

 Student Name: Didier Joseph DESMANGLES
 Student Email: djdesmangles@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!)

IOC in cybersecurity is “Indicator Of Compromise”. It is a digital artifact or sign that suggests a potential security breach, malicious activity, or other unwanted behavior in a network or system. They could be unusual IP addresses, unfamiliar file names or hashes on a system, anomalous account activities like unexpected logins or privilege escalations or unusual network traffic patterns.

If I had to explain "IOC" (Indicator of Compromise) in three emojis, they would be:



-  Red flag for the alert to something suspicious
-  Magnifying glass for investigating it further
-  Computer to show it's a cyber-related threat

 **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?

If an IP address was flagged as malicious a year ago, I'd consider it potentially dangerous and approach it cautiously. Here's why:

IP Reuse and Reassignment: Many IP addresses get reassigned frequently, especially in cloud environments. This IP might now belong to a different, legitimate entity.

But,

Persistence of Threats: Some threat actors maintain control over the same IP addresses for

long periods, particularly if they're using them in advanced, ongoing attack campaigns. In this case, an old report could still be relevant.

Reputation Checks: It's important to check for updated information from threat intelligence sources. If the IP is currently clean, it may have been de-listed or cleared, making it less likely to pose a threat.

Additional Context: Other factors like current network behavior, connection frequency, and whether it's paired with other IOCs could strengthen or weaken its threat profile.

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

TEAM 17 !!! Israel Melendez !!!

Required Challenges (Required)

Match #1

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): 2024-03-04 06:57:28

Affected computer(s): WS-SolarWave-212

Step 2.5: Screenshot of the match in Splunk

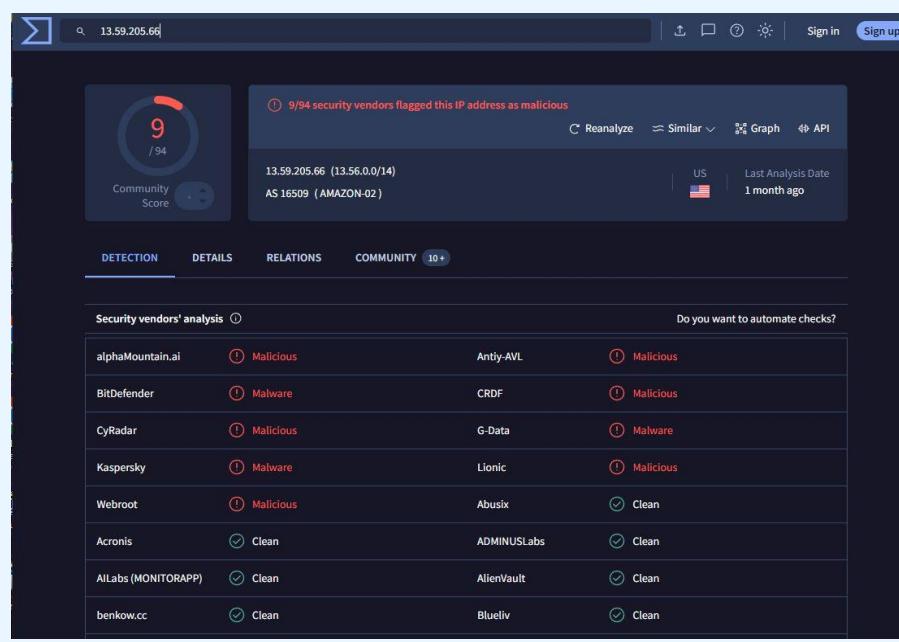
The screenshot shows a Splunk search interface with the following details:

- Search Bar:** Contains the following SPL query:

```
1 | index="pathcode" source="SolarWindsIOCs.csv" OR index="pathcode" source="NetworkProxyLog02.csv"
2 | stats values(source) as sources, values("Computer Name") as ComputerName, values("User Agent") as UserAgent, values(Date)
   as Date, values(Time) as Time by "IP Address"
3 | where mvcount(sources) > 1
4 | table "IP Address", ComputerName, UserAgent, Date, Time|
```
- Statistics Tab:** Selected, showing 1,043 events found.
- Table View:** Displays a table with columns: IP Address, ComputerName, UserAgent, Date, and Time. The first row is highlighted with a green border, corresponding to the IP address 13.59.205.66.

