215.192.52,C2 malware/repository host = lab000000 ⁝ source = SolarWindsIOCs.csv ⁝ sourcetype = csv
>	3/5/24 7:10:28.000 AM	2024-03-05,07:10:28,LN-SolarShadow-552,SolarWinds Orion Core Services,54.215.192.52,10.10.10.242 host = lab000000 ⁝ source = NetworkProxyLog02.csv ⁝ sourcetype = csv

Step 3: Screenshot of VirusTotal search for the IP listed above



9/94 security vendors flagged this IP address as malicious

54.215.192.52 (54.212.0.0/14)
AS 16509 (AMAZON-02)

US

Last Analysis Date
19 hours ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ

Do you want to automate checks?

alphaMountain.ai	ⓘ Malicious	Antiy-AVL	ⓘ Malicious
BitDefender	ⓘ Malware	CRDF	ⓘ Malicious
Fortinet	ⓘ Malware	G-Data	ⓘ Malware
Kaspersky	ⓘ Malware	Lionic	ⓘ Malware
Webroot	ⓘ Malicious	Abusix	✓ Clean
Acronis	✓ Clean	ADMINUSLabs	✓ Clean
AILabs (MONITORAPP)	✓ Clean	AlienVault	✓ Clean
benkow.cc	✓ Clean	Blueliv	✓ Clean
Certego	✓ Clean	Chong Lua Dao	✓ Clean
CINS Army	✓ Clean	CMC Threat Intelligence	✓ Clean
Criminal IP	✓ Clean	Cyble	✓ Clean

Steps 1-2.5: General match data from Splunk (see Step 2.5)

Bonus Task #1

Import a new set of IOC data into Splunk, then search your network data for matches.

> A link to the threat source used:
>
> **TODO**
>
> Screenshot(s) of your Splunk search that shows you investigating with the newly imported data:
>
> **[Insert Screenshot(s) Here]**
>
> A short answer describing your findings: (Even if you didn't find anything, you should explain where you looked and why!)
>
> **TODO**

Submission Checklist

👉*Check off each of the features you have completed.* ***You will only be graded on the features you check off.***

Required Challenges

- ☑ ~~Match #1~~
- ☑ ~~Match #2~~
- ☑ ~~Splunk Dashboard Query~~

Stretch Challenge

- ☑ ~~Match #3~~
- □ Bonus Task #1