IP Address	ComputerName	UserAgent	Date	Time
13.59.205.66	WS-SolarWave-212	SolarWinds Orion Core Services	2024-03-04	06:57:28
5.252.177.25	LN-SolarStrike-14 MX-SolarStorm-136 WS-SolarLight-943	SolarWinds Orion Core Services	2024-03-03 2024-03-05	07:04:28 07:11:28 07:37:28
54.215.192.52	LN-SolarShadow-552	SolarWinds Orion Core Services	2024-03-05	07:10:28

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



Match #2

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):
2024-03-03 07:04:28
2024-03-05 07:11:28
2024-03-05 07:37:28

Affected computer(s):
LN-SolarStrike-14
MX-SolarStorm-136
WS-SolarLight-943

Step 2.5: Screenshot of the match in Splunk

New Search

Save As ▾

Create Table View

Close

```
1 (index="pathcode" source="SolarWindsIOCs.csv") OR (index="pathcode" source="NetworkProxyLog02.csv")
2 | stats values(source) as sources , values("Computer Name") as ComputerName, values("User Agent") as UserAgent, values(Date)
     as Date, values(Time) as Time by "IP Address"
3 | where mvcount(sources) > 1
4 | table "IP Address", ComputerName, UserAgent, Date, Time
```

All time ▾



✓ 1,043 events (before 10/31/24 11:42:12.000 AM) No Event Sampling ▾

Job ▾ || ⌂ ↗ ⌄ ! Smart Mode ▾

Events Patterns Statistics (3) Visualization

100 Per Page ▾ Format Preview ▾

IP Address	ComputerName	UserAgent	Date	Time
13.59.205.66	WS-SolarWave-212	SolarWinds Orion Core Services	2024-03-04	06:57:28
5.252.177.25	LN-SolarStrike-14	SolarWinds Orion Core Services	2024-03-03	07:04:28
	MX-SolarStorm-136		2024-03-05	07:11:28
	WS-SolarLight-943			07:37:28
54.215.192.52	LN-SolarShadow-552	SolarWinds Orion Core Services	2024-03-05	07:10:28

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

The screenshot shows a detailed analysis of the IP address 5.252.177.25. The main header includes a search bar with the IP address, a user icon, and navigation links for 'Rereanalyze', 'Similar', 'Graph', and 'API'. On the left, a large circular 'Community Score' meter shows a value of 12 out of 94. The central panel displays the IP address (5.252.177.25), its subnet (5.252.176.0/22), and Autonomous System information (AS 39798 MivoCloud SRL). It also indicates 12 out of 94 vendors flagged it as malicious. A location indicator shows 'US' with a flag, and the 'Last Analysis Date' is '20 days ago'. Below this, tabs for 'DETECTION', 'DETAILS', 'RELATIONS', and 'COMMUNITY' are visible, with 'COMMUNITY' selected and a note of '10+' entries. A section titled 'Security vendors' analysis' lists 10 vendor verdicts: alphaMountain.ai (Malicious), BitDefender (Malware), CyRadar (Malicious), G-Data (Malware), Lionic (Malicious), SOCRadar (Malware), ESET (Suspicious), Acronis (Clean), and AllLabs (MONITORAPP) (Clean). To the right of this table is a prompt asking 'Do you want to automate checks?'. The overall theme is dark with blue and red highlights for vendor names and verdicts.

Vendor	Verdict	Tool	Verdict
alphaMountain.ai	Malicious	Antiy-AVL	Malicious
BitDefender	Malware	CRDF	Malicious
CyRadar	Malicious	Forcepoint ThreatSeeker	Malicious
G-Data	Malware	Kaspersky	Malware
Lionic	Malicious	MalwareURL	Malware
SOCRadar	Malware	Webroot	Malicious
ESET	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AllLabs (MONITORAPP)	Clean	AlienVault	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="pathcode" source="SolarWindsLOCs.csv" earliest=-24h@h) OR (index=index="pathcode"  
source="NetworkProxyLog02.csv" earliest=-24h@h)  
  
| stats values(source) as sources, values("Computer Name") as ComputerName, values("User  
Agent") as UserAgent, values(Date) as Date, values(Time) as Time by "IP Address"  
  
| where mvcount(sources) > 1  
  
| table "IP Address", ComputerName, UserAgent, Date, Time
```

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): 2024-03-05 07:10:28

Affected computer(s): LN-SolarShadow-552

Step 2.5: Screenshot of the match in Splunk

New Search

Save As ▾ Create Table View Close

```
1 (index="pathcode" source="SolarWindsIOCs.csv") OR (index="pathcode" source="NetworkProxyLog02.csv")
2 | stats values(source) as sources, values("Computer Name") as ComputerName, values("User Agent") as UserAgent, values(Date)
   as Date, values(Time) as Time by "IP Address"
3 | where mvcount(sources) > 1
4 | table "IP Address", ComputerName, UserAgent, Date, Time|
```

All time ▾

✓ 1,043 events (before 10/31/24 11:42:12.000 AM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events Patterns Statistics (3) Visualization

100 Per Page ▾

IP Address	ComputerName	UserAgent	Date	Time
13.59.205.66	WS-SolarWave-212	SolarWinds Orion Core Services	2024-03-04	06:57:28
5.252.177.25	LN-SolarStrike-14 MX-SolarStorm-136 WS-SolarLight-943	SolarWinds Orion Core Services	2024-03-03 2024-03-05	07:04:28 07:11:28 07:37:28
54.215.192.52	LN-SolarShadow-552	SolarWinds Orion Core Services	2024-03-05	07:10:28

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

The screenshot shows a security analysis interface for the IP address 54.215.192.52. The main header displays a large red '10' representing a Community Score out of 94. A status message indicates that 10/94 security vendors flagged the address as malicious. Navigation options include 'Reanalyze', 'Similar', 'Graph', and 'API'. Below the header, the IP address and its ASN (AS 16509, AMAZON-02) are listed, along with a US flag and the last analysis date (1 day ago). The interface features tabs for 'DETECTION', 'DETAILS', 'RELATIONS', and 'COMMUNITY' (with 10+ items). The 'DETECTION' tab is active, showing a table of security vendor analysis. The table includes columns for vendor name, detection status (e.g., Malicious or Clean), and associated threat intelligence sources (e.g., Antiy-AVL, CRDF, Fortinet, Kaspersky, Webroot, Acronis, AllLabs (MONITORAPP), benkow.cc). Each row also includes a 'Do you want to automate checks?' column with a green checkmark icon.

Security vendor	Detection	Associated Threat Intel	Action
alphaMountain.ai	Malicious	Antiy-AVL	Malicious
BitDefender	Malware	CRDF	Malicious
CyRadar	Malicious	Fortinet	Malware
G-Data	Malware	Kaspersky	Malware
Lionic	Malicious	Webroot	Malicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AllLabs (MONITORAPP)	Clean
AlienVault	Clean	benkow.cc	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:

<https://github.com/fox-it/cobaltstrike-extraneous-space/blob/master/cobaltstrike-servers.csv>

Screenshot(s) of your Splunk search that shows you investigating with the newly imported data:

The screenshot shows the Splunk Enterprise search interface. The search bar contains the following SPL query:

```
1 (index="pathcode" source="cobaltstrike-servers.csv") OR (index="pathcode" source="NetworkProxyLog02.csv")
2 | stats values(source) as sources, values("Computer Name") as ComputerName, values("User Agent") as UserAgent, values(Date) as Date, values(Time) as Time by "IP Address"
3 | where mvcount(sources) > 1
4 | table "IP Address", ComputerName, UserAgent, Date, Time
```

The search results summary indicates 10,586 events found before 11/1/24 12:11:48.000 PM. The Statistics tab is selected, showing 0 results. The visualization tab shows a chart with the message "No results found.".

A short answer describing your findings: (Even if you didn't find anything, you should explain where you looked and why!)

We use the same method as in "Required Challenge", which consists in checking that the IPs contained in the IOC file are not present in the "NetworkLog02.csv" file. If the IOC is present, then the system is compromised, as can be seen with the "SolarWinds" file.

In our case, we use the "counterstrike-servers" file, but there's no result.

So the system has not been infected by CounterStrike.

"IP Address" as an IOC (Indicator of Compromise) is relatively common in cybersecurity. IP addresses are often used as IOCs because they can help identify potential threat sources or entities attempting to compromise a network.

Available csv files regularly present IP Address addresses as IOC. But, in regards of "Reflexion Question #2", it is important to regularly check the system with updated IOC csv files.

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~~

💡 Tip: You can see specific grading information, including points breakdown, by going to [the grading page](#) on the course portal.

Submit your work!

Step 1: Click the Share button at the top of your screen double check that anyone with the link can edit.



General access



Anyone with the link ▾

Anyone on the internet with the link can edit

Editor ▾

Step 2: Copy the link to this document.



Step 3: Submit the link on the portal.

